

IL PROBLEMA dello SCAMBIO delle CHIAVI

N utenti vogliono comunicare tra loro su un canale condiviso

(i) Una chiave per ogni coppia di utenti, ognuno memorizza $N-1$ chiavi diverse e le condivide con un altro

(ii) Si ricorre a un trusted 3rd party (TTP), ogni utente genera una chiave per comunicare con TTP che gestisce la creazione delle chiavi

esempio, $A \rightarrow \text{TTP}$: "voglio comunicare con B"

TTP genera K_{AB}

$\text{TTP} \rightarrow A : c_A := (K_{AB}, K_A)$

$\text{TTP} \rightarrow B : c_B := (K_{AB}, K_B)$

$A \rightarrow B : c_B$

A, B possono comunicare

usando K_{AB}

due problemi: - TTP conosce ogni chiave

- TTP deve essere sempre online

Ha senso in ambienti ristretti

CIFRARI A CHIAVE PUBBLICA (ASIMMETRICI)

Prende l'uso di due chiavi

per cifrare K_{pub} e' pubblica

decifrare K_{priv} privata

Servono $2 \cdot N$ chiavi

$$C := C(m, K_{\text{pub}})$$

$$C, K_{\text{pub}} \text{ nota}$$

$$m := D(C, K_{\text{priv}})$$

$$D \text{ nota}$$

E' asimmetrico perché mittente e destinatario hanno ruoli diversi

si usa per lo scambio delle chiavi,

e' basata sulla teoria dei numeri e l'algebra

Requisiti:

- $\forall m, D(C(m, K_{\text{pub}}), K_{\text{priv}}) = m$

correttezza del procedimento di cifratura

e decifrato

- La coppia di chiavi deve essere facile da generare e devono essere casuali
- L'operazione di cifratura deve essere facile conoscendo K_{priv}
- L'operazione di decifrato deve essere difficile senza conoscere K_{priv}

La funzione di cifratura deve essere una one way trapdoor

RSA

Si basa sulla moltiplicazione di due numeri primi p, q

- Calcolare $n = p \cdot q$ e' facile

$$\mathcal{O}(n^2)$$

- Fattorizzare n senza conoscere né p né q e' difficile (subesponentiale)

- Trap door: se si conosce uno dei fattori, ricostruire l'altro e' facile

Cifrario di ELGAMAL Basato sul calcolo del logaritmo discreto

RICHIAMI di ALGEBRA MODULARE

\mathbb{Z}_n insieme degli interi da 0 a $n-1$

\mathbb{Z}_n^* insieme degli elementi di \mathbb{Z}_n coprimi con n

Phi di Eulero $\phi(n) = \#\mathbb{Z}_n^*$

n primo: $\phi(n) = n-1$

composto: $= n(1 - 1/p_1) \dots (1 - 1/p_k)$

semiprimo: $=(p-1)(q-1)$

Se n non e' primo \mathbb{Z}_n^* e' computazionalmente difficile da calcolare

TEOREMA di EULERO $n > 1$, Ha con $\text{mcd}(a, n) = 1$.

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

COROLARIO

Piccolo teorema di FERMAT n primo, Ha $a^n \equiv a \pmod{n}$.

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

Calcolo dell'inverso in modulo Per ogni a primo con n .

$$a^{-1} = a^{\phi(n)-1} \pmod{n}$$

TEOREMA $ax \equiv b \pmod{n}$ risolvibile $\Leftrightarrow \text{mcd}(a, n) \mid b$

con $\text{mcd}(a, n)$ soluzioni distinte

$ax \equiv 1 \pmod{n}$ ha una e una sola soluzione se

$$\begin{aligned} \text{mcd}(a, n) &= 1 \\ \Updownarrow \\ \exists a^{-1} &\text{ inverso di } a \end{aligned}$$

$$a^{-1} = a^{\phi(n)-1} \pmod{n}$$

E' difficile, si puo' usare

Euclide esteso

Risolve $ax + by = \text{mcd}(a, b)$ identita' di Bézout

Euclide Esteso (a, b) :

if ($b=0$) then return $(a, 1, 0)$;

$(d', x', y') = \text{EuclideEsteso}(b, a \pmod{b})$;

$(d, x, y) = (d', g', x' - \text{floor}(a/b) \cdot g')$;

return (d, x, y) ;

$$ax \equiv 1 \pmod{b}$$

$$\Leftrightarrow ax = b\alpha + 1$$

$$\Leftrightarrow ax + by = \text{mcd}(a, b) \text{ con } y = -\alpha \cdot \text{mcd}(a, b)^{-1}$$

α e' il valore dell'inverso

e' il secondo valore della tripla

Esempio : $a = 5^{-1} (132)$

$$5x + 132y = 1$$

$$\text{EE}(5, 132)$$

$$x = 53$$



$$(1, 53, \dots)$$



$$\text{EE}(132, 5)$$

$$(1, -2, 1+2 \cdot 26)$$



$$\text{EE}(5, 2)$$

$$(1, 1, 0-1 \cdot 2)$$



$$\text{EE}(2, 1)$$

$$(1, 0, 1-0 \cdot 2)$$



$$\text{EE}(1, 0) \rightarrow (1, 1, 0)$$

TEOREMA CINESE DEL RESTO n_1, \dots, n_k a due a due coprimi.

Comunque si scelgano interi a_1, \dots, a_k

esiste una unica x soluzione

del sistema

$$x \equiv a_1 \pmod{n_1}$$

:

$$x \equiv a_k \pmod{n_k}$$

$$\text{modulo } n := \prod_{i=1}^k n_i$$

GENERATORE $a \in \mathbb{Z}_n^*$ e' generatore di \mathbb{Z}_n^* se
 $a^k \pmod n$ con $1 \leq k \leq \phi(n)$ genera tutti gli
elementi di \mathbb{Z}_n^* .

Per il teorema di Eulero, si viene
generato solo se $k = \phi(n)$.

Se n e' primo allora \mathbb{Z}_n^* ammette almeno un generatore
(ne ammette $\phi(n-1)$).

Trovare un generatore di \mathbb{Z}_n^* con n primo e' difficile
Risolvere nell'incognito x $a^x \equiv b \pmod n$ e' difficile
(logaritmo discreto)