

CRITTOGRAFIA

lezione di lunedì

23 novembre

ore 11:15



ECC: Scambio di messaggi cifrati

$m \rightarrow P_m$ punto di una curva prma $E_p(a, b)$

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

$x \leftarrow m$

$$\text{Prob} (m^3 + am + b \text{ è un R.Q}) \approx \frac{1}{2}$$

ALGORITMO DI Koblitz pd. -randomizzato

$$m < p \rightarrow P_m \in E_p(a, b)$$

si sceglie h intero t.c. $(m+1)h < p$

$$x = m \cdot h + i \quad 0 \leq i < h$$

$\left\{ \begin{array}{l} h \\ \text{tentativi} \end{array} \right.$

KOBUTZ(m, h, a, b, p) // $(m+1) \cdot h < p$

for ($i=0$; $i < h$; $i++$) {

$$x = mh + i$$

$$z = (x^3 + ax + b) \bmod p$$

if (z è un residuo quadratico) {

$$y = \sqrt{z}$$

$$\text{return } P_m = (x, y)$$

} Corso -
polinomiale

y

$i \in [0, h-1]$

}

return "fallire";

$$\text{Prob. di fallimento} \simeq \left(\frac{1}{2}\right)^h$$

$$\text{Prob. di successo :} \simeq 1 - \left(\frac{1}{2}\right)^h$$

Per risolvere a m da x:

$$\left\lfloor \frac{x}{h} \right\rfloor = \left\lfloor \frac{mh+i}{h} \right\rfloor =$$

$$= \left\lfloor m + \underbrace{\frac{i}{h}}_{<1} \right\rfloor = m$$

Scomba di messaggi

$E_p(a, b)$

B di ordine elevato n

$B \in E_p(a, b)$

h: per alg. koblitz

ogni utente genera $k(\text{pub}), k(\text{priv})$

\cup chiave privata: $n_v < n \leftarrow k(\text{priv})$

chiave pubblica: $P_v = n_v B \leftarrow k(\text{pub})$

Alice (mittente del messaggio)

- m
- mappa m su $P_m \in E_p(a, b)$ (Alg. koblitz)
- sceglie un intero casuale r e calcola $V = r B$

$$W = P_m + r P_{\text{Bob}}$$

choose private
choice pubblica di Bob

$E_p(a, b)$, B ,
 h sono pubblici

$r P_{\text{Bob}}$ → punto "scelto a caso" su $E_p(a, b)$

numero casuale

- invia a Bob $\langle V, W \rangle$

Bob (destinatario)

- riceve $\langle V, W \rangle$ da Alice.

- decifra: $W - n \underset{\text{Bob}}{V} = (P_m + r P_{\text{Bob}}) - n \underset{\text{Bob}}{V} = P_m + r n \underset{\text{Bob}}{B} - n r \underset{\text{Bob}}{B}$

- trasforma P_m in $m =$
 choose private

Bob decifra e riceve

$$P_m = (x, y)$$

calcola m :

$$m = \left[\frac{x}{h} \right]$$

$$m = \left[\frac{x}{h} \right]$$

Sicurezza

bomba nelle difficoltà del Log. discr.
su curve ellittiche

Eve: ~~P_{Bob}~~

→ se trova r , decifr:

$$W - r P_{Bob} = (P_m + r P_{Bob}) - r P_{Bob}$$

$$= P_m$$

per trovare r da $V \in B$

$$V = r B \rightarrow \text{log. discreto}$$

→ deve trovare n_{Bob} da P_{Bob}, B

$$P_{Bob} = n_{Bob} B \rightarrow \text{log di svolto}$$

Sicurezza

× obbligare RSA, DH, El Gamal (algebra modulare)

algoritmi di costo

$$\mathcal{O}(2^{\sqrt{b \log b}})$$

{ index
calcolare

b = #bit del modulo

× obbligare protocolli su CT (log. discreta)

$$\mathcal{O}(2^{b/2})$$

b = #bit dell'ordine di B