Crittografia e sicurezza dei dati

ISIS Solari

Progetto Matematica 0,1,2,3

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su sottilissime lamine di seta, finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scrittore Giambattista Della Porta, XVI secolo).
- Uso di inchiostri simpatici.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Steganografia, l'arte di coprire i messaggi

steganós (coperto) - gráphein (scrivere)

- L'esule greco Demarato inviò agli Spartani un messaggio scritto su una tavoletta sotto uno strato di cera per avvisarli dell'imminente attacco dei Persiani (480 a.C.).
- Istièo rase i capelli ad uno schiavo, scrisse un messaggio sul cuoio capelluto, attese la ricrescita e inviò il messaggero ad Aristagora, incoraggiandolo a ribellarsi ai Persiani.
- Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissime che venivano appallottolate, coperte di cera e quindi inghiottite dal messaggero.
- Inchiostro a base di allume e aceto per scrivere sul guscio di un uovo sodo. L'inchiostro penetra e tinge l'albume solidificato. Sgusciando l'uovo si legge il messaggio (tecnica ideata dallo scienziato Giambattista Della Porta, XVI secolo).
- Uso di inchiostri *simpatici*.

Non è un sistema di trasmissione di messaggi segreti molto sicuro!!!

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)
La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)
La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)
La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)

La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)
La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)
La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Crittografia, l'arte di nascondere i messaggi

Kryptós (nascosto) - gráphein (scrivere)

La **Scitala lacedemonica** - Sparta (400 a.C.)

Piccolo bastone usato dagli spartani per arrotolare strisciolina di pelle su cui era scritto il messaggio (srotolata era impossibile leggere il testo)
La *chiave* per decifrare il messaggio era possedere un bastone dello stesso diametro.

La scitala è il primo esempio di sistema crittografico a **chiave simmetrica**.

Cifrario *Atbash* (IX-XIII secolo): cifratura biblica in cui vengono scambiate lettere equidistanti dagli estremi dell'alfabeto (alef-tav, bet-sin, kaf-lamed,ecc.) (in Geremia 25,26 compare la sostituzione di "Babel" con "Sesach").

Il cifrario di Cesare (100-44 a.C.)

Sostituzione monoalfabetica

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

La chiave è rappresentata dal numero N di posti in cui si "trasla" ogni lettera.

R I E M A N N
↓ ↓ ↓ ↓ ↓ ↓ ↓
U N H P D Q Q

Il cifrario di Cesare (100-44 a.C.)

Sostituzione monoalfabetica

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

La chiave è rappresentata dal numero N di posti in cui si "trasla" ogni lettera.

R	I	E	M	A	N	N
↓	↓	↓	↓	↓	↓	↓
U	N	H	P	D	Q	Q

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
H	U	F	G	D	I	M	L	N	T	P	C	S	R	O	E	B	Z	A	V	Q

In totale esistono $21 \cdot 20 \cdot 19 \cdot 18 \cdots 2 \cdot 1 = 21! \approx 51 \cdot 10^{18}$ chiavi di decrittazione.

Uso di una chiave: GRAVITAZIONALE

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
G	R	A	V	I	T	Z	O	N	L	E	B	C	D	F	H	M	P	Q	S	U

Con un pò di sudore si riesce abbastanza facilmente, a *forza bruta* e con l'aiuto della statistica, a scardinare messaggi cifrati tramite sostituzione monoalfabetica.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
H	U	F	G	D	I	M	L	N	T	P	C	S	R	O	E	B	Z	A	V	Q

In totale esistono $21 \cdot 20 \cdot 19 \cdot 18 \cdots 2 \cdot 1 = 21! \approx 51 \cdot 10^{18}$ chiavi di decrittazione.

Uso di una chiave: GRAVITAZIONALE

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
G	R	A	V	I	T	Z	O	N	L	E	B	C	D	F	H	M	P	Q	S	U

Con un pò di sudore si riesce abbastanza facilmente, a *forza bruta* e con l'aiuto della statistica, a scardinare messaggi cifrati tramite sostituzione monoalfabetica.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
H	U	F	G	D	I	M	L	N	T	P	C	S	R	O	E	B	Z	A	V	Q

In totale esistono $21 \cdot 20 \cdot 19 \cdot 18 \cdots 2 \cdot 1 = 21! \approx 51 \cdot 10^{18}$ chiavi di decrittazione.

Uso di una chiave: GRAVITAZIONALE

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
G	R	A	V	I	T	Z	O	N	L	E	B	C	D	F	H	M	P	Q	S	U

Con un pò di sudore si riesce abbastanza facilmente, a *forza bruta* e con l'aiuto della statistica, a scardinare messaggi cifrati tramite sostituzione monoalfabetica.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
H	U	F	G	D	I	M	L	N	T	P	C	S	R	O	E	B	Z	A	V	Q

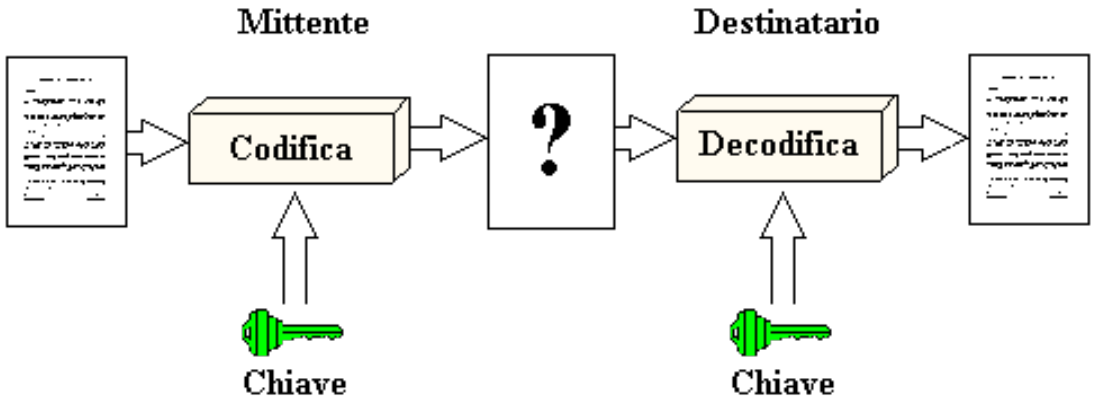
In totale esistono $21 \cdot 20 \cdot 19 \cdot 18 \cdots 2 \cdot 1 = 21! \approx 51 \cdot 10^{18}$ chiavi di decrittazione.

Uso di una chiave: GRAVITAZIONALE

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
G	R	A	V	I	T	Z	O	N	L	E	B	C	D	F	H	M	P	Q	S	U

Con un pò di sudore si riesce abbastanza facilmente, a *forza bruta* e con l'aiuto della statistica, a scardinare messaggi cifrati tramite sostituzione monoalfabetica.

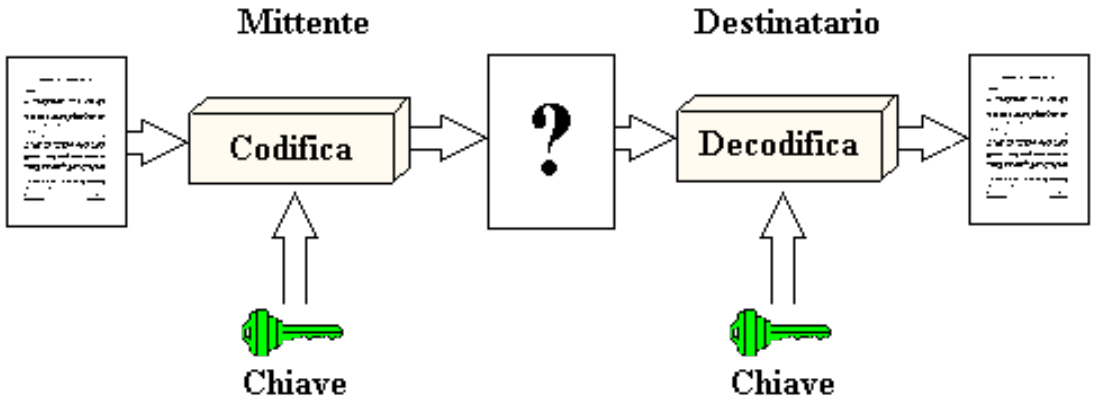
Sistema crittografico



ALGORITMO (procedimento generale di scrittura segreta)
CHIAVE (informazione usata come parametro per l'implementazione dell'algoritmo)
Legge di Kerckoffs *la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo. La sicurezza dipende solo dal tener celata la chiave.*

SIMMETRICA: stessa chiave ASIMMETRICA: due chiavi diverse

Sistema crittografico



ALGORITMO (procedimento generale di scrittura segreta)

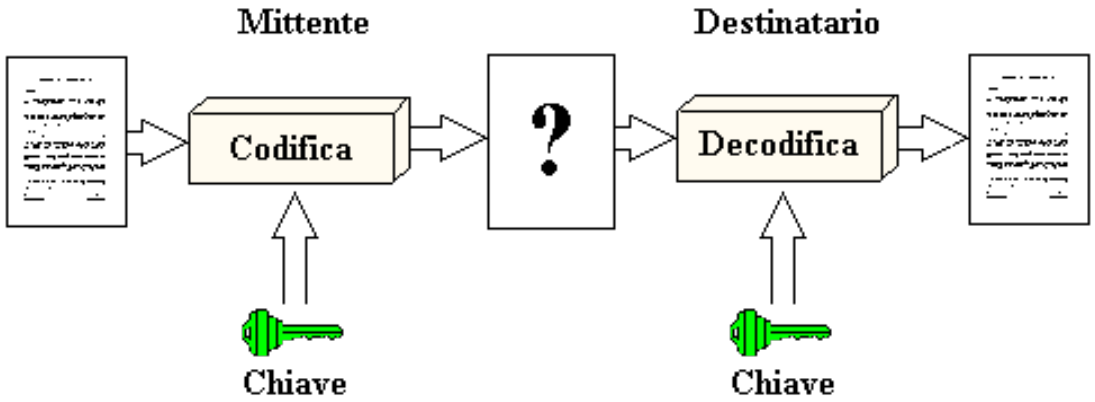
CHIAVE (informazione usata come parametro per l'implementazione dell'algoritmo)

Legge di Kerckoffs *la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo. La sicurezza dipende solo dal tener celata la chiave.*

SIMMETRICA: stessa chiave

ASIMMETRICA: due chiavi diverse

Sistema crittografico

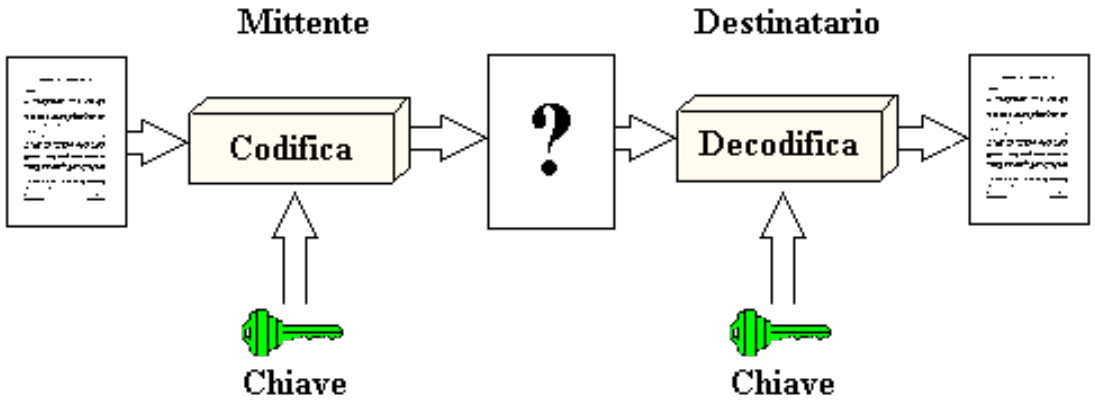


ALGORITMO (procedimento generale di scrittura segreta)
CHIAVE (informazione usata come parametro per l'implementazione dell'algoritmo)

Legge di Kerckoffs *la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo. La sicurezza dipende solo dal tener celata la chiave.*

SIMMETRICA: stessa chiave ASIMMETRICA: due chiavi diverse

Sistema crittografico

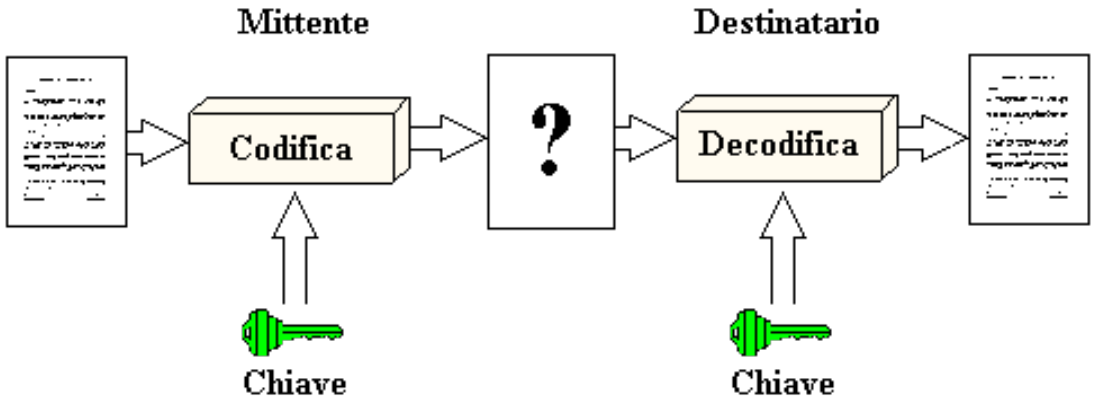


ALGORITMO (procedimento generale di scrittura segreta)
CHIAVE (informazione usata come parametro per l'implementazione dell'algoritmo)

Legge di Kerckoffs *la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo. La sicurezza dipende solo dal tener celata la chiave.*

SIMMETRICA: stessa chiave ASIMMETRICA: due chiavi diverse

Sistema crittografico

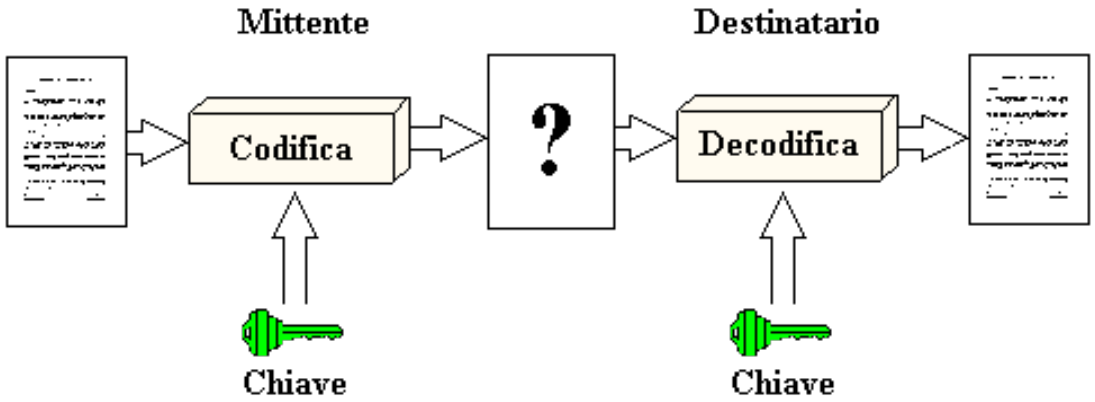


ALGORITMO (procedimento generale di scrittura segreta)
CHIAVE (informazione usata come parametro per l'implementazione dell'algoritmo)
Legge di Kerckoffs *la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo. La sicurezza dipende solo dal tener celata la chiave.*

SIMMETRICA: stessa chiave

ASIMMETRICA: due chiavi diverse

Sistema crittografico



ALGORITMO (procedimento generale di scrittura segreta)
CHIAVE (informazione usata come parametro per l'implementazione dell'algoritmo)
Legge di Kerckoffs *la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo. La sicurezza dipende solo dal tener celata la chiave.*

SIMMETRICA: stessa chiave

ASIMMETRICA: due chiavi diverse

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.

Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".

Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".

Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$ lettera "z": $0,49\%$ lettera "s": $4,98\%$

lettera "t": $5,62\%$ lettera "e": $11,79\%$ lettera "m": $2,52\%$

La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$	lettera "z": $0,49\%$	lettera "s": $4,98\%$
lettera "t": $5,62\%$	lettera "e": $11,79\%$	lettera "m": $2,52\%$

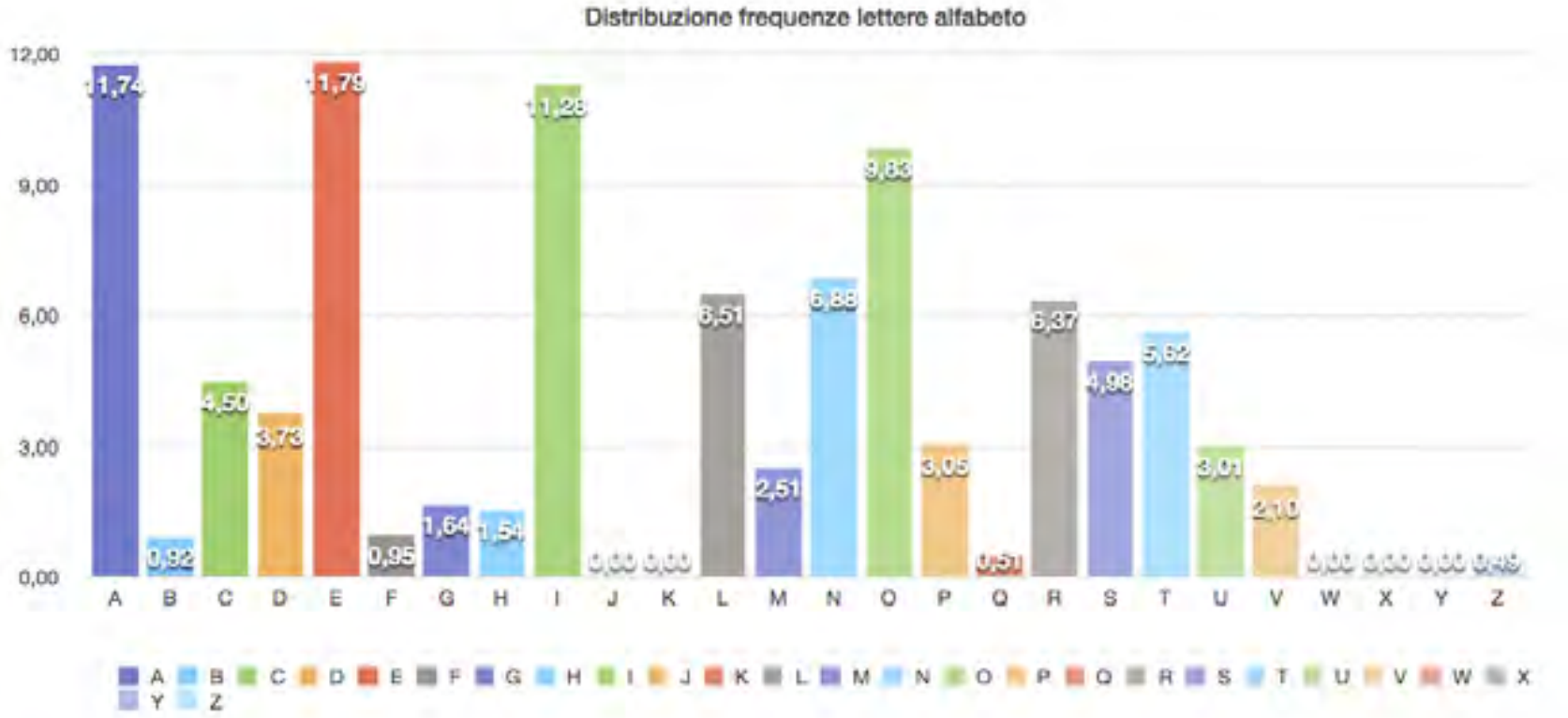
La nascita della crittoanalisi

Scienza dell'interpretazione di un messaggio di cui si ignora la chiave

I primi crittoanalisti furono arabi (IX-X secolo d.C.) e trassero spunto dallo studio del Corano.
Il filosofo degli arabi *al-Kindi* espose il metodo di decrittazione basato sull'**analisi delle frequenze** nella monografia "Sulla decifrazione dei messaggi crittati".
Il metodo è basato sull'analisi delle frequenze con cui compaiono le lettere dell'alfabeto di una determinata lingua (su un testo di lunghezza medio-alta).

Nell'alfabeto italiano:

lettera "a": $11,74\%$	lettera "z": $0,49\%$	lettera "s": $4,98\%$
lettera "t": $5,62\%$	lettera "e": $11,79\%$	lettera "m": $2,52\%$


Distribuzione frequenze lettere alfabeto
12,00
9,00
6,00
3,00
0,00
11,74
0,92
4,50
3,73
11,79
0,95
1,64
1,54
11,28
0,00
0,00
8,51
2,51
6,88
9,83
3,05
0,51
6,37
4,98
5,62
3,01
2,10
0,00
0,00
0,00
0,15
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatrè trentini entrarono a Trento tutti e trentatrè trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di Georges Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalista veneziano del 1500);
- Philibert Babou (cifrista del re di Francia Francesco I) che lui stesso dedicasse giorni e notti alla decrittazione tanti e tali messaggi;
- François Viète (francese) per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno".

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di Georges Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalista veneziano del 1500);
- Philibert Babou (cifrista del re di Francia Francesco I) che lungamente dedicasse giorni e notti alla decrittazione tanti e che posteriore famiglie;
- François Viète (francese), per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in compagnia con Archimede".

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalista veneziano del 1500);
- Philibert Babou (cifrista del re di Francia Francesco I) che impiegava dedicasse giorni e notti alla decrittazione tanto che, secondo un famoso
- François Viète (francese) per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un pericoloso mago in combutta con Aborgeal

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalista veneziano del 1500);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie
- François Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).

Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalista veneziano del 1500);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie
- François Viète (francese), per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I) decifrò lettere dedicasse giorno e notte alla decrittazione tanto che lo stesso re lo
- François Viète (francese) per la sua abilità nel decrittare lunghi messaggi spagnoli fu etichettato come "un arrendevole in combutta col Maligno".

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- François Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- François Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- François Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- Françoys Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).

Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- Françoys Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).
Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- Françoys Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).

Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

La tecnica perde efficacia (almeno in parte):

- testi di breve lunghezza;
- testi anomali del tipo "Trentatré trentini entrarono a Trento tutti e trentatré trotterellando";
- testi anomali in cui mancano del tutto lettere solitamente molto frequenti (*La disparition* di George Perec è un romanzo di 200 pagine non contenente alcuna lettera "e").

In Europa la crittoanalisi iniziò a fiorire a partire dal XVI secolo.

- Giovanni Soro (crittoanalisti veneziano del 1506);
- Philibert Babou (cifrista del re di Francia Francesco I): di lui si dice dedicasse giorni e notti alla decrittazione tant'è che padrone e moglie...
- Françọis Viète (francese): per la sua abilità nel decrittare i messaggi spagnoli fu etichettato come "un arcidiavolo in combutta col Maligno"

La bravura dei crittoanalisti portò all'introduzione nei testi cifrati delle *nulle*, cioè lettere o simboli che non corrispondono a nessun carattere dell'alfabeto (quindi sono privi di significato).

Si iniziò anche a far uso dei *nomenclatori*, cioè modi di crittare che fanno uso di un alfabeto cifrante e di un piccolo numero di parole in codice.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.

Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.

Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti..., l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

Cifrari a sostituzione polialfabetica

- Non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione nel messaggio in chiaro non viene usato lo stesso alfabeto cifrante.
- E' un sistema meno debole del cugino monoalfabetico.
- Conoscere la frequenza con cui compaiono i simboli è di utilità meno diretta.

Codice di Vigenère(Blaise de Vigenère, 1523-1596) le lettere del messaggio non sono traslate tutte dello stesso valore.
Chiave (verme) KEPLERO $\longrightarrow$ $(11, 5, 16, 12, 5, 18, 15)$.
Il primo carattere viene traslato di 10 posti, il secondo carattere di 4 posti, il terzo di 15 posti. . . , l'ottavo carattere è traslato nuovamente di 10 posti e si continua ciclicamente.

N	E	L	M	E	Z	Z	O	D	E	L	C	A	M	M	I	N
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
K	E	P	L	E	R	O	K	E	P	L	E	R	O	K	E	P
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	I	A	X	I	Q	N	Y	H	T	W	G	R	A	W	M	C

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	**X**	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Schema per la cifratura tramite il metodo di Vigenère (alfabeto anglosassone).

N	E	L	M	E	Z	Z	O	D	E	L	C	A	M	M	I	N
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
K	E	P	L	E	R	O	K	E	P	L	E	R	O	K	E	P
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	I	A	X	I	Q	N	Y	H	T	W	G	R	A	W	M	C

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	**X**	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Schema per la cifratura tramite il metodo di Vigenère (alfabeto anglosassone).

N	E	L	M	E	Z	Z	O	D	E	L	C	A	M	M	I	N
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
K	E	P	L	E	R	O	K	E	P	L	E	R	O	K	E	P
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	I	A	X	I	Q	N	Y	H	T	W	G	R	A	W	M	C

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Schema per la cifratura tramite il metodo di Vigenère (alfabeto anglosassone).

Kasiski e Babbage vs Vigenere

- In un crittogramma alla Vigenère si trovano spesso sequenze identiche di caratteri ad una certa distanza una dall'altra.

N	O	N	V	E	D	O	N	O	N	S	E	N	T	O	N	O	N	P	A	R	L	O
S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L
F	**C**	**Y**	Z	W	R	Z	**R**	**G**	**B**	D	I	F	H	Z	**R**	**G**	**B**	A	E	J	Z	Z

- Se due lettere identiche si trovano ad una distanza pari alla lunghezza della chiave o ad un suo multiplo, vengono cifrate allo stesso modo.
- Per congetturare la lunghezza N della chiave, si calcola il massimo comune divisore tra le distanze tra sequenze ripetute.
- Si divide il messaggio cifrato in stringhe di lunghezza N e si mettono tali stringhe in colonna, e si effettua l'analisi delle frequenze su ciascuna colonna.

Kasiski e Babbage vs Vigenere

- In un crittogramma alla Vigenère si trovano spesso sequenze identiche di caratteri ad una certa distanza una dall'altra.

N	O	N	V	E	D	O	N	O	N	S	E	N	T	O	N	O	N	P	A	R	L	O	
S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	
F	**C**	**Y**	Z	W	R	Z	**R**	**G**	**B**	D	I	F	H	Z	**R**	**G**	**B**	A	E	J	Z	Z	

- Se due lettere identiche si trovano ad una distanza pari alla lunghezza della chiave o ad un suo multiplo, vengono cifrate allo stesso modo.
- Per congetturare la lunghezza N della chiave, si calcola il massimo comune divisore tra le distanze tra sequenze ripetute.
- Si divide il messaggio cifrato in strisce di lunghezza N e si sovrappongono tali strisce in colonne, e si effettua l'analisi delle frequenze su ciascuna colonna.

Kasiski e Babbage vs Vigenere

- In un crittogramma alla Vigenère si trovano spesso sequenze identiche di caratteri ad una certa distanza una dall'altra.

  N O N V E D O N O N S E N T O N O N P A R L O
  S O L E S O L E S O L E S O L E S O L E S O L
  F C Y Z W R Z **R G B** D I F H Z **R G B** A E J Z Z

- Se due lettere identiche si trovano ad una distanza pari alla lunghezza della chiave o ad un suo multiplo, vengono cifrate allo stesso modo.
- Per congetturare la lunghezza N della chiave, si calcola il massimo comune divisore tra le distanze tra sequenze ripetute.
- Si divide il messaggio cifrato in stringhe di lunghezza N, si dispongono tali stringhe in colonna, e si effettua l'analisi delle frequenze su ciascuna colonna.

Kasiski e Babbage vs Vigenere

- In un crittogramma alla Vigenère si trovano spesso sequenze identiche di caratteri ad una certa distanza una dall'altra.

  N O N V E D O N O N S E N T O N O N P A R L O
  S O L E S O L E S O L E S O L E S O L E S O L
  F C Y Z W R Z **R G B** D I F H Z **R G B** A E J Z Z

- Se due lettere identiche si trovano ad una distanza pari alla lunghezza della chiave o ad un suo multiplo, vengono cifrate allo stesso modo.
- Per congetturare la lunghezza N della chiave, si calcola il massimo comune divisore tra le distanze tra sequenze ripetute.
- Si divide il messaggio cifrato in stringhe di lunghezza N, si dispongono tali stringhe in colonna, e si effettua l'analisi delle frequenze su ciascuna colonna.

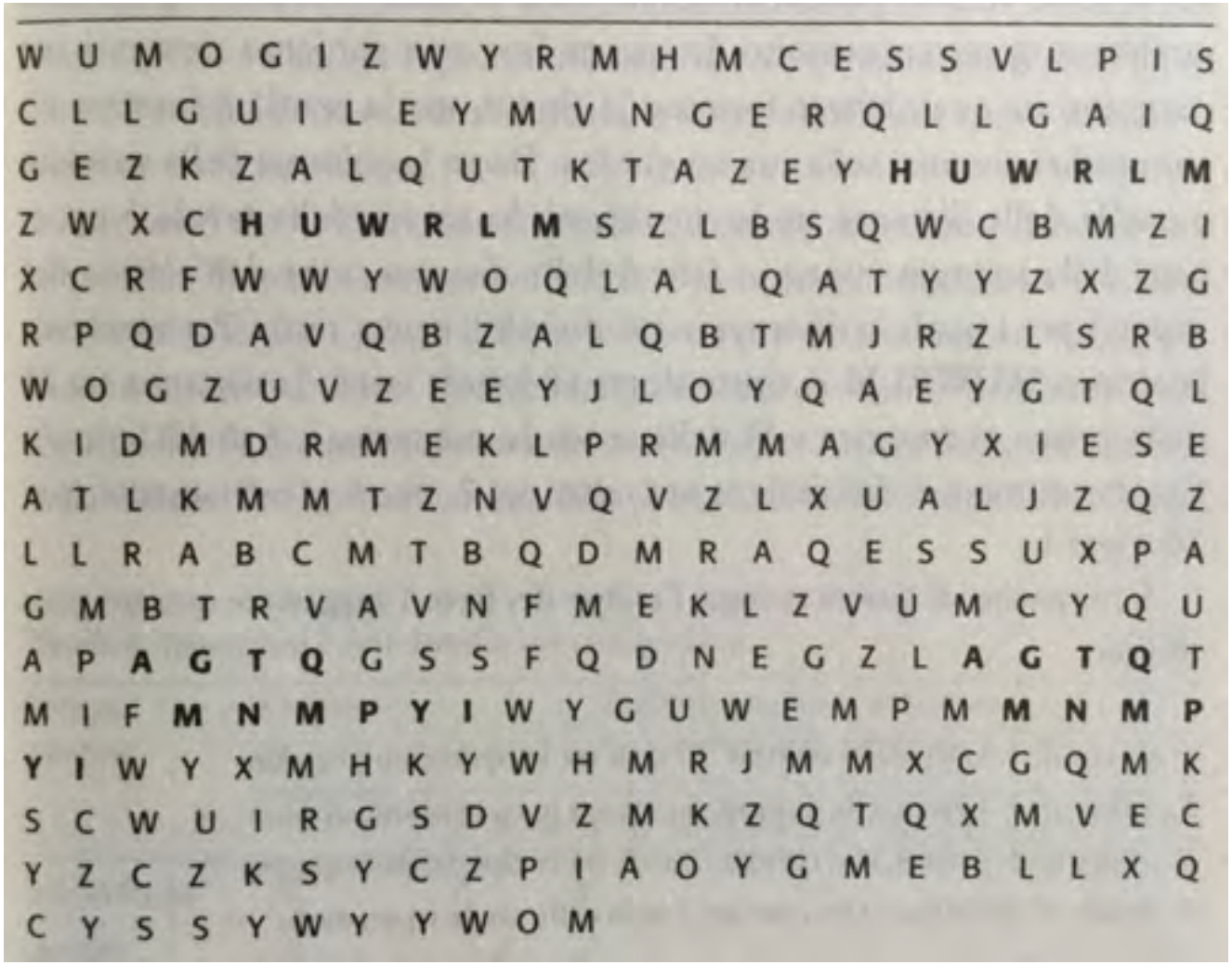
Kasiski e Babbage vs Vigenere

- In un crittogramma alla Vigenère si trovano spesso sequenze identiche di caratteri ad una certa distanza una dall'altra.

  N O N V E D O N O N S E N T O N O N P A R L O
  S O L E S O L E S O L E S O L E S O L E S O L
  F C Y Z W R Z **R G B** D I F H Z **R G B** A E J Z Z

- Se due lettere identiche si trovano ad una distanza pari alla lunghezza della chiave o ad un suo multiplo, vengono cifrate allo stesso modo.
- Per congetturare la lunghezza N della chiave, si calcola il massimo comune divisore tra le distanze tra sequenze ripetute.
- Si divide il messaggio cifrato in stringhe di lunghezza N, si dispongono tali stringhe in colonna, e si effettua l'analisi delle frequenze su ciascuna colonna.

Esempio di crittogramma



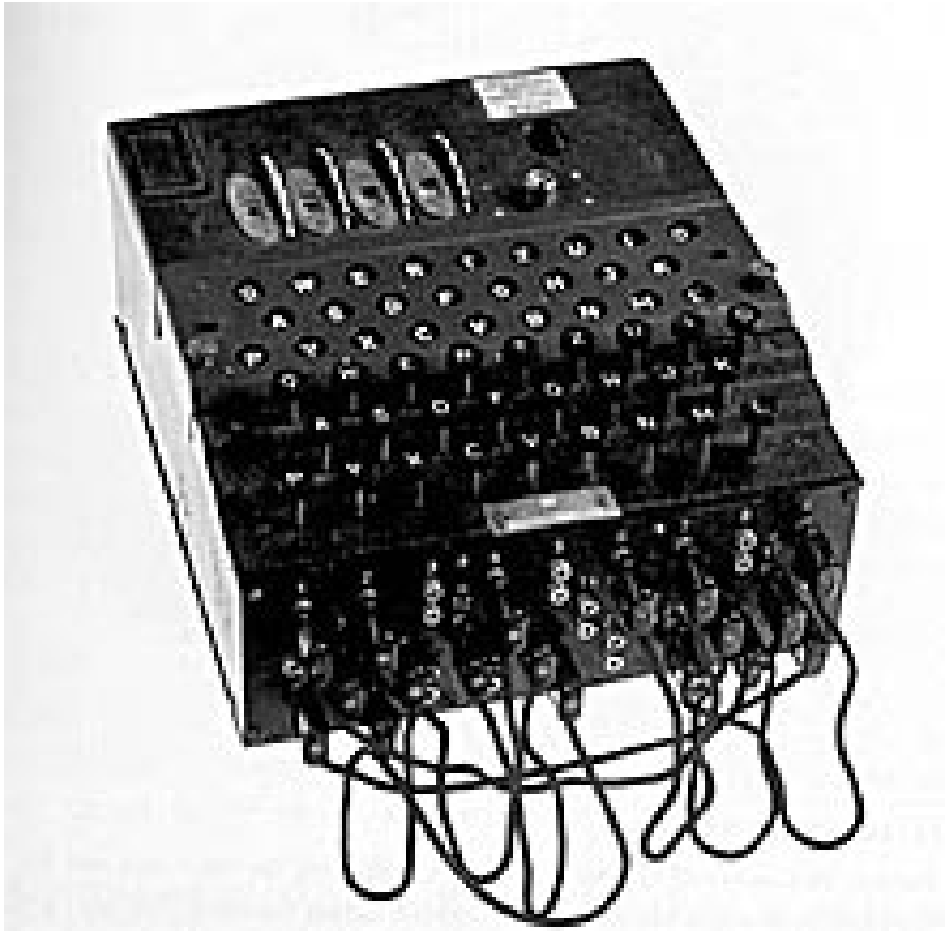
W U M O G I Z W Y R M H M C E S S V L P I S
C L L G U I L E Y M V N G E R Q L L G A I Q
G E Z K Z A L Q U T K T A Z E Y **H U W R L M**
Z W X C **H U W R L M** S Z L B S Q W C B M Z I
X C R F W W Y W O Q L A L Q A T Y Y Z X Z G
R P Q D A V Q B Z A L Q B T M J R Z L S R B
W O G Z U V Z E E Y J L O Y Q A E Y G T Q L
K I D M D R M E K L P R M M A G Y X I E S E
A T L K M M T Z N V Q V Z L X U A L J Z Q Z
L L R A B C M T B Q D M R A Q E S S U X P A
G M B T R V A V N F M E K L Z V U M C Y Q U
A P **A G T Q** G S S F Q D N E G Z L **A G T Q** T
M I F **M N M P Y** I W Y G U W E M P M **M N M P**
Y I W Y X M H K Y W H M R J M M X C G Q M K
S C W U I R G S D V Z M K Z Q T Q X M V E C
Y Z C Z K S Y C Z P I A O Y G M E B L L X Q
C Y S S Y W Y Y W O M

Ripetizioni e loro distanza nel crittogramma

Stringa ripetuta:	Distanza tra le ripetizioni:	Possibile lunghezza della chiave: (fattori della distanza)												
		2	3	4	5	6	7	8	9	10	11	12	13	14	15
HUWRLM	10	✓			✓					✓					
AGTQ	15		✓		✓										✓
MNMPYI	15		✓		✓										✓

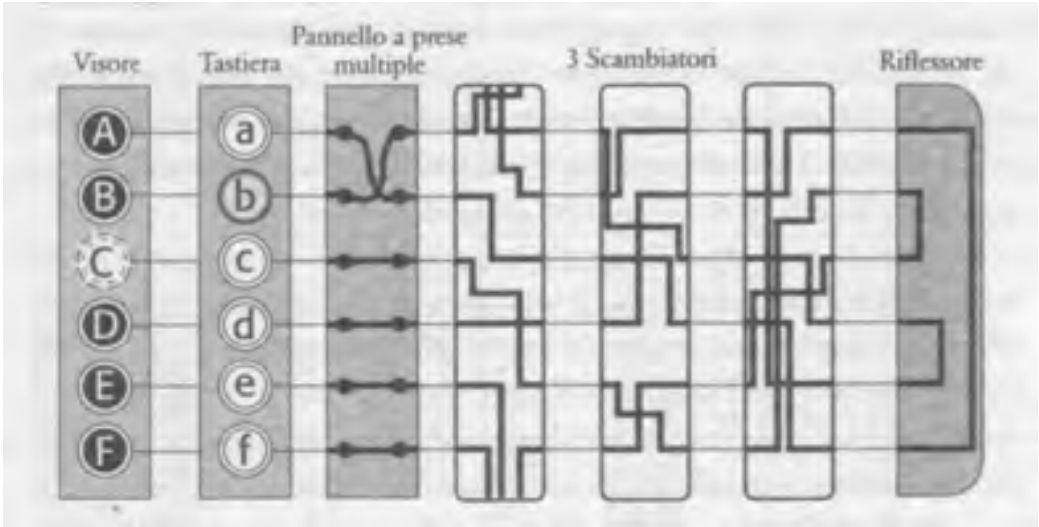
Enigma

Fu brevettata dall'ingegnere tedesco Arthur Scherbius nel 1918 ed adoperata dall'esercito e dalla marina tedesca durante la seconda guerra mondiale.



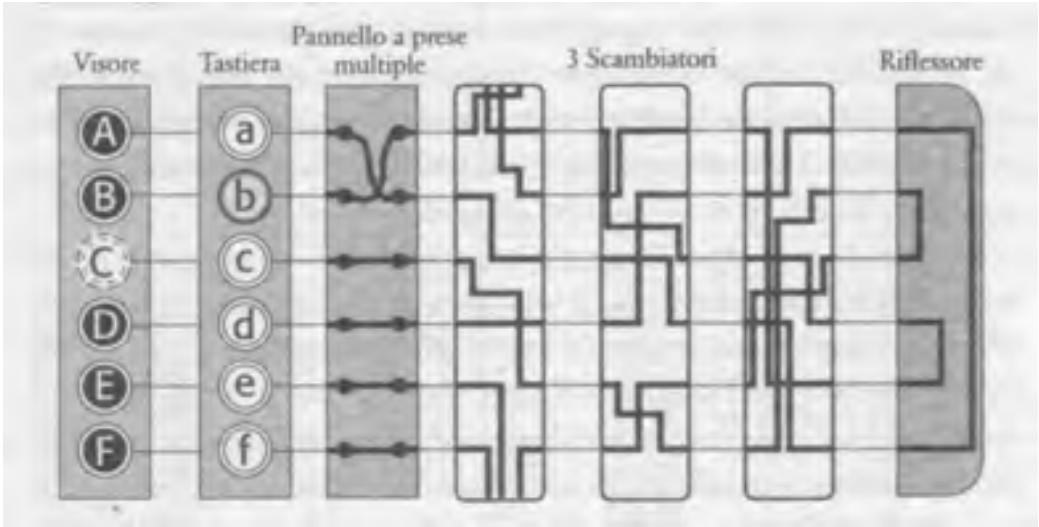
La macchina Enigma era costituita, in una delle versioni più complesse, da:

- una tastiera su cui digitare il testo del messaggio da cifrare;
- un pannello a prese multiple (6) che permetteva di scambiare coppie di lettere all'inizio della cifratura;
- 3 rotori (su alcune versioni 4 o anche più) su ognuno dei quali era incisa una permutazione dell'alfabeto (a volte i rotori a disposizione erano 5 e ne venivano scelti 3);
- un riflessore che "riflette" la lettera cifrata e la invia al visore;
- un visore che visualizza la lettera cifrata (tramite illuminazione del tasto corrispondente).



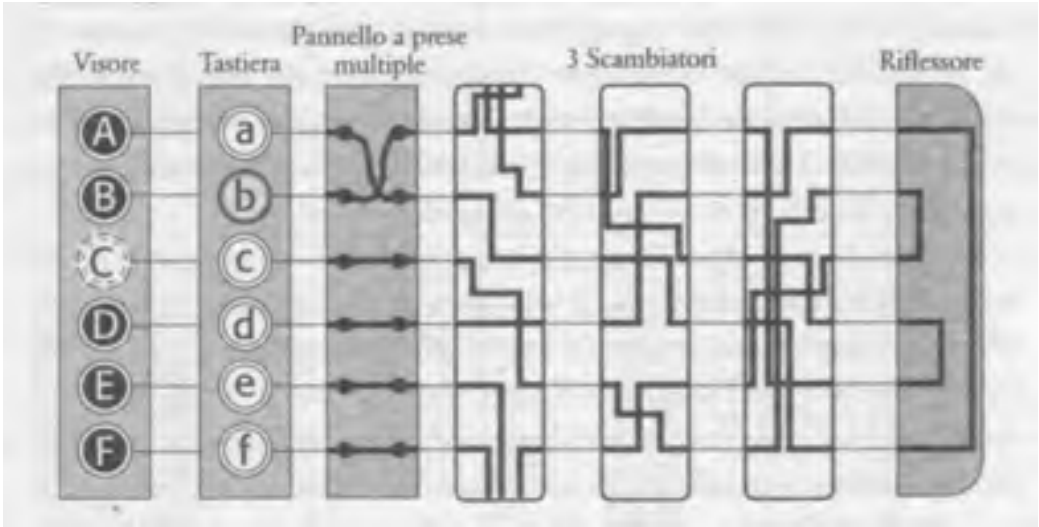
La macchina Enigma era costituita, in una delle versioni più complesse, da:

- una tastiera su cui digitare il testo del messaggio da cifrare;
- un pannello a prese multiple (6) che permetteva di scambiare coppie di lettere all'inizio della cifratura;
- 3 rotori (su alcune versioni 4 o anche più) su ognuno dei quali era incisa una permutazione dell'alfabeto (a volte i rotori a disposizione erano 5 e ne venivano scelti 3);
- un riflessore che "riflette" la lettera cifrata e la invia al visore;
- un visore che visualizza la lettera cifrata (tramite illuminazione del tasto corrispondente).



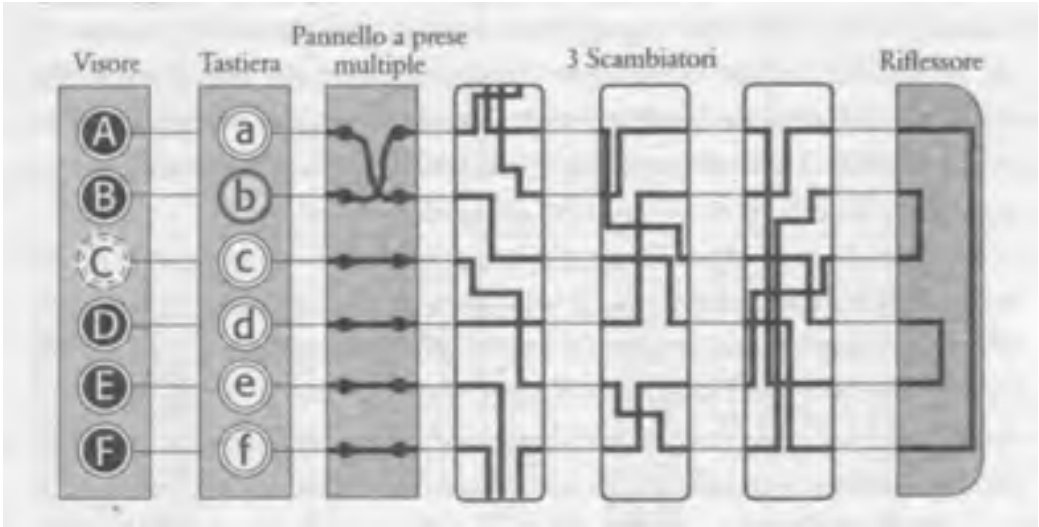
La macchina Enigma era costituita, in una delle versioni più complesse, da:

- una tastiera su cui digitare il testo del messaggio da cifrare;
- un pannello a prese multiple (6) che permetteva di scambiare coppie di lettere all'inizio della cifratura;
- 3 rotori (su alcune versioni 4 o anche più) su ognuno dei quali era incisa una permutazione dell'alfabeto (a volte i rotori a disposizione erano 5 e ne venivano scelti 3);
- un riflessore che "riflette" la lettera cifrata e la invia al visore;
- un visore che visualizza la lettera cifrata (tramite illuminazione del tasto corrispondente).



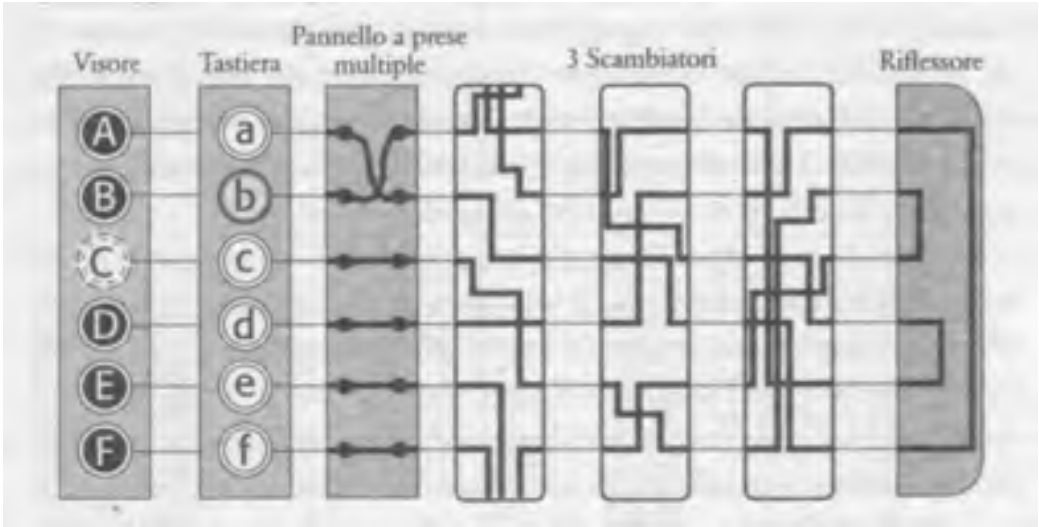
La macchina Enigma era costituita, in una delle versioni più complesse, da:

- una tastiera su cui digitare il testo del messaggio da cifrare;
- un pannello a prese multiple (6) che permetteva di scambiare coppie di lettere all'inizio della cifratura;
- 3 rotori (su alcune versioni 4 o anche più) su ognuno dei quali era incisa una permutazione dell'alfabeto (a volte i rotori a disposizione erano 5 e ne venivano scelti 3);
- un riflessore che "riflette" la lettera cifrata e la invia al visore;
- un visore che visualizza la lettera cifrata (tramite illuminazione del tasto corrispondente).



La macchina Enigma era costituita, in una delle versioni più complesse, da:

- una tastiera su cui digitare il testo del messaggio da cifrare;
- un pannello a prese multiple (6) che permetteva di scambiare coppie di lettere all'inizio della cifratura;
- 3 rotori (su alcune versioni 4 o anche più) su ognuno dei quali era incisa una permutazione dell'alfabeto (a volte i rotori a disposizione erano 5 e ne venivano scelti 3);
- un riflessore che "riflette" la lettera cifrata e la invia al visore;
- un visore che visualizza la lettera cifrata (tramite illuminazione del tasto corrispondente).



Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).

I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.

Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.

Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori per 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

Il punto di forza della macchina Enigma era la sua sicurezza dovuta all'elevato numero di chiavi di codifica (le configurazioni iniziali del pannello a prese multiple e dei rotori).
I tedeschi cambiavano le impostazioni iniziali della macchina periodicamente.
Il numero di possibili configurazioni iniziali su una macchina a 3 rotori tiene conto di:

- circa 10^{11} possibilità di scambiare coppie di lettere tramite il pannello a prese multiple (6);
- 26^3 possibili chiavi iniziali legate ai 3 rotori;
- 6 possibili disposizioni dei 3 rotori nei 3 alloggiamenti;

per un totale di circa 10^{16} configurazioni.
Solo conoscendo la configurazione del giorno e dispondendo di una macchina enigma si era in grado di decifrare i messaggi criptati.

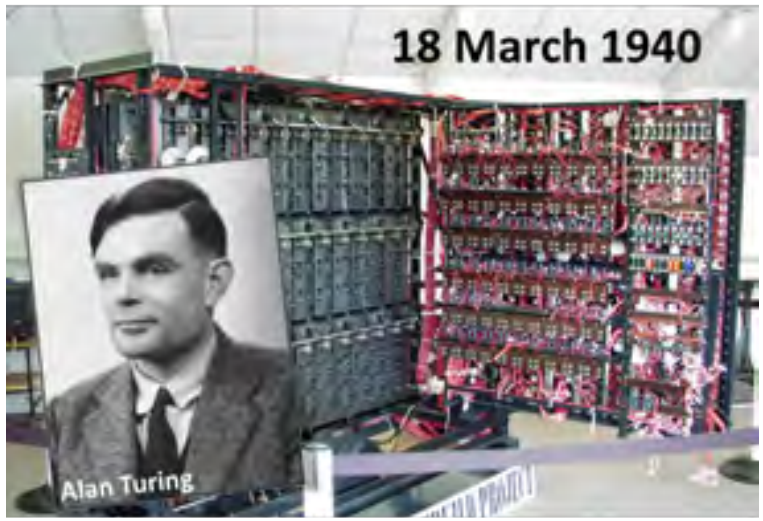
Alan Turing fa breccia in Enigma

Nel 1939 Bletchley Park (Londra) divenne il centro operativo del controspionaggio inglese.

Colui che coordinò il lavoro del team di matematici che si occupava di carpire i segreti della macchina Enigma fu Alan Turing.

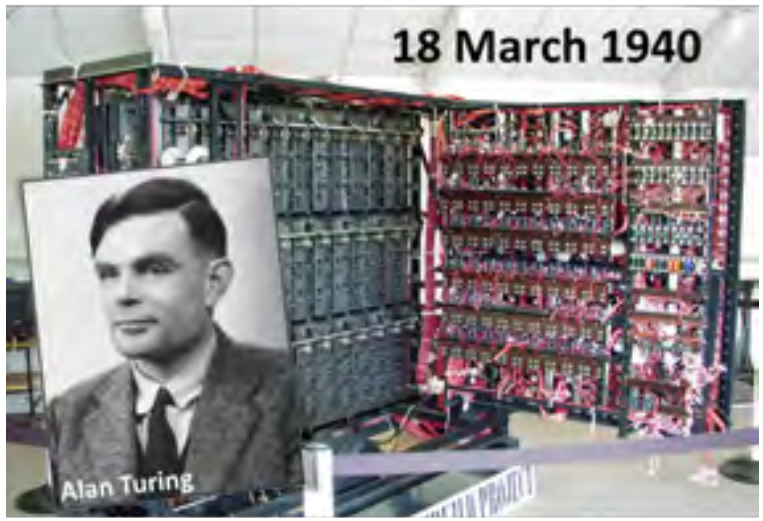
L'obiettivo del team era quello di indovinare la configurazione iniziale della macchina a seguito dell'analisi di messaggi intercettati.

Furono costruite le cosidette *bombe*, cioè delle macchine che simulavano elettromeccanicamente molti Enigma contemporaneamente.



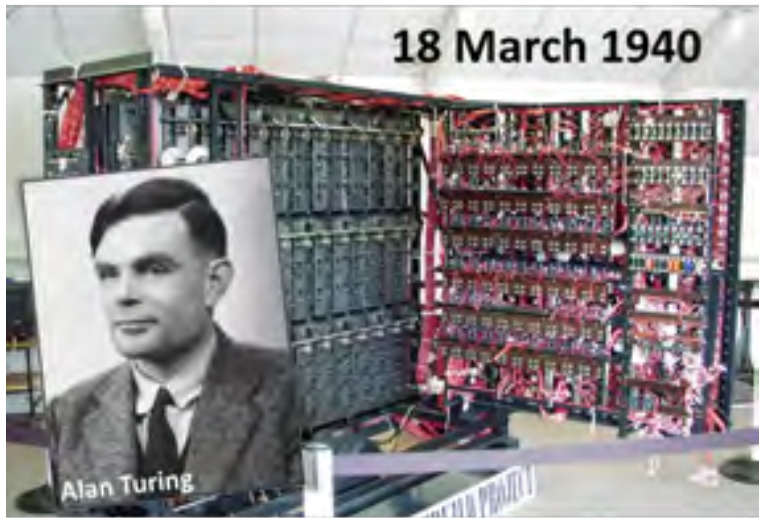
Alan Turing fa breccia in Enigma

Nel 1939 Bletchley Park (Londra) divenne il centro operativo del controspionaggio inglese.
Colui che coordinò il lavoro del team di matematici che si occupava di carpire i segreti della macchina Enigma fu Alan Turing.
L'obiettivo del team era quello di indovinare la configurazione iniziale della macchina a seguito dell'analisi di messaggi intercettati.
Furono costruite le cosidette *bombe*, cioè delle macchine che simulavano elettromeccanicamente molti Enigma contemporaneamente.



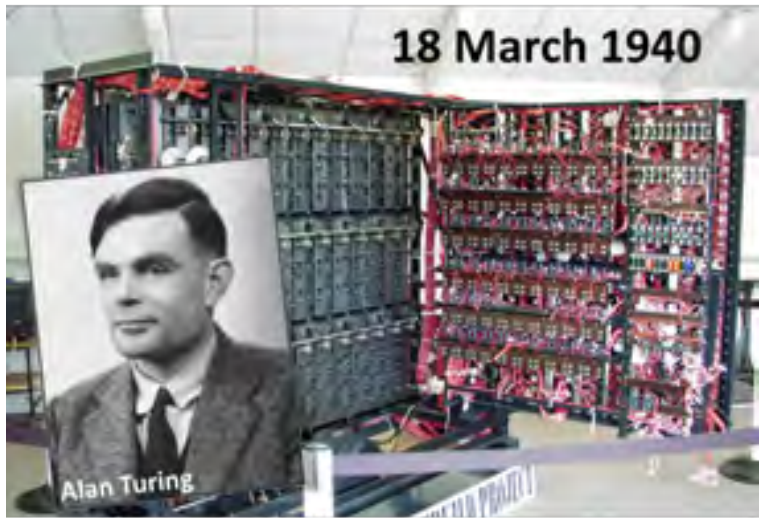
Alan Turing fa breccia in Enigma

Nel 1939 Bletchley Park (Londra) divenne il centro operativo del controspionaggio inglese.
Colui che coordinò il lavoro del team di matematici che si occupava di carpire i segreti della macchina Enigma fu Alan Turing.
L'obiettivo del team era quello di indovinare la configurazione iniziale della macchina a seguito dell'analisi di messaggi intercettati.
Furono costruite le cosidette *bombe*, cioè delle macchine che simulavano elettromeccanicamente molti Enigma contemporaneamente.



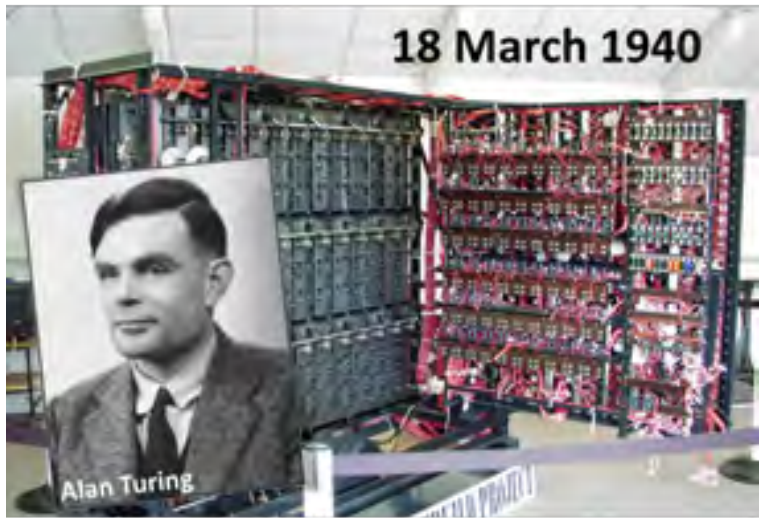
Alan Turing fa breccia in Enigma

Nel 1939 Bletchley Park (Londra) divenne il centro operativo del controspionaggio inglese.
Colui che coordinò il lavoro del team di matematici che si occupava di carpire i segreti della macchina Enigma fu Alan Turing.
L'obiettivo del team era quello di indovinare la configurazione iniziale della macchina a seguito dell'analisi di messaggi intercettati.
Furono costruite le cosidette *bombe*, cioè delle macchine che simulavano elettromeccanicamente molti Enigma contemporaneamente.



Alan Turing fa breccia in Enigma

Nel 1939 Bletchley Park (Londra) divenne il centro operativo del controspionaggio inglese.
Colui che coordinò il lavoro del team di matematici che si occupava di carpire i segreti della macchina Enigma fu Alan Turing.
L'obiettivo del team era quello di indovinare la configurazione iniziale della macchina a seguito dell'analisi di messaggi intercettati.
Furono costruite le cosidette *bombe*, cioè delle macchine che simulavano elettromeccanicamente molti Enigma contemporaneamente.



Il matematico polacco Rejewski e altri collaboratori, realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri di configurazione.

Alla fine degli anni '30 le comunicarono agli inglesi.

Turing mise insieme queste informazioni più altre che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e se ne servìi per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare anche "shark", l'ENIGMA a 4 rotori usato dai sommergibili.

ALAN TURING è considerato il padre dell'informatica e, cosa più importante, è stato fondamentale nella vittoria per gli alleati nella seconda guerra mondiale che ha permesso l'attuale civiltà.

Il matematico polacco Rejewski e altri collaboratori, realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri di configurazione.
Alla fine degli anni '30 le comunicarono agli inglesi.
Turing mise insieme queste informazioni più altre che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e se ne servìi per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare anche "shark", l'ENIGMA a 4 rotori usato dai sommergibili.

ALAN TURING è considerato il padre dell'informatica e, cosa più importante, è stato fondamentale nella vittoria per gli alleati nella seconda guerra mondiale che ha permesso l'attuale civiltà.

Il matematico polacco Rejewski e altri collaboratori, realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri di configurazione.
Alla fine degli anni '30 le comunicarono agli inglesi.
Turing mise insieme queste informazioni più altre che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e se ne servìi per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare anche "shark", l'ENIGMA a 4 rotori usato dai sommergibili.

ALAN TURING è considerato il padre dell'informatica e, cosa più importante, è stato fondamentale nella vittoria per gli alleati nella seconda guerra mondiale che ha permesso l'attuale civiltà.

Il matematico polacco Rejewski e altri collaboratori, realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri di configurazione.
Alla fine degli anni '30 le comunicarono agli inglesi.
Turing mise insieme queste informazioni più altre che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e se ne servìi per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare anche "shark", l'ENIGMA a 4 rotori usato dai sommergibili.

ALAN TURING è considerato il padre dell'informatica e, cosa più importante, è stato fondamentale nella vittoria per gli alleati nella seconda guerra mondiale che ha permesso l'attuale civiltà.

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1946): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di trasmissione e il linguaggio FORTRAN;
- nel 1958 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1946): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di trasmissione in linguaggio FORTRAN;
- nel 1958 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Automazione della crittografia

Nascita primi calcolatori elettronici:

- bombe di Turing;
- Colossus (usato per debellare la cifratura di Lorenz);
- ENIAC (1945): conteneva 18000 valvole ed effettuava fino a 5000 calcoli al secondo;
- la IBM lancia il suo primo elaboratore (1953) dotato di transistor e il linguaggio FORTRAN;
- nel 1959 fu inventato il circuito integrato.

La cifratura richiedeva la conversione del testo in numeri. Fu usato il codice ASCII per la conversione in codice binario (sequenze di 0 e 1 (bit)).

Codice ASCII binario per lettere maiuscole

A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111
F	1000101	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Parola da cifrare: MONTE $\longrightarrow$

1001101 – 1001111 – 1001110 – 1010100 – 1000101

Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111

Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.

L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$

1001101 – 1001111 – 1001110 – 1010100 – 1000101

Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111

Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.

L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Parola da cifrare: MONTE $\longrightarrow$
1001101 – 1001111 – 1001110 – 1010100 – 1000101
Chiave: NERO $\longrightarrow$ 1001110 – 1000101 – 1010010 – 1001111
Per cifrare si "somma" ogni elemento del testo chiaro al corrispondente elemento della chiave.
L'addizione segue le regole:

- se gli elementi del testo chiaro e della chiave sono uguali, nel testo cifrato si scrive 0;
- se gli elementi del testo chiaro e della chiave sono diversi, nel testo cifrato si scrive 1;

Testo chiaro	1001101	1001111	1001110	1010100	1000101
Chiave	1001110	1000101	1010010	1001111	1001110
Testo cifrato	0000011	0001010	0011100	0011011	0001011

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Il sistema di cifratura Lucifer (ideato da Horst Feistel)

- La stringa è divisa in blocchi da 64 bit crittati separatamente;
- si mescolano i 64 bit del blocco;
- si divide in due blocchi da 32 bit: SINISTRA^0 e DESTRA^0;
- i bit di DESTRA^0 vengono trasformati tramite una funzione "deformante" che esegue un complesso procedimento di sostituzione tramite una chiave;
- i bit DESTRA^0 deformati si sommano ai bit SINISTRA^0 e generano il blocco da 32 bit DESTRA^1;
- l'originale DESTRA^0 è rinominato SINISTRA^1;
- si ripete l'operazione con i blocchi DESTRA^1 e SINISTRA^1;
- complessivamente si compiono 16 "giri".

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi ragionevoli)?
- tramite servizio postale?
- brevi manu?

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi recenti)?
- tramite servizio postale?
- brevi mani?

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi ressa)?
- tramite servizio postale?
- brevi manu?

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi ressa)?
- tramite servizio postale?
- brevi manu?

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi recenti)?
- tramite servizio postale?
- brevi incontri?

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi recenti)?
- tramite servizio postale?
- *brevi manu?*

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi recenti)?
- tramite servizio postale?
- *brevi manu?*

Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi recenti)?
- tramite servizio postale?
- *brevi manu?*

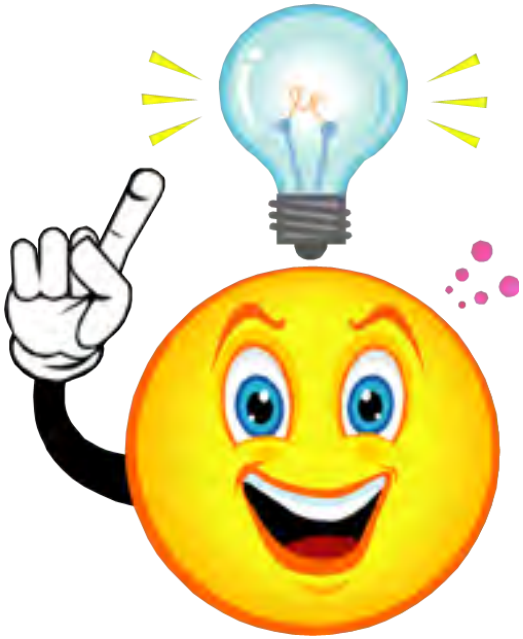
Nel 1976 fu adottata dalla NSA (National Security Agency) la versione a 56 bit di Lucifer (meno dispendiosa in termini di calcoli) e prese il nome di **DES** (Data Encryption Standard).

Il DES divenne lo standard di cifratura di informazioni riservate.

MITTENTE $\longrightarrow$ cifra il messaggio;
DESTINATARIO $\longrightarrow$ riceve il messaggio cifrato e la chiave di decrittazione.

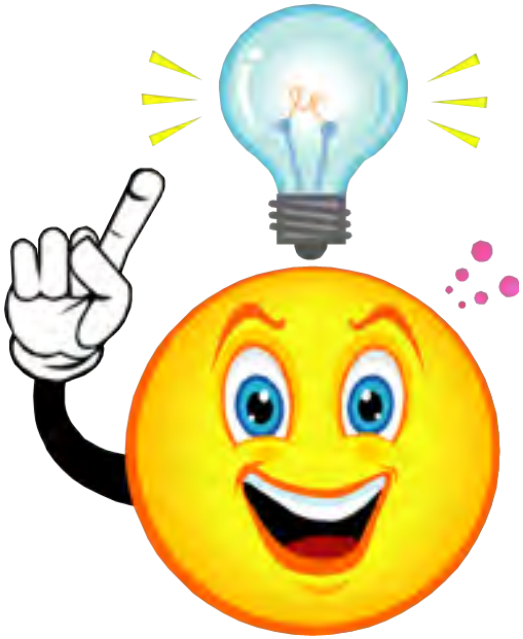
PROBLEMA: distribuzione delle chiavi

- via telefono?
- via mail (in tempi recenti)?
- tramite servizio postale?
- *brevi manu*?



Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.
Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.
Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



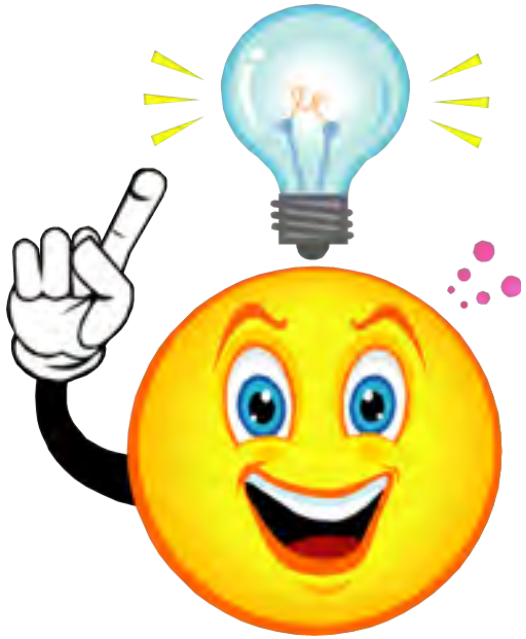
Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.

Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.

Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.

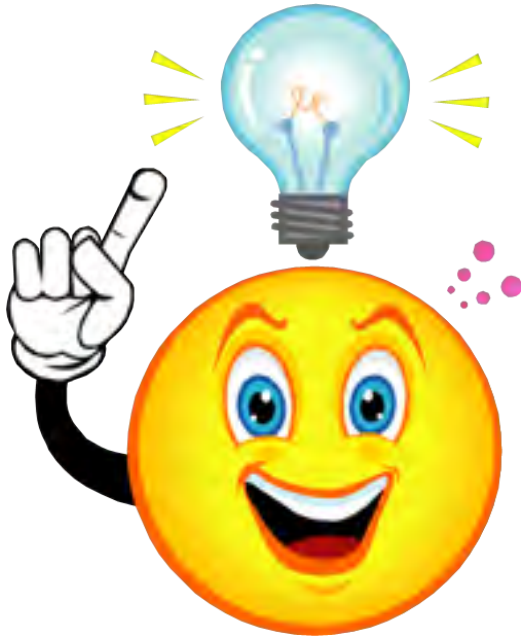
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.
Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.
Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



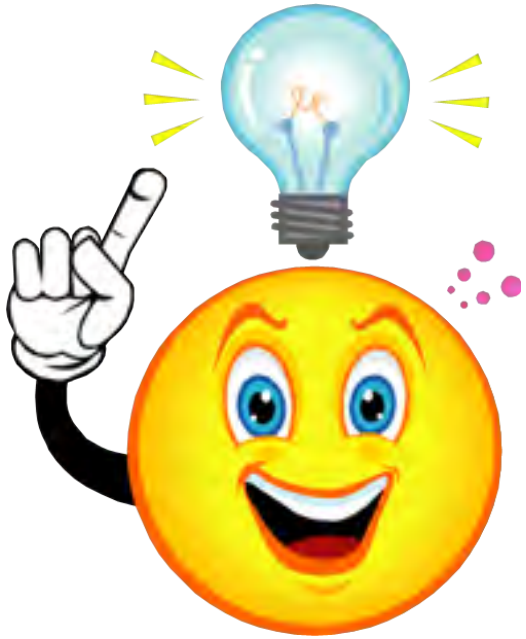
Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.

Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.

Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.

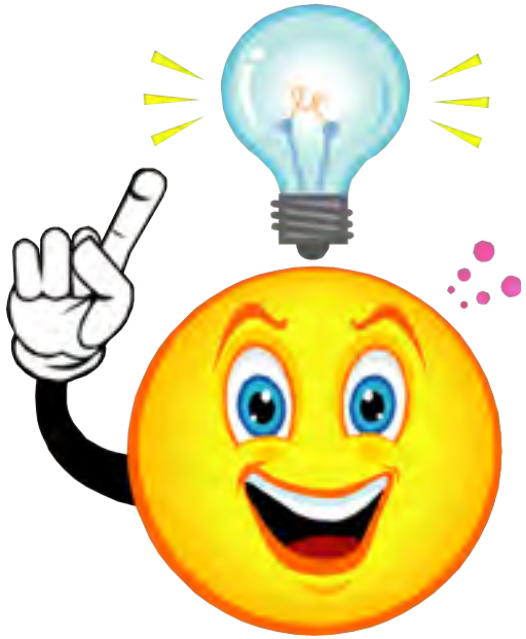
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



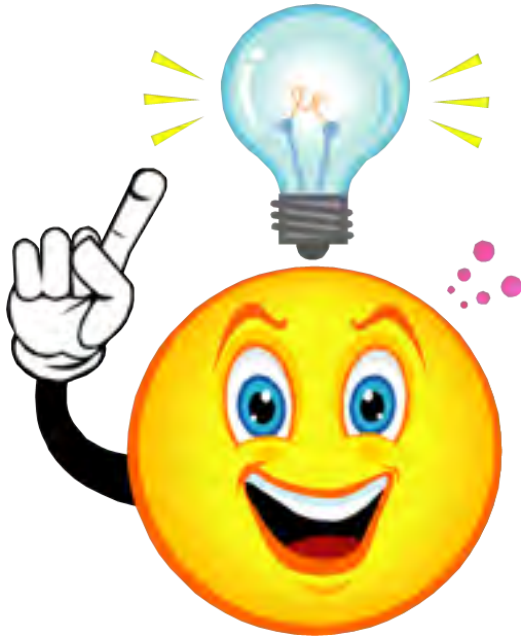
Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.
Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.
Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



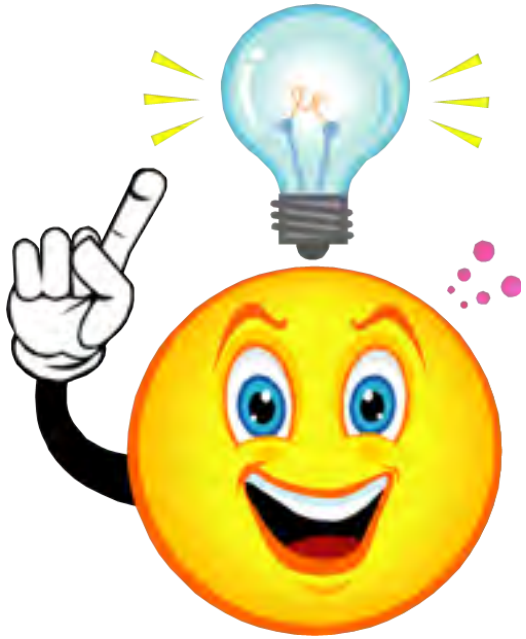
Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.
Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.
Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.
Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.
Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!



Immaginiamo che Alice voglia inviare un messaggio molto personale a Bob. Lo colloca così in una scatola con un lucchetto e lo spedisce a Bob tenendo la chiave.
Ricevuta la scatola, Bob le applica un secondo lucchetto e tiene la chiave del secondo lucchetto, rispedendola ad Alice.
Ricevuta la scatola, Alice toglie il proprio lucchetto e la rispedisce a Bob.
A questo punto Bob toglie il proprio lucchetto, apre la scatola e legge il messaggio.

Per leggere il messaggio non è stato necessario recapitare la chiave!!


Whitfield Diffie
Martin Hellman

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).

Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod{P}$$

dove P è un numero primo e Y è un intero positivo minore di P.

Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^A \pmod{P}$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^B \pmod{P}$, cioè $11^9 \pmod{17}$ ottenendo 7;
- Bob comunica ad Alice il numero 7;
- Alice calcola $7^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod{P}$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^A \pmod{P}$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^B \pmod{P}$, cioè $11^9 \pmod{17}$ ottenendo 12;
- Bob comunica ad Alice il numero 8;
- Alice calcola $8^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod{P}$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^A \pmod{P}$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^B \pmod{P}$, cioè $11^9 \pmod{17}$ ottenendo 7;
- Bob comunica ad Alice il numero 7;
- Alice calcola $7^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod{P}$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod{P}$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod{P}$, cioè $11^9 \pmod{17}$ ottenendo 12;
- Bob comunica ad Alice il numero 12;
- Alice calcola $12^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Diffie ed Hellman idearono un metodo per stabilire la chiave che fa uso dell'aritmetica modulare (o dell'orologio).
Si basa sull'utilizzo della funzione unidirezionale

$$Y^x \pmod P$$

dove P è un numero primo e Y è un intero positivo minore di P.
Alice e Bob seguono la procedura seguente:

- concordano i valori di Y e P: ad esempio $Y = 11$ e $P = 17$;
- Alice sceglie un numero A, ad esempio 3, e calcola $Y^3 \pmod P$, cioè $11^3 \pmod{17}$ ottenendo 5;
- Alice comunica a Bob il numero 5 (anche telefonicamente);
- Bob sceglie un numero B, ad esempio 9, e calcola $Y^9 \pmod P$, cioè $11^9 \pmod{17}$ ottenendo 6;
- Bob comunica ad Alice il numero 6;
- Alice calcola $6^A \pmod{17}$ e Bob calcola $5^B \pmod{17}$;
- ottengono entrambi 12.

La chiave che Alice e Bob useranno per scambiarsi i messaggi è: 12.

Crittografia RSA

E' un tipo di crittografia a ***chiave pubblica asimmetrica***, cioè la chiave (pubblica) per codificare il messaggio è diversa dalla chiave (privata) per decodificarlo. E' stato ideato da tre ricercatori del MIT (Massachusetts Institute of Technology): Ron Rivest, Adi Shamir, Leonard Adleman.

E' basato sull'impossibilità di fattorizzare in tempi brevi un intero avente un numero di cifre dell'ordine di 2-3 centinaia.

Crittografia RSA

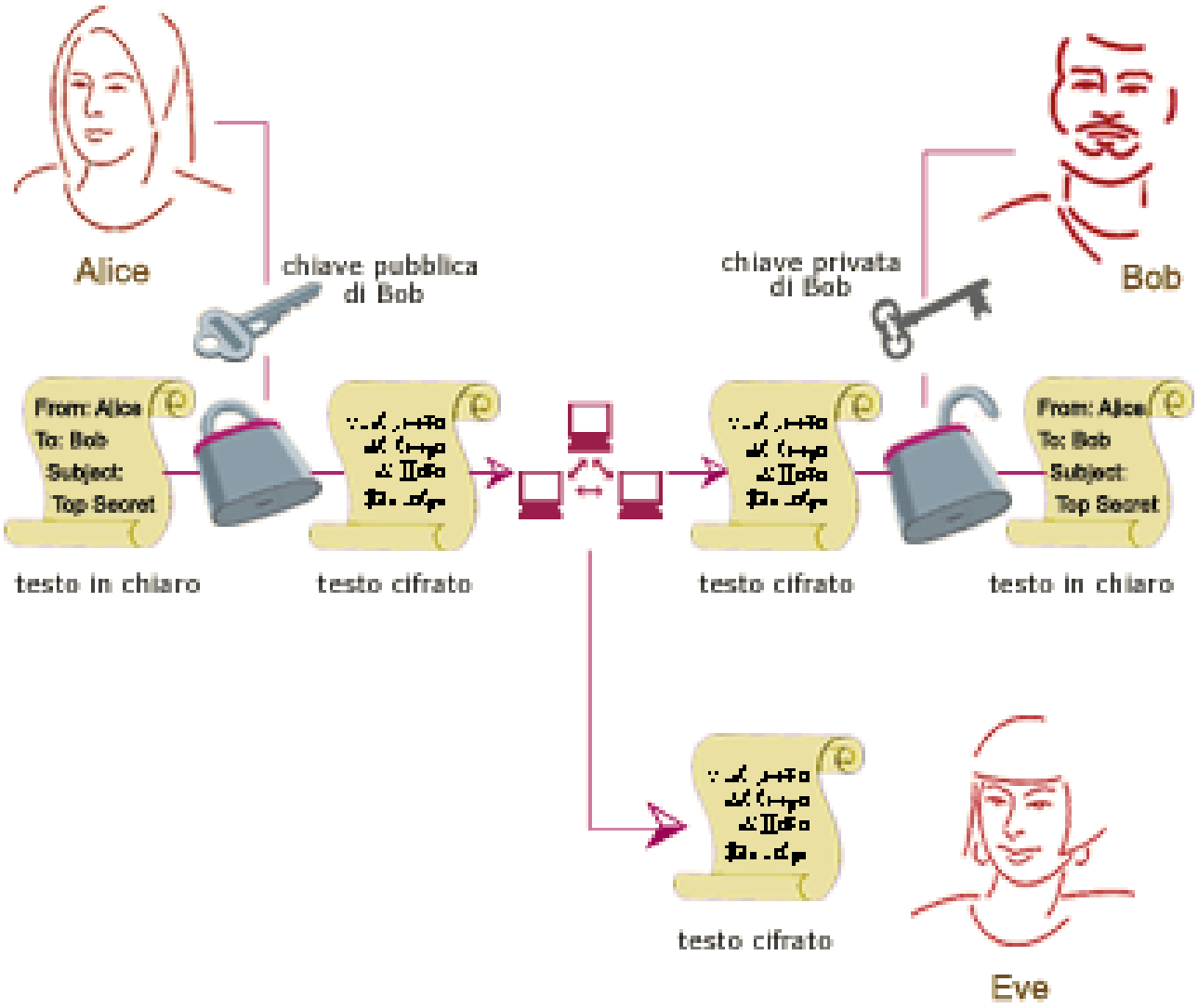
E' un tipo di crittografia a ***chiave pubblica asimmetrica***, cioè la chiave (pubblica) per codificare il messaggio è diversa dalla chiave (privata) per decodificarlo.E' stato ideato da tre ricercatori del MIT (Massachusetts Institute of Technology): Ron Rivest, Adi Shamir, Leonard Adleman.

E' basato sull'impossibilità di fattorizzare in tempi brevi un intero avente un numero di cifre dell'ordine di 2-3 centinaia.

Crittografia RSA

E' un tipo di crittografia a ***chiave pubblica asimmetrica***, cioè la chiave (pubblica) per codificare il messaggio è diversa dalla chiave (privata) per decodificarlo.E' stato ideato da tre ricercatori del MIT (Massachusetts Institute of Technology): Ron Rivest, Adi Shamir, Leonard Adleman.

E' basato sull'impossibilità di fattorizzare in tempi brevi un intero avente un numero di cifre dell'ordine di 2-3 centinaia.


Alice
chiave pubblica di Bob
chiave privata di Bob
Bob
From: Alice
To: Bob
Subject:
Top Secret
testo in chiaro
testo cifrato
testo cifrato
From: Alice
To: Bob
Subject:
Top Secret
testo in chiaro
testo cifrato
Eve

Ogni utente possiede una *chiave pubblica* accessibile a tutti e una *chiave privata* di sua esclusiva conoscenza.

La chiave pubblica serve per codificare il messaggio.

La chiave privata serve per decodificare il messaggio cifrato.

Chiavi pubblica e privata sono coppie di numeri che verificano certe condizioni.

Simuliamo uno scambio di messaggi tra i due utenti, Alice e Bob. In particolare è Alice a voler inviare un messaggio segreto a Bob.

Ad Alice serve la chiave pubblica di Bob

Ogni utente possiede una *chiave pubblica* accessibile a tutti e una *chiave privata* di sua esclusiva conoscenza.
La chiave pubblica serve per codificare il messaggio.
La chiave privata serve per decodificare il messaggio cifrato.
Chiavi pubblica e privata sono coppie di numeri che verificano certe condizioni.

Simuliamo uno scambio di messaggi tra i due utenti, Alice e Bob. In particolare è Alice a voler inviare un messaggio segreto a Bob.

Ad Alice serve la chiave pubblica di Bob

Ogni utente possiede una *chiave pubblica* accessibile a tutti e una *chiave privata* di sua esclusiva conoscenza.
La chiave pubblica serve per codificare il messaggio.
La chiave privata serve per decodificare il messaggio cifrato.
Chiavi pubblica e privata sono coppie di numeri che verificano certe condizioni.

Simuliamo uno scambio di messaggi tra i due utenti, Alice e Bob. In particolare è Alice a voler inviare un messaggio segreto a Bob.

Ad Alice serve la chiave pubblica di Bob

Ogni utente possiede una *chiave pubblica* accessibile a tutti e una *chiave privata* di sua esclusiva conoscenza.
La chiave pubblica serve per codificare il messaggio.
La chiave privata serve per decodificare il messaggio cifrato.
Chiavi pubblica e privata sono coppie di numeri che verificano certe condizioni.

Simuliamo uno scambio di messaggi tra i due utenti, Alice e Bob. In particolare è Alice a voler inviare un messaggio segreto a Bob.

Ad Alice serve la chiave pubblica di Bob

Ogni utente possiede una *chiave pubblica* accessibile a tutti e una *chiave privata* di sua esclusiva conoscenza.
La chiave pubblica serve per codificare il messaggio.
La chiave privata serve per decodificare il messaggio cifrato.
Chiavi pubblica e privata sono coppie di numeri che verificano certe condizioni.

Simuliamo uno scambio di messaggi tra i due utenti, Alice e Bob. In particolare è Alice a voler inviare un messaggio segreto a Bob.

Ad Alice serve la chiave pubblica di Bob

Ogni utente possiede una *chiave pubblica* accessibile a tutti e una *chiave privata* di sua esclusiva conoscenza.
La chiave pubblica serve per codificare il messaggio.
La chiave privata serve per decodificare il messaggio cifrato.
Chiavi pubblica e privata sono coppie di numeri che verificano certe condizioni.

Simuliamo uno scambio di messaggi tra i due utenti, Alice e Bob. In particolare è Alice a voler inviare un messaggio segreto a Bob.

Ad Alice serve la chiave pubblica di Bob

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

- a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
- b non deve avere fattori in comune con $p-1$ e $q-1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

1. a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
2. b non deve avere fattori in comune con $p-1$ e $q-1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

1. a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
2. b non deve avere fattori in comune con $p - 1$ e $q - 1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

1. a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
2. b non deve avere fattori in comune con $p - 1$ e $q - 1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

1. a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
2. b non deve avere fattori in comune con $p - 1$ e $q - 1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

1. a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
2. b non deve avere fattori in comune con $p - 1$ e $q - 1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

La chiave pubblica di Bob è una coppia di numeri interi (a, b) verificanti le seguenti condizioni:

1. a deve essere il prodotto di due numeri primi molto grandi e non vicini tra loro (almeno 300 cifre ciascuno): p e q;
2. b non deve avere fattori in comune con $p - 1$ e $q - 1$.

A titolo di esempio, possiamo scegliere per Bob, $p = 19$ e $q = 23$. In questo modo: $a = 19 \cdot 23 = 437$ e come valore di b si può prendere $b = 35$ (35 non ha fattori in comune né con 18 né con 22).

La chiave pubblica di Bob è quindi $(437, 35)$.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

- eleva 67 al numero $b = 35$: 67^{35};
- calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).

Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

1. eleva 67 al numero $b = 35$: 67^{35};
2. calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

1. eleva 67 al numero $b = 35$: 67^{35};
2. calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

- eleva 67 al numero $b = 35$: 67^{35};
- calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

1. eleva 67 al numero $b = 35$: 67^{35};
2. calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

1. eleva 67 al numero $b = 35$: 67^{35};
2. calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

1. eleva 67 al numero $b = 35$: 67^{35};
2. calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Alice vuol inviare un messaggio cifrato a Bob. Per farlo deve prima tradurlo in una stringa numerica n il cui valore è minore di a (eventualmente può spezzare il messaggio in più messaggi).
Supponiamo che l'alfabeto a disposizione di Alice sia il seguente:

A	C	D	E	I	L	P	R	T
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9

Se volesse inviare il messaggio LP, dovrebbe tradurlo nella stringa $n = 67$.
A questo punto Alice cifra il messaggio nel modo seguente:

1. eleva 67 al numero $b = 35$: 67^{35};
2. calcola il resto della divisione di 67^{35} per $a = 437$.

Ottiene quindi il numero $m = 249$, che è il messaggio cifrato, e lo invia a Bob.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.

Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

a) eleva $m = 249$ al numero $d = 215$: 249^{215};

b) calcola il resto della divisione di 249^{215} per $p \cdot q = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $p \cdot q = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $p \cdot q = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $a = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $a = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $a = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di $K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $a = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

Bob deve quindi decifrare il messaggio che Alice gli ha inviato.
Per far questo deve usare la propria chiave privata, cioè la coppia di numeri (a, d), dove d è l'unico numero minore di
$K = (p-1)(q-1) = 18 \cdot 22 = 396$ verificante la condizione seguente:

$$b \cdot d \text{ dà resto 1 se diviso per } K = 396.$$

Nel caso di Bob si ottiene $d = 215$ (infatti $35 \cdot 215$ dà resto 1 se diviso per 396).

La chiave privata di Bob è quindi $(437, 215)$.

Infine Bob, per decifrare il messaggio $m = 249$ di Alice, procede nel modo seguente:

1. eleva $m = 249$ al numero $d = 215$: 249^{215};
2. calcola il resto della divisione di 249^{215} per $a = 437$.

Ottiene così il numero 67 che corrisponde al messaggio LP.

La conoscenza dei due fattori primi di a, cioè p e q, consentirebbe ad un malintenzionato di procurarsi la chiave privata di Bob e decifrare tutti i messaggi che egli riceve.

La sicurezza del sistema RSA risiede nell'impossibilità, a tutt'oggi, di conoscere in tempi brevi la fattorizzazione di a.

"La sicurezza della cifratura RSA dipende dalla nostra incapacità di rispondere a questioni fondamentali sui numeri primi. Siamo in grado di capire una metà dell'equazione ma non l'altra. Quanto più penetriamo nel mistero dei numeri primi, tuttavia, tanto meno sicuri diventano i codici usati in Internet. I numeri primi sono le chiavi delle serrature che proteggono i sistemi elettronici del mondo. Ciò che si riuscirà a scoprire potrebbe servire a violare quei codici." (cit. Marcus du Sautoy, "L'enigma dei numeri primi").

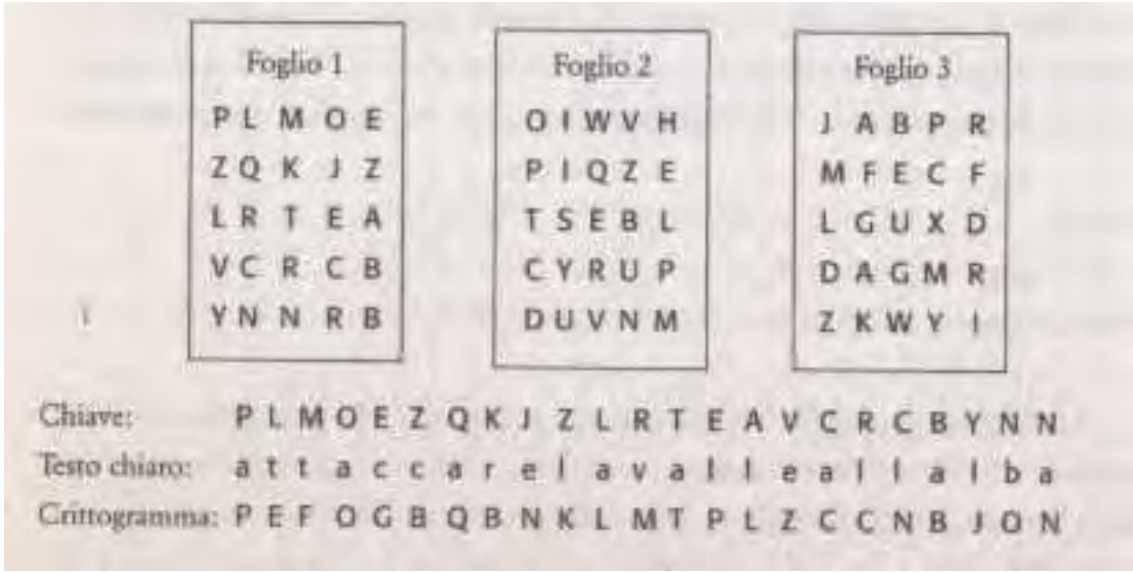
La conoscenza dei due fattori primi di a, cioè p e q, consentirebbe ad un malintenzionato di procurarsi la chiave privata di Bob e decifrare tutti i messaggi che egli riceve.
La sicurezza del sistema RSA risiede nell'impossibilità, a tutt'oggi, di conoscere in tempi brevi la fattorizzazione di a.

"La sicurezza della cifratura RSA dipende dalla nostra incapacità di rispondere a questioni fondamentali sui numeri primi. Siamo in grado di capire una metà dell'equazione ma non l'altra. Quanto più penetriamo nel mistero dei numeri primi, tuttavia, tanto meno sicuri diventano i codici usati in Internet. I numeri primi sono le chiavi delle serrature che proteggono i sistemi elettronici del mondo. Ciò che si riuscirà a scoprire potrebbe servire a violare quei codici." (cit. Marcus du Sautoy, "L'enigma dei numeri primi").

La conoscenza dei due fattori primi di a, cioè p e q, consentirebbe ad un malintenzionato di procurarsi la chiave privata di Bob e decifrare tutti i messaggi che egli riceve.
La sicurezza del sistema RSA risiede nell'impossibilità, a tutt'oggi, di conoscere in tempi brevi la fattorizzazione di a.

"La sicurezza della cifratura RSA dipende dalla nostra incapacità di rispondere a questioni fondamentali sui numeri primi. Siamo in grado di capire una metà dell'equazione ma non l'altra. Quanto più penetriamo nel mistero dei numeri primi, tuttavia, tanto meno sicuri diventano i codici usati in Internet. I numeri primi sono le chiavi delle serrature che proteggono i sistemi elettronici del mondo. Ciò che si riuscirà a scoprire potrebbe servire a violare quei codici." (cit. Marcus du Sautoy, "L'enigma dei numeri primi").

Il Santo Graal della crittografia



Foglio 1				
P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Foglio 2				
O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

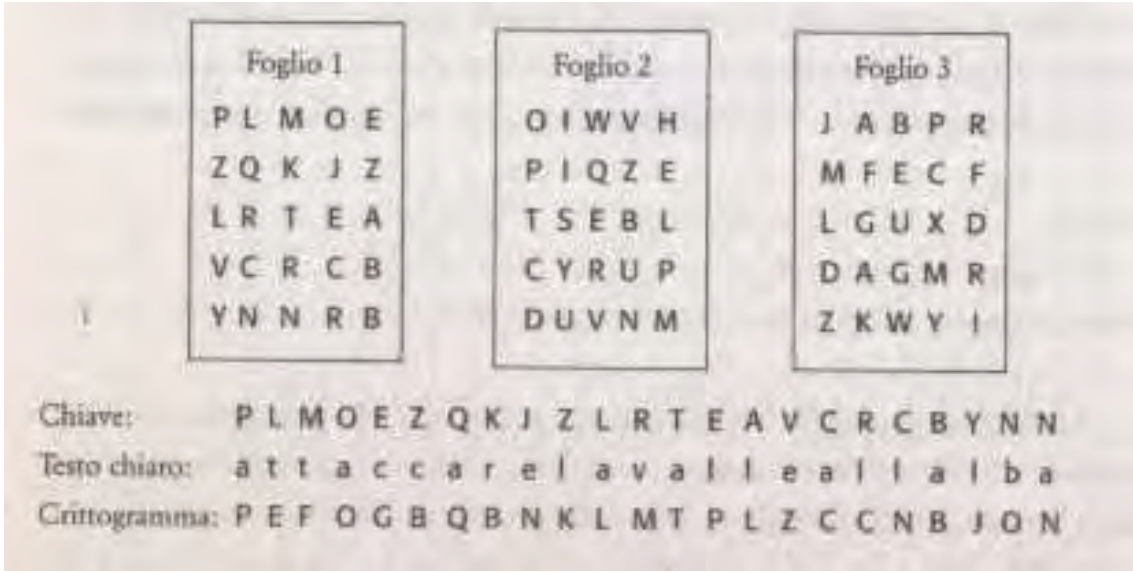
Foglio 3				
J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

Chiave:	P	L	M	O	E	Z	Q	K	J	Z	L	R	T	E	A	V	C	R	C	B	Y	N	N
Testo chiaro:	a	t	t	a	c	c	a	r	e	l	a	v	a	l	l	e	a	l	l	a	l	b	a
Crittogramma:	P	E	F	O	G	B	Q	B	N	K	L	M	T	P	L	Z	C	C	N	B	J	O	N

Il sistema di cifratura a blocchi monouso (*one-time pad cipher*) è inviolabile!
Non è utilizzato (se non da potenti come i presidenti americano e russo) perché:

- è "complicato" produrre un numero molto grande di chiavi casuali in termini di tempo, fatica e denaro;
- è "complicato" distribuire le chiavi casuali.

Il Santo Graal della crittografia



Foglio 1				
P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Foglio 2				
O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

Foglio 3				
J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

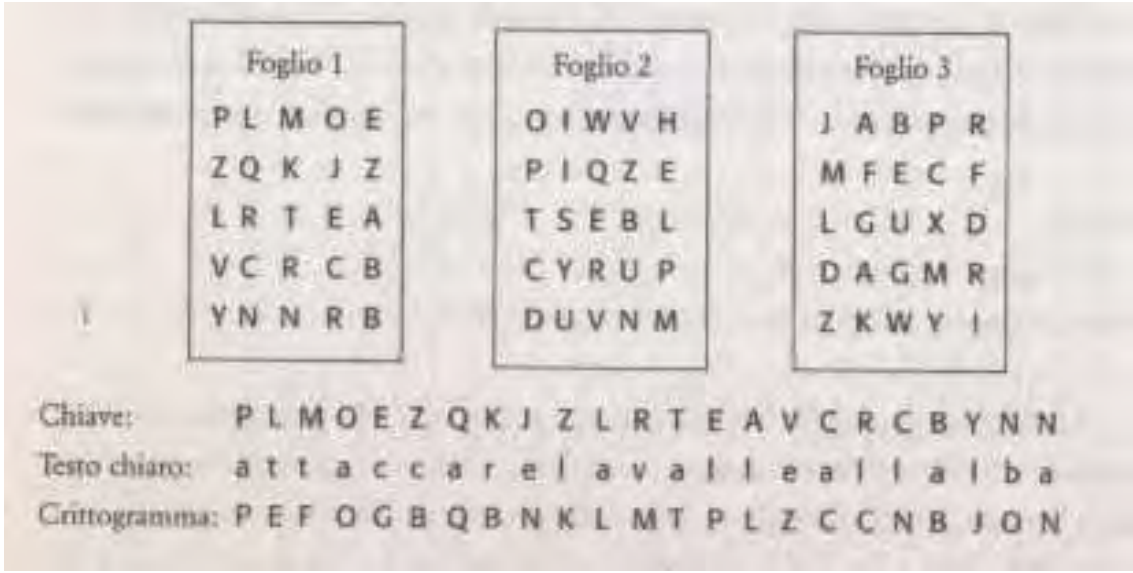
Chiave:	P	L	M	O	E	Z	Q	K	J	Z	L	R	T	E	A	V	C	R	C	B	Y	N	N
Testo chiaro:	a	t	t	a	c	c	a	r	e	l	a	v	a	l	l	e	a	l	l	a	l	b	a
Crittogramma:	P	E	F	O	G	B	Q	B	N	K	L	M	T	P	L	Z	C	C	N	B	J	O	N

Il sistema di cifratura a blocchi monouso (*one-time pad cipher*) è inviolabile!

Non è utilizzato (se non da potenti come i presidenti americano e russo) perché:

- è "complicato" produrre un numero molto elevato di chiavi casuali in termini di tempo, fatica e denaro;
- è "complicato" distribuire le chiavi casuali.

Il Santo Graal della crittografia



Foglio 1				
P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Foglio 2				
O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

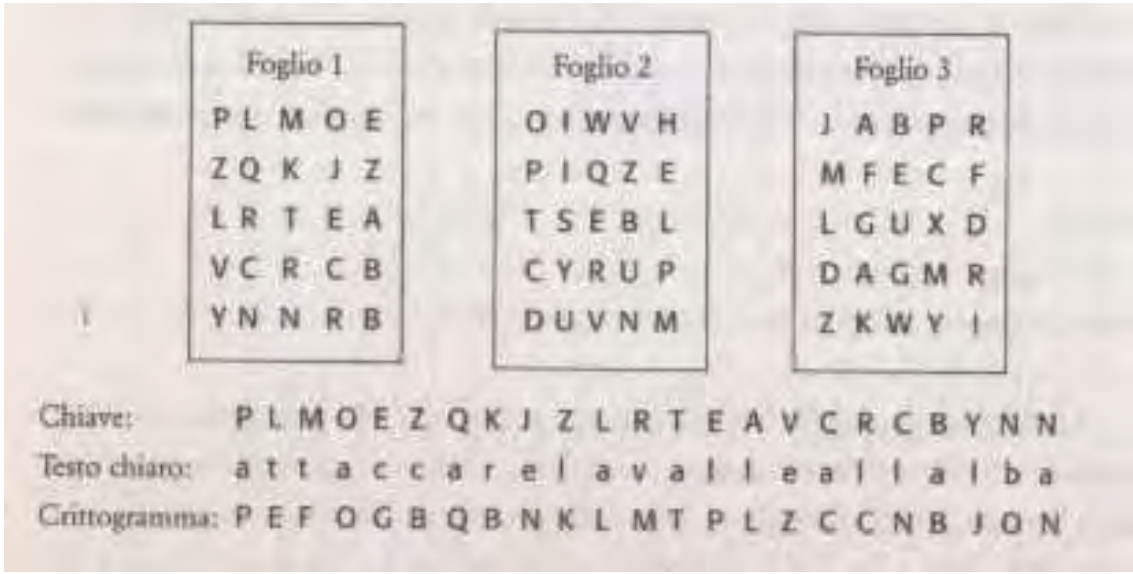
Foglio 3				
J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

Chiave:	P	L	M	O	E	Z	Q	K	J	Z	L	R	T	E	A	V	C	R	C	B	Y	N	N			
Testo chiaro:	a	t	t	a	c	c	a	r	e	l	a	v	a	l	l	e	a	l	l	a	l	b	a			
Crittogramma:	P	E	F	O	G	B	Q	B	N	K	L	M	T	P	L	Z	C	C	N	B	J	O	N			

Il sistema di cifratura a blocchi monouso (*one-time pad cipher*) è inviolabile!
Non è utilizzato (se non da potenti come i presidenti americano e russo) perché:

- è "complicato" produrre un numero molto elevato di chiavi casuali in termini di tempo, fatica e denaro;
- è "complicato" distribuire le chiavi casuali.

Il Santo Graal della crittografia



Foglio 1				
P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Foglio 2				
O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

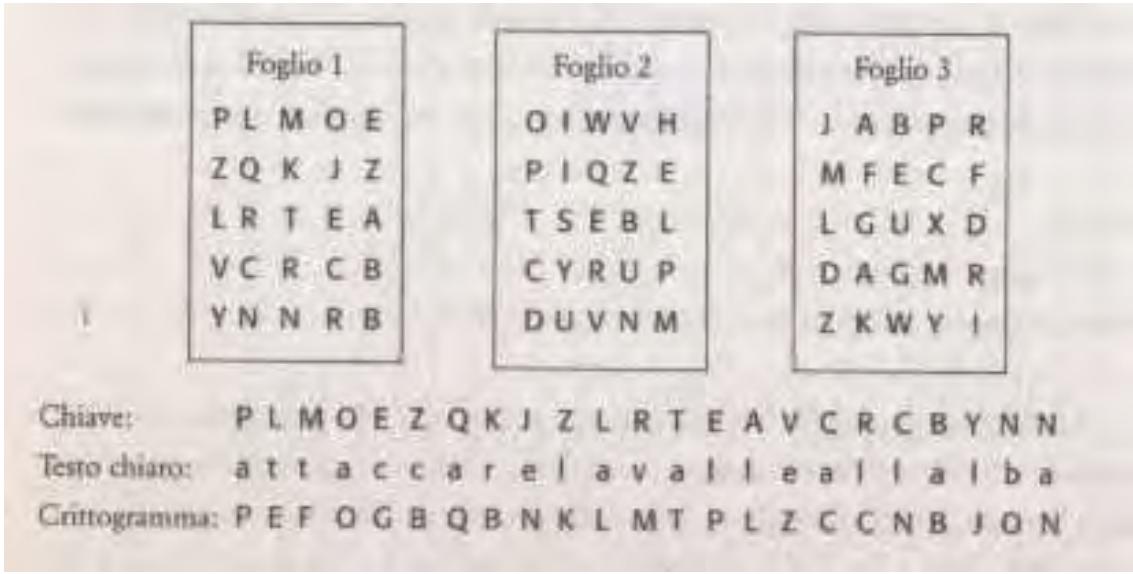
Foglio 3				
J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

Chiave:	P	L	M	O	E	Z	Q	K	J	Z	L	R	T	E	A	V	C	R	C	B	Y	N	N
Testo chiaro:	a	t	t	a	c	c	a	r	e	l	a	v	a	l	l	e	a	l	l	a	l	b	a
Crittogramma:	P	E	F	O	G	B	Q	B	N	K	L	M	T	P	L	Z	C	C	N	B	J	O	N

Il sistema di cifratura a blocchi monouso (*one-time pad cipher*) è inviolabile!
Non è utilizzato (se non da potenti come i presidenti americano e russo) perché:

- è "complicato" produrre un numero molto elevato di chiavi casuali in termini di tempo, fatica e denaro;
- è "complicato" distribuire le chiavi casuali.

Il Santo Graal della crittografia



Foglio 1				
P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Foglio 2				
O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

Foglio 3				
J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

Chiave:	P	L	M	O	E	Z	Q	K	J	Z	L	R	T	E	A	V	C	R	C	B	Y	N	N
Testo chiaro:	a	t	t	a	c	c	a	r	e	l	a	v	a	l	l	e	a	l	l	a	l	b	a
Crittogramma:	P	E	F	O	G	B	Q	B	N	K	L	M	T	P	L	Z	C	C	N	B	J	O	N

Il sistema di cifratura a blocchi monouso (*one-time pad cipher*) è inviolabile!
Non è utilizzato (se non da potenti come i presidenti americano e russo) perché:

- è "complicato" produrre un numero molto elevato di chiavi casuali in termini di tempo, fatica e denaro;
- è "complicato" distribuire le chiavi casuali.

Nel tempo libero...

Bibliografia

Marcus du Sautoy, *L'enigma dei numeri primi*, BUR Editore
Simon Singh, *Codici e segreti*, BUR Editore
Simon Singh, *L'ultimo teorema di Fermat*, BUR Editore
David Leavitt, *L'uomo che sapeva troppo*, Codice Editore

Sitografia

Simulatore macchina Enigma: http://users.telenet.be/d.rijmenants/
Simulatore RSA: http://crema.di.unimi.it/∼citrini/MD/RSA/esempio.htm

LWFENJ
UJW
Q'FYYJSENTSJ