Crittografia a chiave pubblica

La matematica per la crittografia

a cura di Alessandro Musesti

Università Cattolica del Sacro Cuore, Brescia

Settimana della Scienza, Brescia, 21 ottobre 2025

UNIVERSITÀ
CATTOLICA
del Sacro Cuore

La sostituzione monoalfabetica

Nella sostituzione monoalfabetica si sostituisce ad ogni lettera un'altra lettera (o un altro simbolo), in modo che a simbolo uguale corrisponda lettera uguale.

La sostituzione monoalfabetica

Nella sostituzione monoalfabetica si sostituisce ad ogni lettera un'altra lettera (o un altro simbolo), in modo che a simbolo uguale corrisponda lettera uguale.
Un esempio è il **metodo Atbash**: si sostituisce la prima lettera dell'alfabeto con l'ultima, la seconda con la penultima, e così via.

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

La sostituzione monoalfabetica

Nella sostituzione monoalfabetica si sostituisce ad ogni lettera un'altra lettera (o un altro simbolo), in modo che a simbolo uguale corrisponda lettera uguale.
Un esempio è il **metodo Atbash**: si sostituisce la prima lettera dell'alfabeto con l'ultima, la seconda con la penultima, e così via.

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

Provate a decifrare la frase

HVGGRNZMZ WVOOZ HXRVMAZ

La sostituzione monoalfabetica

Nella sostituzione monoalfabetica si sostituisce ad ogni lettera un'altra lettera (o un altro simbolo), in modo che a simbolo uguale corrisponda lettera uguale.
Un esempio è il **metodo Atbash**: si sostituisce la prima lettera dell'alfabeto con l'ultima, la seconda con la penultima, e così via.

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

Provate a decifrare la frase

`settimana della scienza`

La sostituzione monoalfabetica

Un altro esempio è il **cifrario di Cesare**: si sostituisce ogni lettera con quella che viene tre lettere dopo nell'alfabeto (quando si arriva in fondo, si ricomincia da capo).

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P
Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usato qualsiasi altro spostamento (compreso tra 1 e 25).

La sostituzione monoalfabetica

Un altro esempio è il **cifrario di Cesare**: si sostituisce ogni lettera con quella che viene tre lettere dopo nell'alfabeto (quando si arriva in fondo, si ricomincia da capo).

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P
Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usato qualsiasi altro spostamento (compreso tra 1 e 25).

Provate a decifrare la frase

DWWDFFKHUHPR D PHCCDQRWWH

La sostituzione monoalfabetica

Un altro esempio è il **cifrario di Cesare**: si sostituisce ogni lettera con quella che viene tre lettere dopo nell'alfabeto (quando si arriva in fondo, si ricomincia da capo).

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usato qualsiasi altro spostamento (compreso tra 1 e 25).

Provate a decifrare la frase

attaccheremo a mezzanotte

Cifrari per sostituzione

Si possono anche usare rimescolamenti "casuali" per la sostituzione, ad esempio

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

a patto che ogni lettera vada in una lettera diversa.

Cifrari per sostituzione

Si possono anche usare rimescolamenti "casuali" per la sostituzione, ad esempio

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

a patto che ogni lettera vada in una lettera diversa.
In tutto ci sono

$$!26 = 148\,362\,637\,348\,470\,135\,821\,287\,825$$

possibilità (dismutazioni), cioè all'incirca 148 milioni di miliardi di miliardi di modi di scambiare tutte le lettere!

Cifrari per sostituzione

Si possono anche usare rimescolamenti "casuali" per la sostituzione, ad esempio

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

a patto che ogni lettera vada in una lettera diversa.
In tutto ci sono

$$!26 = 148\,362\,637\,348\,470\,135\,821\,287\,825$$

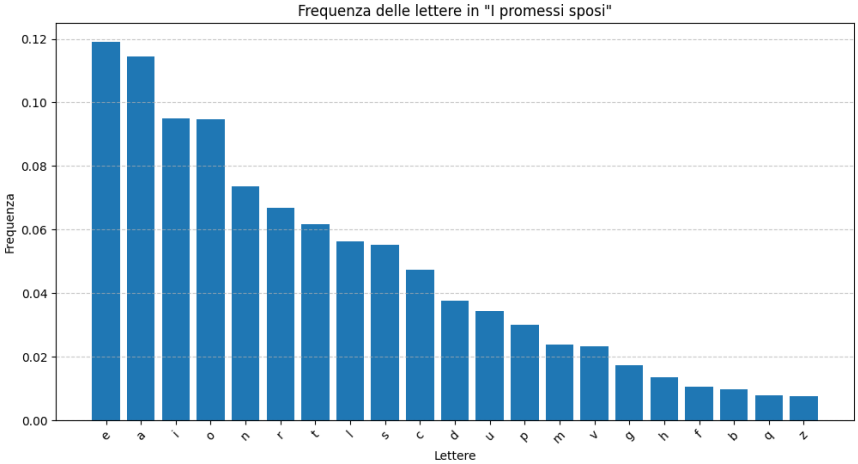
possibilità (dismutazioni), cioè all'incirca 148 milioni di miliardi di miliardi di modi di scambiare tutte le lettere!

Ma c'è un problema...

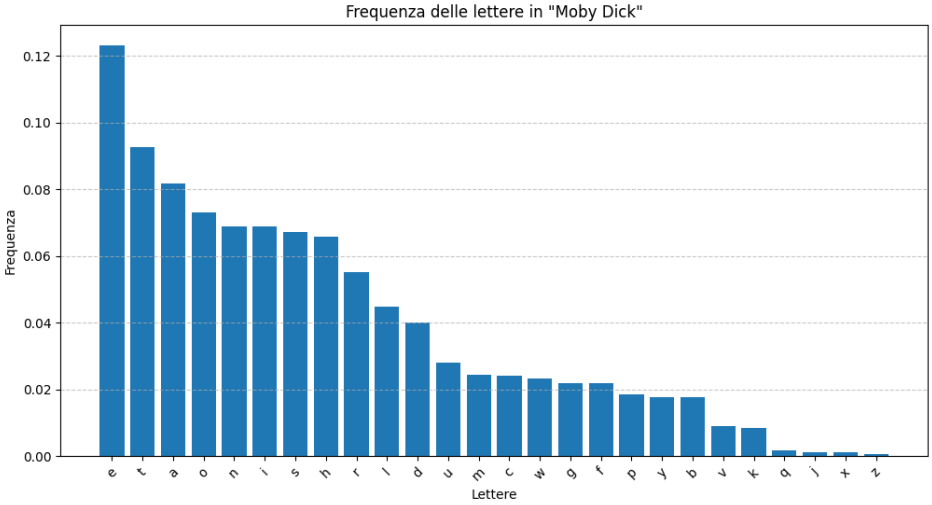
a simbolo uguale corrisponde lettera uguale

al-Kindi, scienziato arabo del IX secolo d.C, cominciò a studiare l'**analisi delle frequenze**.

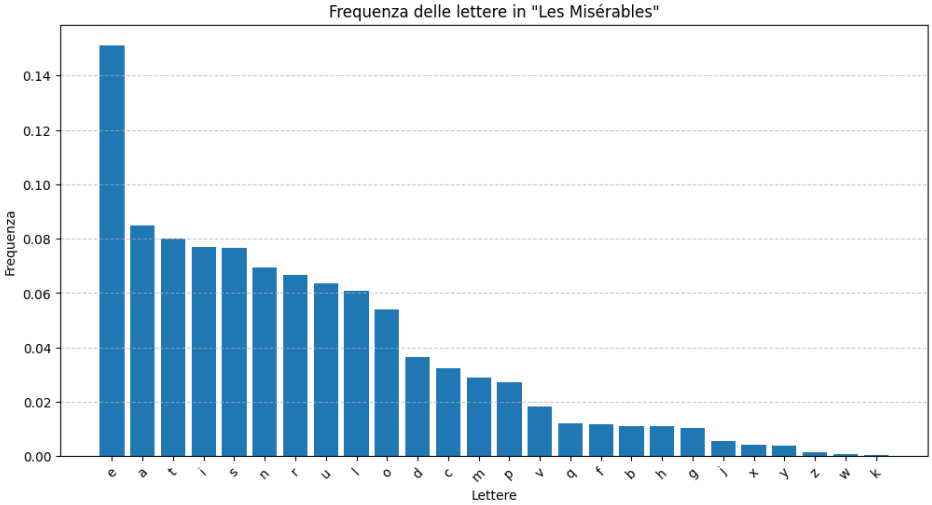
Analisi delle frequenze: italiano



Analisi delle frequenze: inglese



Analisi delle frequenze: francese



La sostituzione polialfabetica: il cifrario di Vigenère (1586)

Storicamente inventato da Giovan Battista Bellaso (Brescia, 1505 – . . .)
In questo metodo bisogna stabilire un numero (preferibilmente grande) comune: questo sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia `177839` e supponiamo di voler cifrare la frase "`mi piace la matematica`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, il numero-chiave. Poi ad ogni lettera "sommiamo" il valore della cifra corrispondente del numero-chiave, trovando una nuova lettera:

La sostituzione polialfabetica: il cifrario di Vigenère (1586)

Storicamente inventato da Giovan Battista Bellaso (Brescia, 1505 – . . .)
In questo metodo bisogna stabilire un numero (preferibilmente grande) comune: questo sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia `177839` e supponiamo di voler cifrare la frase "`mi piace la matematica`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, il numero-chiave. Poi ad ogni lettera "sommiamo" il valore della cifra corrispondente del numero-chiave, trovando una nuova lettera:

Chiaro	m	i	p	i	a	c	e	l	a	m	a	t	e	m	a	t	i	c	a
Chiave	1	7	7	8	3	9	1	7	7	8	3	9	1	7	7	8	3	9	1
Cifrato	N	P	W	Q	D	L	F	S	H	U	D	C	F	T	H	B	L	L	B

La sostituzione polialfabetica: il cifrario di Vigenère (1586)

Storicamente inventato da Giovan Battista Bellaso (Brescia, 1505 – . . .)
In questo metodo bisogna stabilire un numero (preferibilmente grande) comune: questo sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia `177839` e supponiamo di voler cifrare la frase "`mi piace la matematica`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, il numero-chiave. Poi ad ogni lettera "sommiamo" il valore della cifra corrispondente del numero-chiave, trovando una nuova lettera:

Chiaro	m	i	p	i	a	c	e	l	a	m	a	t	e	m	a	t	i	c	a
Chiave	1	7	7	8	3	9	1	7	7	8	3	9	1	7	7	8	3	9	1
Cifrato	N	P	W	Q	D	L	F	S	H	U	D	C	F	T	H	B	L	L	B

Questo codice è piuttosto robusto (non basta l'analisi delle frequenze per forzarlo) ma dipende molto dalla lunghezza del numero-chiave: se questa è corta, diventa abbastanza debole.

La sostituzione polialfabetica: il cifrario di Vigenère (1586)

Storicamente inventato da Giovan Battista Bellaso (Brescia, 1505 – . . .)
In questo metodo bisogna stabilire un numero (preferibilmente grande) comune: questo sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia `177839` e supponiamo di voler cifrare la frase "`mi piace la matematica`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, il numero-chiave. Poi ad ogni lettera "sommiamo" il valore della cifra corrispondente del numero-chiave, trovando una nuova lettera:

Chiaro	m	i	p	i	a	c	e	l	a	m	a	t	e	m	a	t	i	c	a
Chiave	1	7	7	8	3	9	1	7	7	8	3	9	1	7	7	8	3	9	1
Cifrato	N	P	W	Q	D	L	F	S	H	U	D	C	F	T	H	B	L	L	B

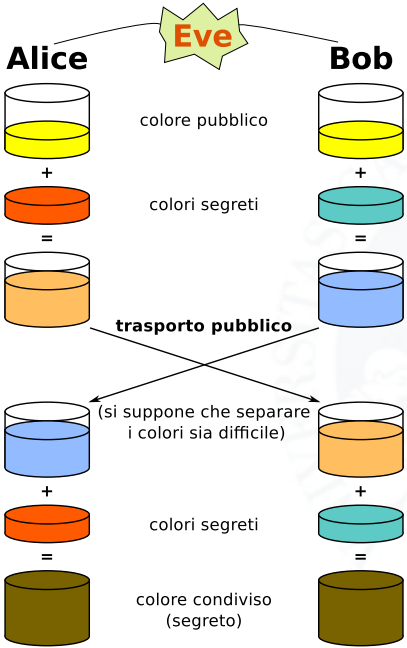
Questo codice è piuttosto robusto (non basta l'analisi delle frequenze per forzarlo) ma dipende molto dalla lunghezza del numero-chiave: se questa è corta, diventa abbastanza debole.

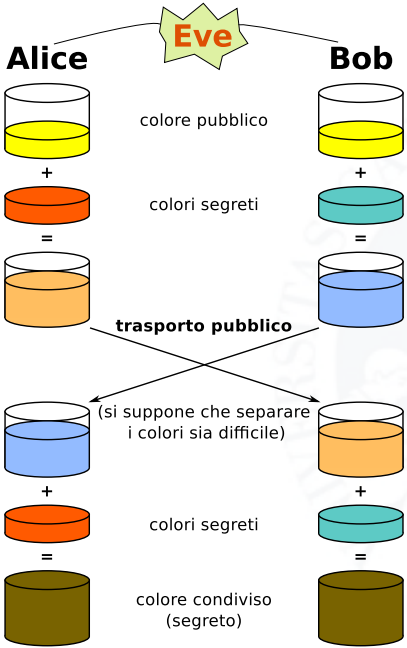
Inoltre, bisogna prima condividere la chiave!

Condivisione di una chiave: l'esempio con i colori

Alice e Bob vogliono poter scambiare messaggi senza che altri (rappresentati da Eve, che origlia) li capiscano. Per fare questo devono entrambi avere una "chiave" su cui basare uno scambio di messaggi crittografico. Come possono fare a condividere questa chiave?

Vediamo un esempio, fatto coi colori, che si basa su un colore segreto (la chiave privata) e un colore noto a tutti (la chiave pubblica). Entrambi giungono a condividere un colore senza che Eve ne sia a conoscenza.


Eve
Alice
Bob
colore pubblico
+
+
colori segreti
=
=
trasporto pubblico
(si suppone che separare
i colori sia difficile)
+
+
colori segreti
=
=
colore condiviso
(segreto)



È **facile** mescolare i colori, ma è **difficile** capire quali colori formano una miscela.

Si parla di
funzione unidirezionale

Un attrezzo matematico: le moltiplicazioni e le potenze “sull’orologio”

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Un attrezzo matematico: le moltiplicazioni e le potenze “sull’orologio”

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.

Un attrezzo matematico: le moltiplicazioni e le potenze “sull’orologio”

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.
Se l’orologio segna le 5 si “moltiplica” quest’ora per 8, che ora risulterà?

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?

Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?

Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4. Nell'aritmetica "dell'orologio" non interessa il numero dei giri, ma solo quello che avanza alla fine (il **resto** della divisione). Questa si chiama **aritmetica modulare**.

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 =$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod} 11),$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 =$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11),$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11), \quad 2^6 =$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11), \quad 2^6 = 9(\mathrm{mod}11)$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11), \quad 2^6 = 9(\mathrm{mod}11)$$

L'insieme dei numeri $\{0, 1, \ldots, p-1\}$ dotato di queste operazioni particolari si denota con $\mathbb{Z}_p$.

Generatori di $\mathbb{Z}_p$

Un **generatore** g in $\mathbb{Z}_p$ è un numero più piccolo di p tale che calcolando

$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} (\mathrm{mod}\, p)$$

si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 2 è un generatore per $p = 11$, poiché

n	1	2	3	4	5	6	7	8	9	10
$2^n (\mathrm{mod} 11)$	2	4	8	5	10	9	7	3	6	1

Generatori di $\mathbb{Z}_p$

Un **generatore** g in $\mathbb{Z}_p$ è un numero più piccolo di p tale che calcolando

$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} (\mathrm{mod}\, p)$$

si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 2 è un generatore per $p = 11$, poiché

n	1	2	3	4	5	6	7	8	9	10
$2^n (\mathrm{mod} 11)$	2	4	8	5	10	9	7	3	6	1

Teorema

Se p è primo, esiste sempre almeno un generatore in $\mathbb{Z}_p$.

Dimostrazione...

Dimostrazione dell'esistenza di un generatore modulo p^k, p dispari [modifica | modifica wikitesto]

La dimostrazione dell'esistenza del generatore procede dapprima provando che essa esiste per ogni numero primo p, poi dimostrando che, se a è una radice primitiva di p, allora o a o $p+a$ è una radice primitiva di p^2, e che questa è poi radice primitiva anche di ogni potenza successiva di p. Infatti, sia a una radice primitiva modulo p. Allora, per definizione di radice primitiva

$$a^{p-1} \equiv 1 \mod p,$$

e $p-1$ è il più piccolo esponente per cui ciò avviene. Poiché $\phi(p^2) = p(p-1)$, l'ordine moltiplicativo di a modulo p^2 divide $p(p-1)$, ed è multiplo di $p-1$, e quindi può essere solamente $p-1$ o lo stesso $p(p-1)$. In quest'ultimo caso a è una radice primitiva modulo p^2; altrimenti, sviluppiamo con la formula del binomio di Newton

$$(p+a)^{p-1} = p^{p-1} + \cdots + \binom{p-1}{p-2} p a^{p-2} + a^{p-1} \equiv (p-1)pa^{p-2} + a^{p-1} \mod p^2 \equiv 1 - pa^{p-2} \mod p^2,$$

che non può essere 1, perché altrimenti p dividerebbe a^{p-2}, il che è assurdo, e quindi l'ordine di $p+a$ non è $p-1$, e deve essere $p(p-1)$, cioè abbiamo trovato una radice primitiva modulo p^2.

Per dimostrare la proposizione per p^k, con $k > 2$, si procede per induzione: supponiamo che a sia una radice primitiva per tutti i p^j con $j < k$. In particolare

$$a^{\phi(p^{k-2})} \equiv 1 \mod p^{k-2},$$

ossia

$$a^{\phi(p^{k-2})} = 1 + lp^{k-2},$$

per un qualche l. Questa relazione vale anche modulo p^k; inoltre l'ordine di a modulo p^k deve essere un multiplo di $\phi(p^{k-1})$, perché ha quest'ordine modulo p^{k-1}. Quindi, poiché $\phi(p^k) = p\phi(p^{k-1})$, l'ordine può essere solo $\phi(p^{k-1})$ o $p\phi(p^{k-1})$; in particolare, a è una radice primitiva se il suo ordine è il secondo di questi valori. Se p è un primo dispari

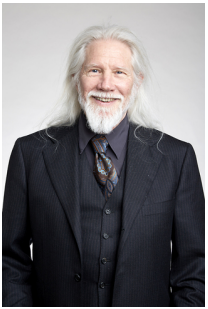
$$a^{\phi(p^{k-1})} = (a^{\phi(p^{k-2})})^p = (1 + lp^{k-2})^p \equiv 1 + \binom{p}{p-1} lp^{k-2} \mod p^k \equiv 1 + lp^{k-1} \mod p^k.$$

Questa quantità è uguale a 1 se e solo se l è divisibile per p; tuttavia, se lo fosse, si avrebbe

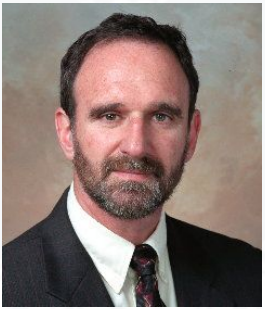
$$a^{\phi(p^{k-2})} = 1 + lp^{k-2} \equiv 1 \mod p^{k-1}$$

contro l'ipotesi che l'ordine di a modulo p^{k-1} sia $\phi(p^{k-1})$. Questo è assurdo, e quindi l'ordine di a modulo p^k è esattamente $\phi(p^k)$, e a è una radice primitiva modulo p^k. Per induzione questo è valido per ogni k.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)



Whitfield Diffie



Martin Hellman

Ralph Merkle

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.

È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.

È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.

Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.

È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.

Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Nella pratica p è un numero molto grande (1024 bit), mentre g può anche essere piccolo.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.

È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.

Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Nella pratica p è un numero molto grande (1024 bit), mentre g può anche essere piccolo.

Poi si esegue la procedura seguente:

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod} p) = 6^{10} (\mathrm{mod} 17) = 15$
Bob calcola il numero $B = g^b (\mathrm{mod} p) = 6^{14} (\mathrm{mod} 17) = 9$.

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$
Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$
Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola
$B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$
Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola
$B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.
Bob prende la chiave pubblica di Alice, $A = 15$, e calcola
$A^b (\mathrm{mod}\, p) = 15^{14} (\mathrm{mod} 17) = 13$.

La procedura Diffie-Hellman-Merkle

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Ad esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$
Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola
$B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.
Bob prende la chiave pubblica di Alice, $A = 15$, e calcola
$A^b (\mathrm{mod}\, p) = 15^{14} (\mathrm{mod} 17) = 13$.

Stesso numero: $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a = 13 (\mathrm{mod}\, p)$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Allora le chiavi pubbliche sono $A = g^a = 19135999$, $B = g^b = 5444512$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Allora le chiavi pubbliche sono $A = g^a = 19135999$, $B = g^b = 5444512$.

E si ha $A^b = B^a = 18352668$, che è la chiave condivisa.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Ma allora dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga!

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Ma allora dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga!

Questa operazione si chiama **logaritmo discreto**, ed è una funzione unidirezionale: è abbastanza facile calcolare $A = g^a$, ma è molto difficile scoprire l'esponente a conoscendo g e A. Anche i computer attualmente più potenti impiegherebbero centinaia di anni.

La fattorizzazione dei numeri interi

Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

La fattorizzazione dei numeri interi

Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...

La fattorizzazione dei numeri interi

Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...
E invece verificate, con la calcolatrice, quanto fa

$$14087 \times 27749$$

La fattorizzazione dei numeri interi

Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

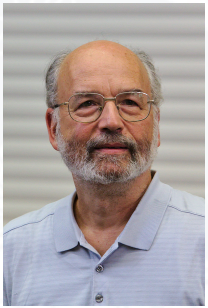
Provate a fattorizzare il numero 390900163...
E invece verificate, con la calcolatrice, quanto fa

$$14087 \times 27749$$

Nelle attuali applicazioni informatiche si usano numeri di 1024 bit, che superano le 300 cifre decimali, o addirittura di 2048 bit!

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

Ronald Rivest



Adi Shamir

Leonard Adleman

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.
Scegliamo $e = 5$, che non ha fattori in comune con 36.

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.
Scegliamo $e = 5$, che non ha fattori in comune con 36.
Si verifica che $5 \cdot 29 = 1 (\mathrm{mod} 36)$, quindi prendiamo $d = 29$.

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.
Scegliamo $e = 5$, che non ha fattori in comune con 36.
Si verifica che $5 \cdot 29 = 1 (\mathrm{mod} 36)$, quindi prendiamo $d = 29$.
Ora teniamo segreta la chiave privata 29 e rendiamo pubblica la coppia $(57, 5)$, ad esempio scrivendola su un sito.

La procedura RSA

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un messaggio (numerico) m, ad esempio $m = 10$. Deve procedere così:

La procedura RSA

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un messaggio (numerico) m, ad esempio $m = 10$. Deve procedere così:

prende $(57, 5)$, che è pubblica, e calcola

$$10^5 (\mathrm{mod} 57) = 22;$$

poi ci comunica il risultato 22.

La procedura RSA

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un messaggio (numerico) m, ad esempio $m = 10$. Deve procedere così:

prende $(57, 5)$, che è pubblica, e calcola

$$10^5 (\mathrm{mod} 57) = 22;$$

poi ci comunica il risultato 22.

Usando la nostra chiave privata, noi poi calcoliamo

$$22^{29} (\mathrm{mod} 57) = 10$$

ottenendo proprio il numero di partenza.

Un esempio con numeri più grandi

- $p = 8117, \quad q = 27\,647, \quad N = p \cdot q = 224\,410\,699,$
  $r = (p-1) \cdot (q-1) = 224\,374\,936$

Un esempio con numeri più grandi

- $p = 8117, \quad q = 27\,647, \quad N = p \cdot q = 224\,410\,699,$
  $r = (p-1) \cdot (q-1) = 224\,374\,936$
- $e = 3$

Un esempio con numeri più grandi

- $p = 8117, \quad q = 27\,647, \quad N = p \cdot q = 224\,410\,699,$
  $r = (p-1) \cdot (q-1) = 224\,374\,936$
- $e = 3$
- $d = 149\,583\,291$ tale che $e \cdot d = 1 (\mathrm{mod}\, r)$

Un esempio con numeri più grandi

- $p = 8117, \quad q = 27\,647, \quad N = p \cdot q = 224\,410\,699,$
  $r = (p-1) \cdot (q-1) = 224\,374\,936$
- $e = 3$
- $d = 149\,583\,291$ tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- $(224\,410\,699, 3)$ è la chiave pubblica, $149\,583\,291$ la chiave privata.

Se qualcuno vuole comunicarci segretamente il messaggio $m = 97\,108\,101$ (`ale`), procede così:

Un esempio con numeri più grandi

- $p = 8117, \quad q = 27\,647, \quad N = p \cdot q = 224\,410\,699,$
  $r = (p-1) \cdot (q-1) = 224\,374\,936$
- $e = 3$
- $d = 149\,583\,291$ tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- $(224\,410\,699, 3)$ è la chiave pubblica, $149\,583\,291$ la chiave privata.

Se qualcuno vuole comunicarci segretamente il messaggio $m = 97\,108\,101$ (`ale`), procede così: calcola

$$97\,108\,101^3 (\mathrm{mod}\, 224\,410\,699) = 117\,560\,046$$

e ci comunica il risultato;

Un esempio con numeri più grandi

- $p = 8117, \quad q = 27\,647, \quad N = p \cdot q = 224\,410\,699,$
  $r = (p-1) \cdot (q-1) = 224\,374\,936$
- $e = 3$
- $d = 149\,583\,291$ tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- $(224\,410\,699, 3)$ è la chiave pubblica, $149\,583\,291$ la chiave privata.

Se qualcuno vuole comunicarci segretamente il messaggio $m = 97\,108\,101$ (`ale`), procede così: calcola

$$97\,108\,101^3 (\mathrm{mod}\, 224\,410\,699) = 117\,560\,046$$

e ci comunica il risultato;
usando la nostra chiave privata, noi calcoliamo

$$117\,560\,046^{149\,583\,291} (\mathrm{mod}\, 224\,410\,699) = 97\,108\,101$$

che è proprio il numero di partenza.

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29:

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29:
basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29:
basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Ma per fattorizzare N bisogna andare per tentativi!
Usando numeri primi di più di 300 cifre sarebbero richieste centinaia di anni di calcoli con un super-computer...

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29:
basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Ma per fattorizzare N bisogna andare per tentativi!
Usando numeri primi di più di 300 cifre sarebbero richieste centinaia di anni di calcoli con un super-computer...

A meno di non trovare un metodo alternativo (che nessuno ha ancora scoperto!)

La firma digitale

Il metodo RSA può essere usato anche “al contrario”, per garantire chi sia l’autore di un certo messaggio.

La firma digitale

Il metodo RSA può essere usato anche "al contrario", per garantire chi sia l'autore di un certo messaggio.
Se io voglio "firmare" il messaggio 97 108 101 (`ale`), uso la mia chiave **privata** per crittarlo:

$$97\,108\,101^{149\,583\,291} (\mathrm{mod} 224\,410\,699) = 121\,786\,413.$$

La firma digitale

Il metodo RSA può essere usato anche "al contrario", per garantire chi sia l'autore di un certo messaggio.
Se io voglio "firmare" il messaggio 97 108 101 (`ale`), uso la mia chiave **privata** per crittarlo:

$$97\,108\,101^{149\,583\,291} (\mathrm{mod} 224\,410\,699) = 121\,786\,413.$$

Il numero ottenuto è l'unico numero tale che, usando la **mia** chiave pubblica, produca il messaggio originale:

$$121\,786\,413^{3} (\mathrm{mod} 224\,410\,699) = 97\,108\,101.$$

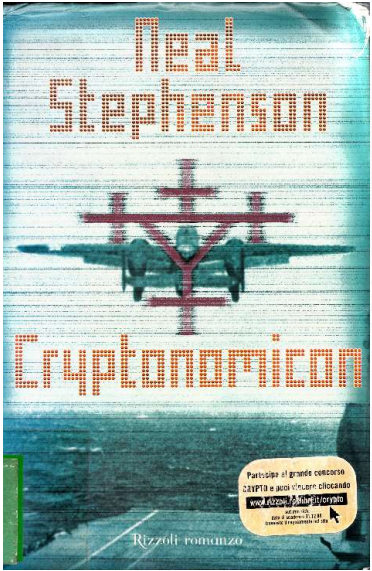
I rischi di codici non sicuri

Maria Stuarda (1542-1587), regina di Scozia, tradita da un cifrario troppo debole, decifrato da Thomas Phelippes.

Crittografia al cinema

Crittografia al cinema

Crittografia nei libri



Fine

Grazie dell'attenzione