

# CRITTOGRAFIA

---

lezione di

lunedì 16, ore 11:15

- DH
- El Gamal
- ECC

---

---

---

---



Cifra con la chiave pubblica  $\rightarrow$  per lo scambio delle chiavi

### CIFRARI IBRIDI

Alice

RSA + AES

Bob

Alice

- sceglie una chiave per AES  $k_{\text{session}}$
- la cifra con la chiave pubblica RSA di Bob
- cifra il messaggio con  $k_{\text{session}}$
- invia i due ciphogrammi a Bob

$\left< \underset{\text{RSA}}{G(k_{\text{session}})}, \underset{\text{Bob}}{k_{\text{pub}}}, \underset{\text{AES}}{G(m, k_{\text{session}})} \right>$

Bob: decifra il primo ciphogramma con  $k_{\text{Bob}}(\text{priv})$ , ha  $k_{\text{session}}$  e decifra il 2° ciphogramma

## Protocollo Diffie Hellman

- Alice e Bob si accordano pubblicamente su un numero primo  $P$  molto grande, e su un generatore  $g$  di  $\mathbb{Z}_P^*$

$$\mathbb{Z}_P^* = \{1, 2, \dots, P-1\}$$

$$= \{g^k \bmod P, \quad 1 \leq k \leq P-1\}$$

$\exists g$  perché  $P$  è primo

~~pero~~ (Alice e Bob possono anche scegliere di usare una coppia  $\langle P, g \rangle$  già disponibile)

Alice

- sceglie  $x$  così  
 $1 < x < p-1$

(intero positivo)

e calcola

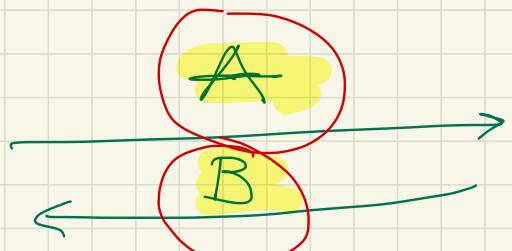
$$A = g^x \bmod p$$

- ~~B~~ Riceve  $B$  da ~~Bob~~ e calcola

$$k(\text{session}) = B^x \bmod p$$

$$= g^{xy} \bmod p$$

$\langle g, P \rangle$



Bob

- sceglie  $y$  così  
 $1 < y < p-1$

(intero positivo)

e calcola

$$B = g^y \bmod p$$

- Riceve  $A$  da Alice  
e calcola

$$k(\text{session}) = A^y \bmod p$$

$$= g^{xy} \bmod p$$

ATTACCHI

otto chiavi possibili



il crittoanalista conosce  $p, g, A, B$

per calcolare  $k$  (session) deve trovare  $x, o y$

$$\begin{aligned} A &= g^x \bmod p \\ B &= g^y \bmod p \end{aligned} \quad \left. \begin{array}{l} \text{logaritmo discreto} \\ \text{(difficile quanto la} \\ \text{fattorizzazione)} \end{array} \right.$$

DH è ~~vulnerabile~~ vulnerabile agli otto chiavi ottime  
"man-in-the-middle"

Alice

$$A = g^x \bmod p$$

Eve.  $g, p$

sottrare A  
B dal  
Console, e  
li sostituirsi con

$$E = g^z \bmod p$$

$$1 < z < p-1$$

$\leftarrow E$

$$k_A = E^x \bmod p = g^{xz} \bmod p$$

Bob

$$B = g^y \bmod p$$

$\rightarrow E$

$$K_B = E^y \bmod p = g^{yz} \bmod p$$

Conosce  $k_A$

$$k_A = A^z \bmod p$$

$$= g^{xz} \bmod p$$

so

$$k_B = B^z \bmod p$$

$$= g^{zy} \bmod p$$

$$k_A \neq k_B$$

## CIFRARIO A EL GAMAL

(logaritmo discreto)

Alice

$\xrightarrow{m}$

Bob

Bob

- sceglie  $p$ , numero primo molto grande, e  $g$ ; generatore per  $\mathbb{Z}_p^*$

- sceglie  $2 \leq x \leq p-2$

CHIAVE PRIVATA

$$k(\text{priv}) = \langle x \rangle$$

- calcola  $y = g^x \bmod p$

- pubblica  $k(\text{pub}) = \langle p, g, y \rangle$

Alice

$$0 \leq m < p$$

Alice

- si procede  $k(\text{pub}) = \langle g^r, y \rangle$
- sceglie a caso  $2 \leq r \leq p-2$  (numero degrado)  
e calcola

$$c = g^r \pmod{p}$$

- calcola  $d = m \cdot y^r \pmod{p}$
- invia a Bob la coppia  $\langle c, d \rangle$

Bob:

riceve  $\langle c, d \rangle$  e decifra:

$$m = \frac{d}{c^x} \pmod{p} = d \cdot (c^x)^{-1} \pmod{p}$$

$c^x \rightarrow$  chiave privata di Bob

(- : moltiplicazione  
per l'inverso)

CORRETTEZZA :

$$\frac{d}{c^x} \bmod p = \frac{y^r \cdot m}{c^x} \bmod p = \frac{\cancel{y}^r \cdot m}{(\cancel{y^r})^x} \bmod p$$

$= m \bmod p = m$   
 $m < p$

EVE : Conosce  $p, g, y, c, d$   
(tutto tranne  $r \in \mathbb{Z}$ )

se conosce  $x \rightarrow$  calcola  $m = \frac{d}{c^x} \bmod p$

se conosce  $r \rightarrow$   $m = \frac{d}{y^r} \bmod p = \frac{m \cdot y^r}{y^r} \bmod p = m$

# ECC : elliptic curve cryptography

AES	RSA, DH, El Gamal	ECC
128 bit	3072 bit di n di p $\approx 15\ 000$ bit	256 bit
256 bit		512 bit

~~as~~ Curve ellittiche

1985

Miller (IBM)  
Koblitz (Univ. ~~of~~ of Washington)

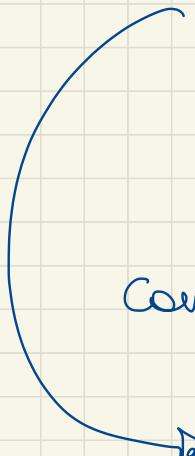
## Curva ellittica: definizione generale

campo  $k$

insieme di punti  $(x, y) \in k^2$  t.c.

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

$$a, b, c, d, e \in k$$



Caratteristica di  $k \neq 2, 3$

forma normale di  
Weierstrass

$$y^2 = x^3 + ax + b$$

$$a, b \in k$$

$$E(a, b) = \{ (x, y) \in k^2 \mid y^2 = x^3 + ax + b \} \cup \overline{\text{punto all'infinito, elementi neutri}}$$

$k = \mathbb{R}$

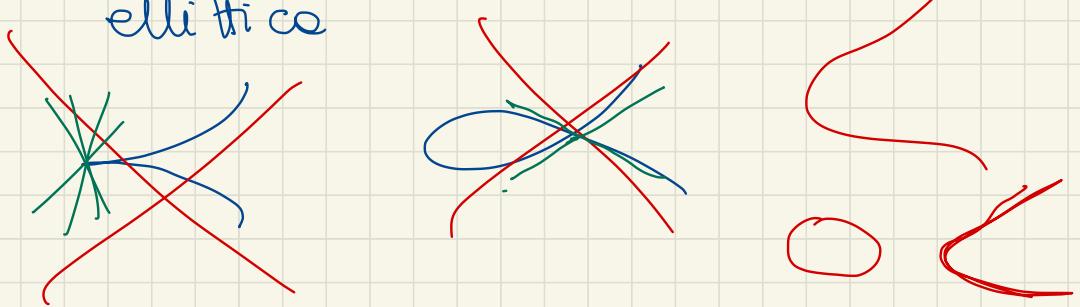
$$E(0, b) = \{ (x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + bx + b \} \cup \{0\}$$

Assumiamo dc

$$4a^3 + 27b^2 \neq 0$$

(~~in questo caso~~  $x^3 + bx + b$  non ha radici multiple)

↓  
garantisce l'esistenza delle tangente in ogni punto della ~~curva~~ curva ellittica



## Simmetria orizzontale

$$P = (x, y) \in E(0, b)$$

$$y^2 = \cancel{x^3} + bx + b$$

$\Rightarrow$  onde il punto  $-P = (x, -y) \in E(0, b)$

infatti

$$(-y)^2 = y^2 = x^3 + bx + b$$

si pone

$$-O = O$$

$$O = -O$$