

Esperti nella gestione dei
sistemi informativi e tecnologie
informatiche

Analisi del rischio e Sicurezza delle attività

Docente: Eduard Roccatello
Email: eduard@roccatello.it
Sito: <http://www.roccatello.it/teaching/rsa/>

Storia e motivazione

- Primo utilizzo dai Romani

“Dyh Fdhvdu”

“Ave Caesar”

Metodo primitivo:

Spostamento di tre lettere nel
alfabeto (A->D, B->E, C->F...)

Storia e motivazione

- La rivelazione del codice del sistema Enigma dei sottomarini tedeschi permise agli Inglesi di decifrare la comunicazione tedesca e fu cruciale per l'andamento della guerra.
-

Storia e motivazione

□ La macchina Enigma:



Storia e motivazione

- Una chiave consisteva nella posizione dei rotori che veniva cambiata ogni 24 ore secondo una regola prefissata.
 - Un' ulteriore chiave veniva trasmessa in ogni messaggio due volte.
 - Nel 1932 il matematico polacco Marian Rejewski è riuscito a ricostruire la struttura dell'Enigma.
-

Cos'è la crittografia?

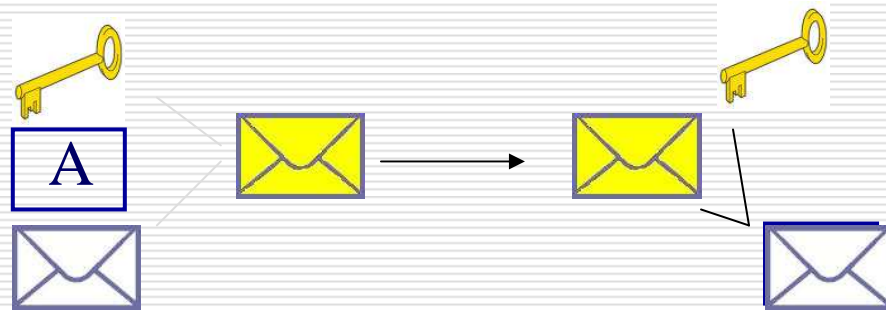


Obiettivi

- Segretezza
 - Il messaggio non deve essere leggibile a terzi.
 - Autenticazione
 - Il destinatario deve poter essere sicuro del mittente.
 - Integrità
 - Il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.
 - Attendibilità
 - Il mittente non deve poter negare di aver inviato questo messaggio.
-

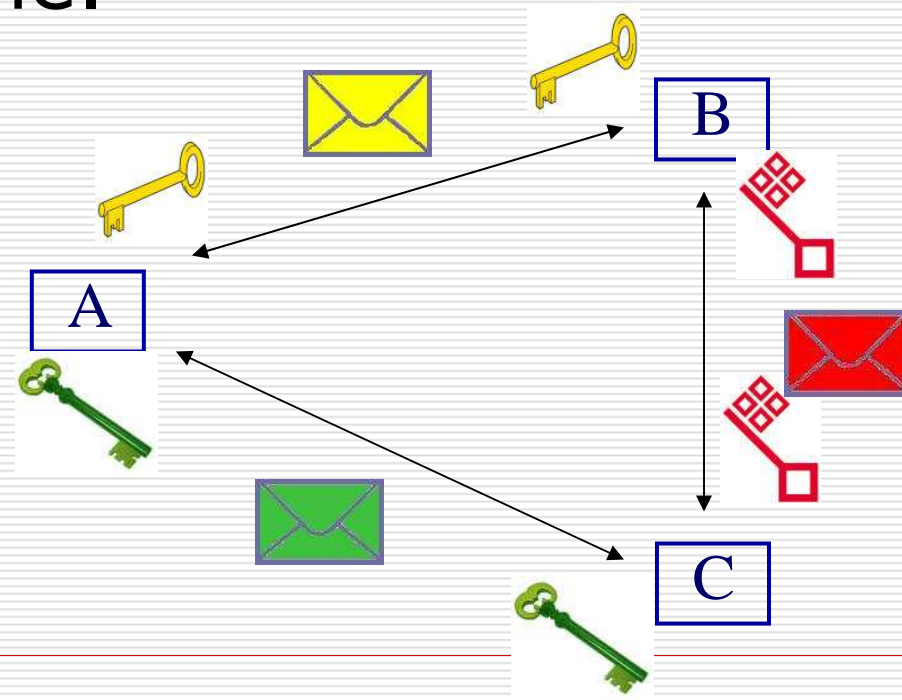
Crittografia classica

- ❑ Il mittente e il destinatario usavano una chiave comune che conoscono soltanto loro.
- ❑ Per questa ragione si parla anche di crittografia a chiave segreta o di crittografia simmetrica.



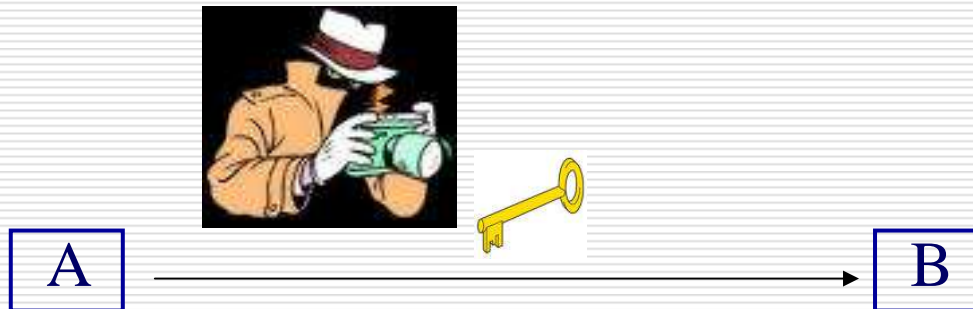
Crittografia classica: problemi

- Una persona deve possedere una chiave per ciascun partner di comunicazione.

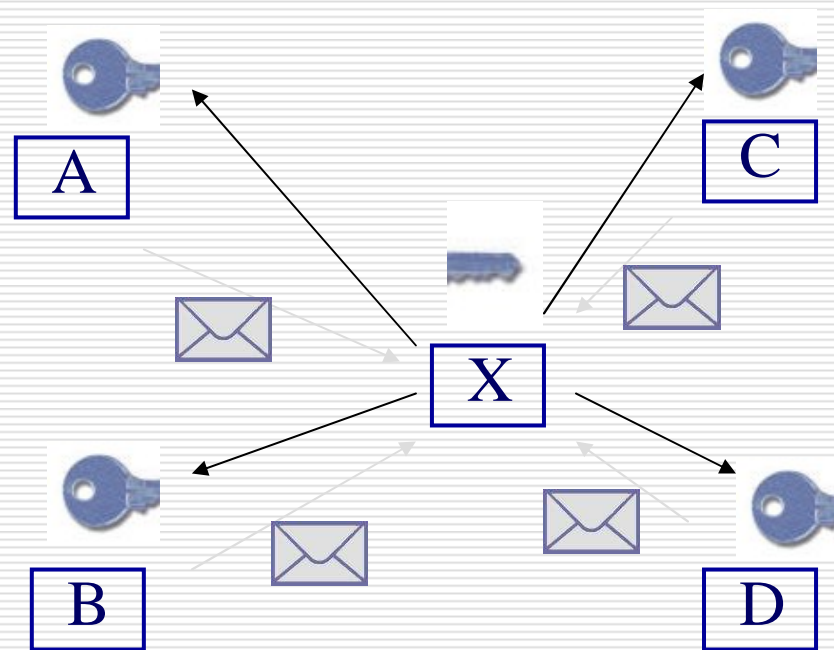


Crittografia classica: problemi

- ❑ La chiave va trasmessa attraverso metodi non crittografici (trasmissione protetta da possibili intercettazioni oppure attraverso un corriere fidato)

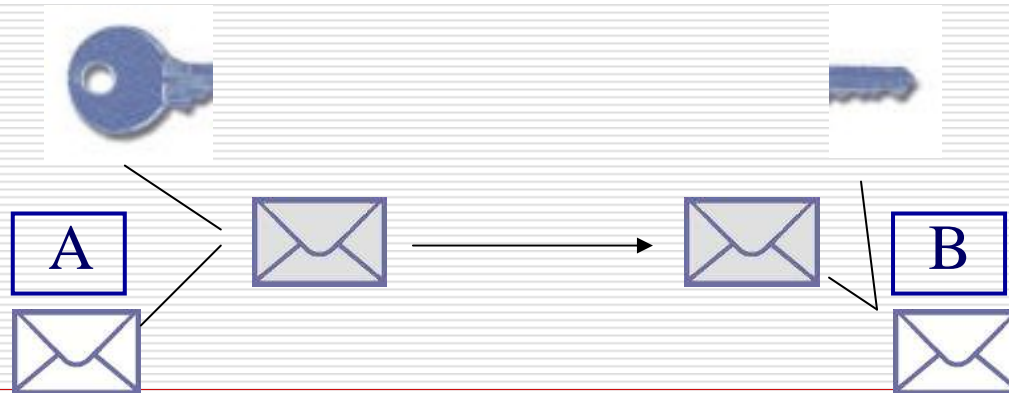


La crittografia public key



La crittografia public key

- ❑ Ogni partecipante dispone di una chiave pubblica e di una chiave privata.
- ❑ Quindi si parla di metodi asimmetrici.



La crittografia public key

- ❑ Ogni partecipante pubblica la sua chiave pubblica.
 - ❑ A usa la chiave pubblica di B per la cifratura di un messaggio per B.
 - ❑ B è in grado di decifrare questo messaggio con la sua chiave privata.
-

La crittografia public key

- ❑ Il problema consisteva nell'individuare metodi matematici appropriati.
 - ❑ La decifrazione deve essere inversa alla cifratura.
 - ❑ Ciò nonostante la chiave pubblica usata per la cifratura non deve permettere di decifrare il messaggio.
-

Il metodo RSA

- ❑ Fu inventato nel 1978 da R. Rivest, A. Shamir e L. Adleman.
 - ❑ La prima implementazione della crittografia public key.
 - ❑ Si basa sull'aritmetica congruenziale e sulla teoria dei campi.
-

L'aritmetica congruenziale

- $10 \text{ MOD } 3 = 1$
 $13 \text{ MOD } 3 = 1$
 - Il risultato dell'operatore MOD è il resto della divisione.
 - Vantaggi:
 - I numeri non superano un limite dato dal n in $x \text{ MOD } n$
 - Il valore finale non rivela il valore iniziale ($1 = \text{ sia } 10 \text{ MOD } 3 \text{ sia } 13 \text{ MOD } 3$)
-

Il metodo RSA

- ❑ A invia un messaggio a B.
 - ❑ B sceglie due numeri primi molto grandi P e Q .
 - ❑ B calcola i valori $N = P * Q$ e $\Phi(N) = (P-1)*(Q-1)$.
 - ❑ B sceglie un numero E che non abbia fattori primi in comune con $\Phi(N)$.
-

Il metodo RSA

- B calcola un numero D , tale che $D * E \text{ MOD } \Phi(N) = 1$.
 - Dunque la chiave è costituita dalle variabili $P, Q, N, \Phi(N), E, D$
-

Il metodo RSA

- Per adottare questi metodi numerici è necessario trasformare il testo in chiaro in numeri (p.e. codice di ASCII - vedi sotto)

ASCII-Zeichensatz										
+	0	1	2	3	4	5	6	7	8	9
30			!	"	#	\$	%	&	'	
40	()	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[\]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{		}	~			

Il metodo RSA

- Dal testo chiaro T si ottiene il testo cifrato con l'operazione
$$C = (T^E) \text{ MOD } N$$
 - Il testo decifrato si ottiene così:
$$R = (C^D) \text{ MOD } N$$
 - Si può dimostrare che queste due operazioni siano inverse (Eulero)
-

Il metodo RSA

- ❑ Siccome le variabili N e E sono necessarie per la cifratura, esse vanno rese pubbliche come chiave pubblica.
 - ❑ Le variabili D , P , Q e $\Phi(N)$ invece sono necessarie per la decifrazione e quindi non devono essere pubblicate!
-

Il metodo RSA: un esempio

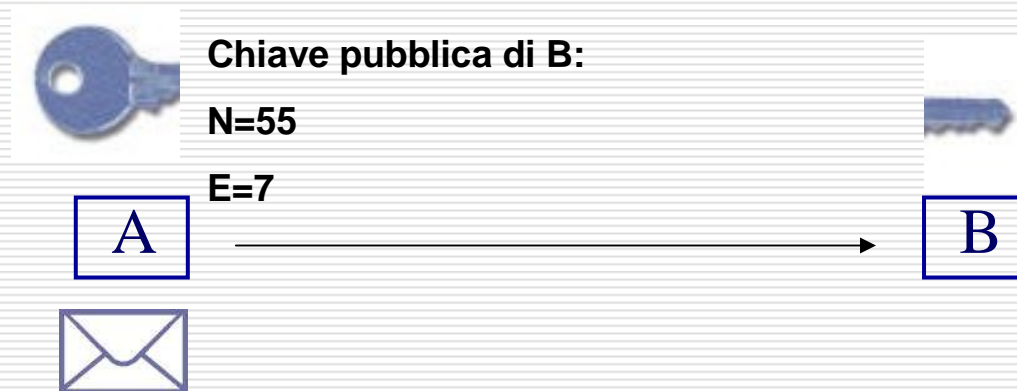
- A vuole trasmettere il messaggio "OK" a B.



- B sceglie due numeri primi $P=5$ e $Q=11$.
 - B calcola i valori $N=P*Q=55$ e $\Phi(N)=(N-1)*(Q-1)=40$.
-

Il metodo RSA: un esempio

- B sceglie un valore $E = 7$ che non ha fattori primi in comune con $\Phi(N)$.



Il metodo RSA: un esempio

- B calcola D tale che
 $D * E \text{ MOD } \Phi(N) = 1.$

$$D=1? \rightarrow 1 * 7 \text{ MOD } 40 = 7 \rightarrow \text{NO}$$

$$D=2? \rightarrow 2 * 7 \text{ MOD } 40 = 14 \rightarrow \text{NO}$$

...

$$D=22? \rightarrow 22 * 7 \text{ MOD } 40 = 34 \rightarrow \text{NO}$$

$$D=23? \rightarrow 23 * 7 \text{ MOD } 40 = 1 \rightarrow \text{SÌ}$$

- $D = 23$
-

Il metodo RSA: un esempio

- Perché A possa inviare un messaggio a B, B pubblica la chiave pubblica $N = 55$ e $E = 7$.
 - A trasforma il messaggio "OK" nei valori numerici 15 11 (posizione nel alfabeto).
-

Il metodo RSA: un esempio

- A calcola il valore cifrato:

$$C1 = 15^7 \text{ MOD } 55 = 5$$

$$C2 = 11^7 \text{ MOD } 55 = 11$$



Il metodo RSA: un esempio

- A invia a B il testo cifrato (5,11).
- B decifra il messaggio con la sua chiave privata (P,Q, $\Phi(N)$,D) calcolando.

$$R1 = 5^{23} \text{ MOD } 55 = 15$$

$$R2 = 11^{23} \text{ MOD } 55 = 11$$

Il metodo RSA: un esempio

- Assegnando lettere ai valori numerici, B ottiene il messaggio "OK".
-

Il metodo RSA: un esempio

- Come un osservatore avrebbe potuto decifrare il messaggio conoscendo la chiave pubblica di B?
 - Deve calcolare la chiave privata di B analizzando i fattori primi P e Q per cui vale $P * Q = 55$.
-> $P * Q = 5 * 11 = 55$
-

Il metodo RSA: un esempio

- $\Phi(N) = (P-1)*(Q-1) = 4*10 = 40$
 - Manca ancora D con
$$(D * E) \text{ MOD } \Phi(N) = 1$$
$$(D * 7) \text{ MOD } 40 = 1$$
$$D = 23 \text{ (vedi sopra)}$$
 - Adesso è in grado di decifrare il messaggio:
$$R1 = 5^{23} \text{ MOD } 55 = 15 \text{ (-> O)}$$
$$R2 = 11^{23} \text{ MOD } 55 = 11 \text{ (-> K)}$$
-

Il metodo RSA: un esempio

- ❑ Perché era così facile calcolare la chiave privata?



- ❑ Perché i numeri primi erano molto piccoli.
 - ❑ Gli inventori del RSA raccomandano numeri primi maggiori a 10^{100} !
-

Il metodo RSA: un secondo esempio

- Un cracker legge il messaggio (174; 887) e conosce la chiave pubblica costituita da $N = 1271$ ed $E = 343$.
- Come può decifrare il messaggio?



Il metodo RSA: un secondo esempio

- ❑ Trova dapprima i due numeri primi per cui vale $P * Q = N = 1271$.
Ottiene $P = 31$ e $Q = 41$.
 - ❑ Calcola $\Phi(N) = (P-1)*(Q-1)=1200$.
 - ❑ Trova un D per cui vale $D * E \text{ MOD } \Phi(N) = 1$.
Ottiene $D = 7$.
-

Il metodo RSA: un secondo esempio

- Adesso è in grado di decifrare il messaggio:

$$174 ^ 7 \text{ MOD } 1271 = 100$$

$$887 ^ 7 \text{ MOD } 1271 = 7$$

Il metodo RSA: vantaggi

- ❑ Metodo sicuro per $N > 10^{100}$.
 - ❑ Al contrario della crittografia public key, il destinatario non è obbligato a trasferire la chiave che permette di decifrare il codice cifrato.
-

Il metodo RSA: svantaggio

- ❑ Lentezza della codifica (calcolo della potenza)



Il metodo AES (Advanced Encryption Standard)

- ❑ È stato sviluppato nel 1999 dai belgi Joan Daemen e Vincent Rijmen.
 - ❑ È diventato il metodo standard dopo aver vinto un concorso contro sistemi di IBM, della Deutsche Telekom e. al. nel 2001.
 - ❑ Costituisce il successore dell'anziano DES.
-

Il metodo AES

- ❑ Utilizza la crittografia private key (metodo simmetrico).
 - ❑ È molto più veloce del RSA (più di 1000x)
-

Lo standard sul Web: PGP

- Il programma di crittografia più diffuso per applicazioni Web è PGP (Pretty Good Privacy) e si basa sulla tecnologia di RSA e su un metodo di crittografia privata.
-

Lo standard sul Web: PGP

- Utilizza il metodo RSA (crittografia public key) per la trasmissione della chiave e un metodo private key per la trasmissione dei messaggi.



- Tanto sicuro come RSA!
 - Molto più veloce!
-