Crittografia

Sicurezza e privacy

2014-2016:

- WhatsApp (Jan Koum [ucraino], Brian Action) – California – 450 milioni di utenti
- 2012 – attacco hacker
- Maxie Marlinspike (crittografo)
- AES-256 cifratura US
- Diffie ed Helman (base teorica)
- Rivesr, Shamir, Adieman: RSA
- Garantire la riservatezza futura

Fermat

Il piccolo teorema di Fermat dice che se p è un numero primo, allora per ogni intero a:

$$a^p \equiv a \pmod{p}$$

Questo significa che se si prende un qualunque numero a, lo si moltiplica per se stesso p volte e si sottrae a, il risultato è divisibile per p (aritmetica modulare).

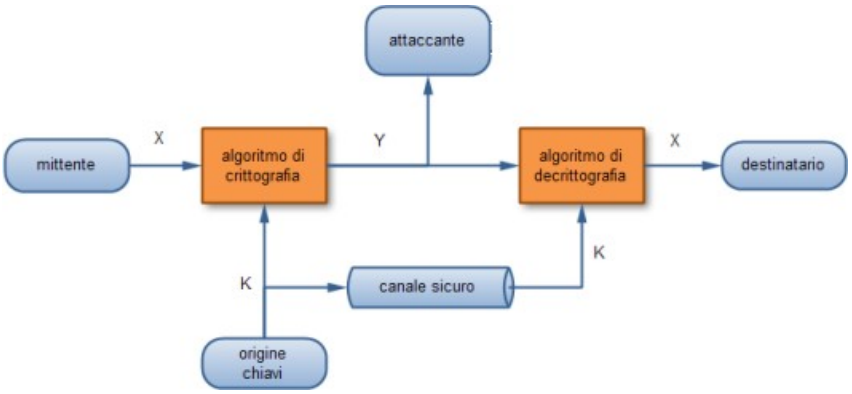
È spesso espresso nella forma equivalente: se p è primo e a è un intero coprimo con p, allora:

$$a^{p-1} \equiv 1 \pmod{p}$$

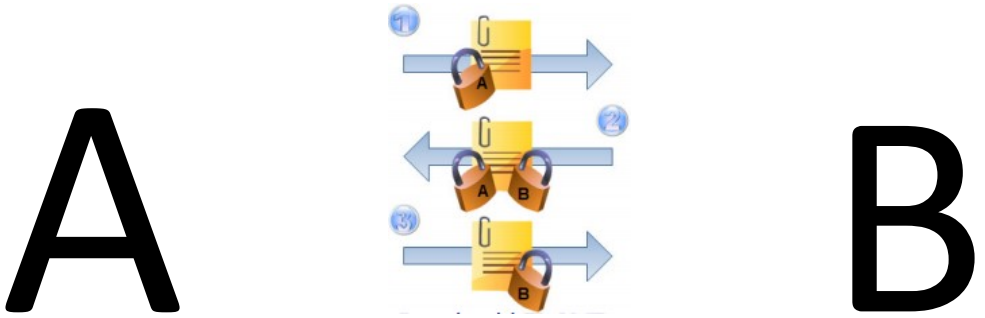
Va notato che la prima espressione è in un certo senso più generale: è infatti valida per numeri interi arbitrari, come 0 o multipli di p, che invece non rientrano nelle ipotesi della seconda.

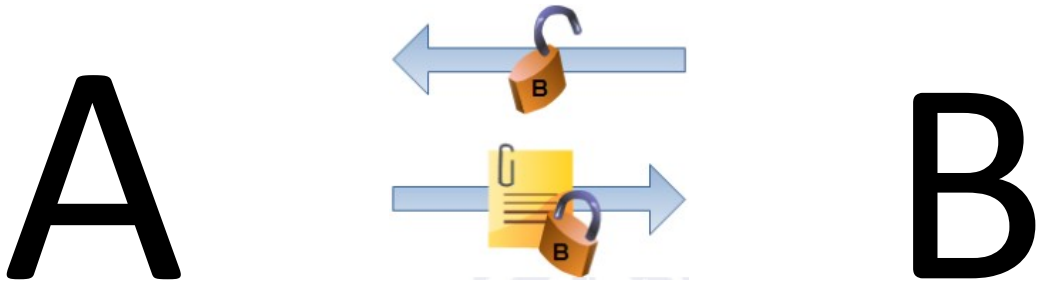
Simmetrica

Il principale problema della crittografia simmetrica sta nella necessità di disporre di un canale sicuro per la **trasmissione della chiave**.



Trasmissione chiave



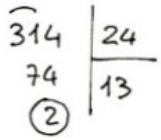


$C=F(M)$	facile
$M=F^{-1}(C)$	difficile se non si conosce la chiave

Aritmetica modulare o aritmetica dell'orologio

Alice, Bob e Eva — L'orologio

"Che ore saranno tra 314 ore?"
"Eh? Boh, devo fare il conto, non so."
"Fai il conto, allora"
"Uhm, 314 ore, ci sono 24 ore in un giorno, 314 diviso 24 fa 13.08(3)"
"E quindi?".
"E quindi 314 ore sono un po' più di 13 giorni."
"Vabbé, ma se vuoi sapere che ore saranno con precisione?"
"Uhm, allora, rimane un resto di zero virgola zero otto tre periodico …"
"Che non è propriamente un resto."
"Eh?"
"Eh, no. Non è il resto della divisione che hai fatto. Hai presente la regola per la divisione che hai imparato alle elementari?"
"Uh, quella! Da quanto tempo non ne faccio una. Eccola qua:"



"Oh, bene. Quindi vedi che 314 diviso 24 ti dà come quoziente 13 e come resto 2. Quello che ti interessa, ai fini della risposta alla mia domanda, è proprio il resto."
"Ah, ho capito: 314 ore corrispondono a 13 giorni e 2 ore, **quindi per sapere che ore saranno devo guardare l'orologio adesso e aggiungere 2 ore**. Facile."
"Benissimo. Il calcolo che hai fatto potrebbe essere scritto anche in questo modo: "

$$314 = 13 \cdot 24 + 2$$

"Vero."
"I veri matematici lo scrivono anche così: "

$$314 \equiv 2 \bmod 24$$

"Eh?"
"Significa che 314 e 2 danno lo stesso resto nella divisione per 24; il resto è naturalmente 2, che è minore di 24. Si legge in questo modo: "

314 è congruente (o congruo) a 2 modulo 24

"**Manca però il 13, il quoziente della divisione**."
"**Quello non ci interessa molto**. "

Quando siamo interessati di più ai resti che ai quozienti, utilizziamo questo tipo di scrittura. Ed entriamo nel cosiddetto campo dell'*aritmetica modulare*

"Che non è altro che un modo pomposo per definire l'aritmetica dell'orologio, a quanto vedo."
"Bè, sì, l'aritmetica dell'orologio è l'aritmetica modulo 24, ma naturalmente possiamo scegliere qualunque numero come base per i nostri moduli."
"E questo è interessante?"
"Certo."
"Voglio dire, serve a qualcosa?"
"Stranamente, sì. Non che ai Veri Matematici questo fatto interessi molto, però l'aritmetica modulare ha una effettiva applicazione pratica. Praticamente quotidiana."

Aritmetica modulare

a mod m = resto divisione
a ≡ b mod m significa a mod m = b mod m

Proprietà aritmetica modulare:

$[(a \bmod m) + (b \bmod m)] \bmod m = (a+b) \bmod m$
$[(a \bmod m) - (b \bmod m)] \bmod m = (a-b) \bmod m$
$[(a \bmod m) \cdot (b \bmod m)] \bmod m = (a \cdot b) \bmod m$
$[(a \bmod m)^k] \bmod m = a^k \bmod m$

Esempi:

a = 6
b = 7
m = 5
$[(a \bmod m) + (b \bmod m)] \bmod m = (a+b) \bmod m$
$[(6 \bmod 5) + (7 \bmod 5)] \bmod 5 = (6+7) \bmod 5$
$(1 + 2) \bmod 5 = 13 \bmod 5$
$3 \bmod 5 = 13 \bmod 5$
3 = 3

$[(a \bmod m)^k] \bmod m = a^k \bmod m$
$[(6 \bmod 5)^2] \bmod 5 = 6^2 \bmod 5$
$1 \bmod 5 = 36 \bmod 5$
1 = 1

Una conseguenza è che **funzioni invertibili diventano NON invertibili in aritmetica modulare**:

$a^b = c$	$b = \log_a c$
$a^b \bmod m = c$	b = ?

Algoritmo di Diffie-Hellman

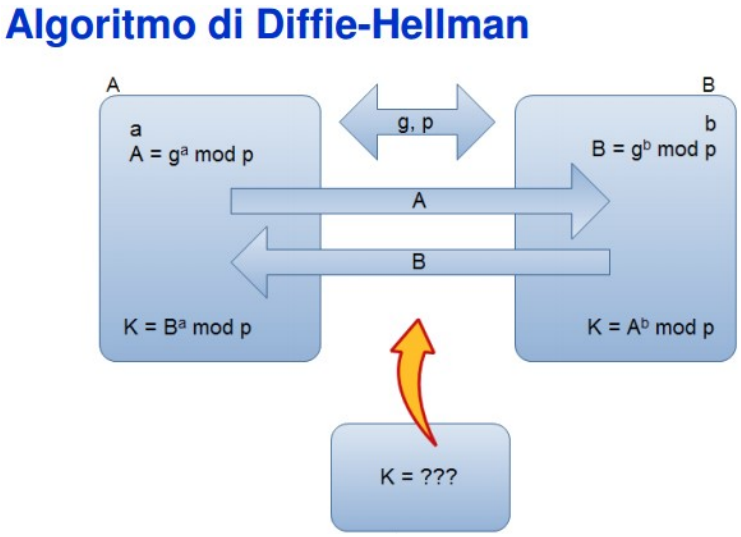
A e B conoscono due numeri g e p pubblici (p **primo** *cioè un numero naturale maggiore di 1 che sia divisibile solamente per 1 e per sé stesso*)
A conosce un numero segreto a
B conosce un numero segreto b

A calcola	$A = g^a \bmod p$	e lo comunica a	B
B calcola	$B = g^b \bmod p$	e lo comunica a	A
A calcola	$K = B^a \bmod p$		
B calcola	$K = A^b \bmod p$		

Ma:

$K = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ba} \bmod p$
$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$

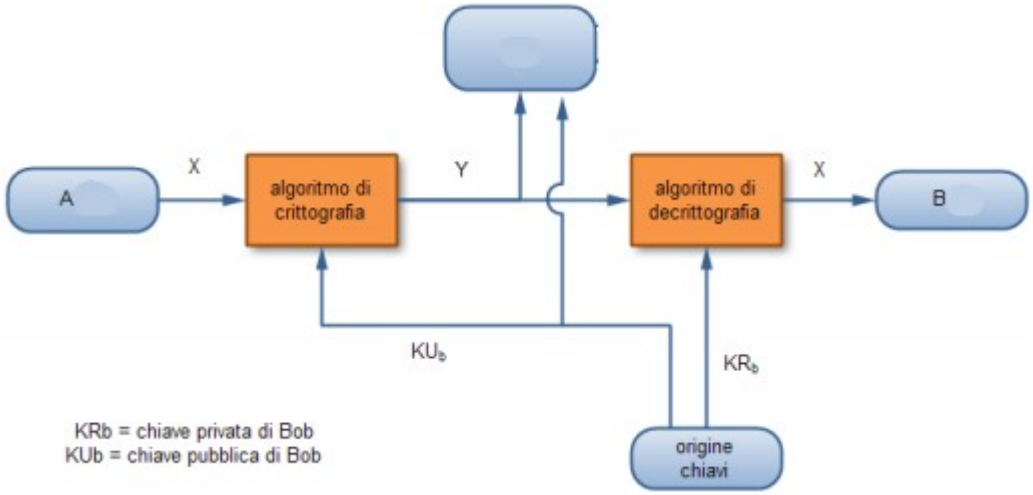
A e B hanno condiviso un segreto (**il numero K**) senza comunicarlo esplicitamente!
Un eventuale attaccante può osservare A, B, g, p ma questa informazione non è sufficiente per ricavare K.
K è calcolabile solo conoscendo a o b, che tuttavia sono segreti e non vengono mai trasmessi. Ricavare a da A (o analogamente b da B) significa risolvere un logaritmo discreto, difficile dal punto di vista computazionale.



Considerazioni sull'algoritmo di Diffie-Hellman:

- Usando l'algoritmo sviluppato da Diffie ed Hellman nel 1976, A e B possono condividere un numero segreto senza trasmetterlo.
- **Se questo numero è la chiave di un algoritmo a cifratura simmetrica, si è trovato un modo per condividere la chiave senza la necessità di un canale di comunicazione sicuro!**
- L'unico modo che un intruso ha di trovare la chiave è quello di calcolare un logaritmo discreto. Tuttavia attualmente non sono noti algoritmi che risolvano questo problema in maniera efficiente.

Asimmetrica (a chiave pubblica)



RSA

- L'algoritmo RSA (dal nome degli inventori Rivest, Shamir e Adleman) è il più famoso algoritmo di crittografia a chiave pubblica
- Inventato nel 1977, poco dopo l'algoritmo di DiffieHellman
- Due componenti principali
    - Algoritmo di generazione delle chiavi
    - Algoritmo crittografico vero e propri

RSA – generazione delle chiavi da parte di Bob

- Scegliere **due numeri primi** **p e q**
- Calcolare **n = pq**
- Occorre sapere **quanti sono i numeri compresi tra 1 e n che siano coprimi con n** per sceglierne uno
- La φ(n) di Eulero serve a tale scopo e Il risultato è **f = φ (n) = (p – 1)(q – 1) = n – p – q + 1**.
- Scegliere **e** **1 <= e < (p-1) (q-1)** *con **e** coprimo con* φ(n)
- Calcolare **d** tale che **de ≡ 1 mod (p-1) (q-1)** che sarà compreso tra 1 e φ(n)
- La coppia **(n, e)** *è la **chiave pubblica di Bob***
- La coppia **(n, d)** *è la **chiave privata di Bob***
- Non è possibile risalire facilmente dalla chiave pubblica a quella privata (e viceversa), in quanto servirebbe conoscere il numero (p-1)(q-1), e questo implica fattorizzare n nei suoi fattori p e q (problema difficile)

Nota:

- due interi *a* e *b* si dicono **coprimi** (o **primi tra loro** o **relativamente primi**) se e solo se essi non hanno nessun divisore comune eccetto 1 e -1 o, in modo equivalente, se il loro massimo comune divisore è 1.
- a è coprimo di b se il massimo comune divisore tra a e b è 1 (7 e 15 sono coprimi, mentre 8 e 10 no, hanno in comune il divisore 2).
- se a è primo, allora è coprimo di qualsiasi numero che non sia diviso da a. Ad es. 7 è coprimo di tutti i numeri che non sono multipli di 7.
- **n** viene detto **modulo dell'RSA**.
- **e** viene detto **esponente pubblico**.
- **d** viene detto **esponente privato**.
- Il numero **d** compreso tra 1 e φ(n) che Bob calcola (usando **l'algoritmo di Euclide esteso**) è l'**inverso (mod f) di e**.

CONSULTARE ALLEGATI.

Esempio 1 :

- Supponiamo che i due numeri primi scelti da Bob siano **p = 23** e **q = 73**.
- Bob calcola **n = 23 x 73 = 1679.**
- Bob calcola la f = φ(n) di Eulero di 1679. Il risultato è **f = φ(1679) = 22 x 72 = 1584.**
- Bob sceglie un numero **e** compreso tra 1 e 1584 e coprimo con 1584. Supponiamo che sia **e = 5** il numero scelto da Bob.
- Bob calcola **d** usando l'algoritmo di Euclide esteso. Il risultato è **d = 317**.
- I numeri **n = 1679** ed **e = 5** sono la **chiave pubblica** di Bob.
- I numeri **p = 23**, **q = 73** e **d = 317** sono la **chiave privata** di Bob.

La chiave pubblica di Bob viene pubblicata su Internet

- Bob salva la chiave pubblica e quella privata su una pennetta USB.
- Bob si reca di persona presso una Certification Authority, ovvero un'azienda che è autorizzata per legge a pubblicare le chiavi pubbliche dell'RSA su Internet.
- La Certification Authority controlla che Bob abbia generato correttamente le due chiavi (pubblica e privata).
- La Certification Authority controlla che le chiavi generate da Bob siano sicure, ovvero che sia difficilissimo risalire alla chiave privata conoscendo soltanto la chiave pubblica. In altre parole, la Certification Authority si mette nei panni di un eventuale hacker e prova a calcolare **p**, **q** e **d** conoscendo soltanto **n** ed **e**.
- Se le chiavi di Bob superano i test di correttezza e di sicurezza (vedi i due punti precedenti), allora Bob riceve dalla Certification Authority un certificato contenente tutti i dettagli relativi alla sua chiave privata.
- La Certification Authority pubblica il certificato di Bob su Internet.

Alice** invia un messaggio cifrato a **Bob

- Alice cerca su Internet il certificato con la chiave pubblica di Bob. In altre parole, Alice cerca i due numeri **n** ed **e** che Bob ha generato.
- Alice sceglie il messaggio da inviare a Bob. Il messaggio è un numero **m** compreso tra 1 ed (n – 1).
- Alice calcola $\mathbf{c = m^e \pmod n}$.
- Alice invia il numero **c** a Bob.

Esempio di invio:

- Alice cerca su Internet il certificato con la chiave pubblica di Bob. Scopre così che **n = 1679** ed **e = 5**.
- Alice sceglie un messaggio **m** compreso tra 1 e 1678. Supponiamo che il messaggio di Alice sia **m = 144**.
- Alice calcola $\mathbf{144^5 \pmod{1679}}$**.** Il risultato è **c = 1428**.
- Alice invia il numero 1428 a Bob.

Bob decifra il messaggio di Alice

- Bob calcola $\mathbf{c^d \pmod n}$. Il risultato che ottiene Bob è uguale al messaggio **m** di Alice!

Esempio ricezione messaggio:

- Il messaggio cifrato che Bob ha ricevuto da Alice è **c = 1428**.
- (Ricordiamo che l'esponente privato di Bob è d = 317). Bob calcola $\mathbf{1428^{317} \pmod{1679}}$**.** Il risultato è 144, ovvero il messaggio m di Alice!

Un hacker intercetta il messaggio cifrato e prova a decifrarlo.

- Per decifrare il messaggio cifrato (cioè c), l'hacker deve calcolare $\mathbf{c^d \pmod n}$.
- Per calcolare $c^d \pmod n$, l'hacker deve scoprire quanto vale l' esponente privato **d**.
- Per scoprire il valore di d, l'hacker deve calcolare **φ (n)** (questo perché d è l'inverso (mod n) dell'esponente pubblico e).
- Per calcolare facilmente **φ (n)**, l'hacker deve trovare due numeri primi p e q tali che n = p*q. Detto in altre parole, l'hacker deve fattorizzare **n**.
- Siccome fattorizzare n è un problema difficile da risolvere (anche per un computer!), l'hacker non è in grado di calcolare i due numeri p e q che moltiplicati tra loro danno come risultato n. La segretezza della comunicazione tra Alice e Bob è salva!

Esempio 2 :

Siano p = 3, q = 11
n = pq = 33, (p-1) (q-1) = 20
Scegliamo e = 7 *(7<20, 7 coprimo di 20)*
d = 3 *infatti 3*7 = 21 ≡ 1 mod 20*
La chiave pubblica è (33, 7)
La chiave privata è (33, 3)

Calcolo di d (*metodo di **Euclide***) (*Il procedimento si ripete, aggiungendo nuove righe alla tabella e calcolandone i valori usando le due righe precedenti. Ci si ferma quando nella prima colonna compare un 1*)

(p-1) (q-1)	a = 0	
e	b = 1	c = (p-1) (q-1) / e (**intero**)
(p-1) (q-1) mod e (**resto**)	a – b*c	

Sostituisco i valori per trovare d * 7 ≡ 1 mod 20:

20	a = 0	
7	b = 1	c = 2
6	– 2	c = 1
1	3	

d = 3 *(se il numero è negativo, si somma il modulo)*

Esercizio:
Dati p = 7, q = 13, e = …, calcolare la chiave pubblica (n,e) e privata (n,d).
p = 7, q = 13
n = p*q = 91
(p-1)*(q-1) = 72
e = 11 *(11<72, 11 coprimo di 72)*

Calcolo di d

(p-1) (q-1)	a = 0		
e	b = 1	c = (p-1) (q-1) / e	(intero)
(p-1) (q-1) mod e	a – b*c		
72	0		
11	1	6	
6	-6	1	
5	7	1	
1	-13		

d = -13 + 72 = 59

Pubblica: (91,11) Privata: (91, 59)

RSA – cifratura e decifratura

Dato un messaggio m (0 < m < n)

1. Cifratura: calcolare $c = m^e \bmod n$
2. Decifratura: calcolare $m = c^d \bmod n$

Esempi:
La chiave pubblica è (33, 7)
La chiave privata è (33, 3)

$c = 2^7 \bmod 33 = 29$
$m = 29^3 \bmod 33 = 2$

$c = 15^7 \bmod 33 = 27$
$m = 27^3 \bmod 33 = 15$