Cifratura Ibrida

A genera k (256 bit)

$A \xrightarrow{C_{RSA}(k,\, k_{pub\,B})} B$

B può decifrare con $k_{priv\,B}$

B trova k

$A \xrightarrow{C_{AES}(m,k)} B$ B può decifrare e ricavare m

Protocollo Diffie Hellman

A,B scelgono p numero primo molto grande

$A \xleftrightarrow{p} B$

A,B scelgono un generatore g per $\mathbb{Z}_p^*$

$A \xleftrightarrow{g} B$

A sceglie $a \in \mathbb{Z}^+$. $a \in]1; p-1[$

A calcola $A = g^a \bmod p$

$A \xrightarrow{A} B$

B sceglie $b \in \mathbb{Z}^+$. $b \in]1; p-1[$

B calcola $B = g^b \bmod p$

$A \xleftarrow{B} B$

A calcola $k = B^a \bmod p = g^{b \cdot a} \bmod p$

B calcola $k = A^b \bmod p = g^{b \cdot a} \bmod p$

E deve risolvere il logaritmo discreto per trovare la chiave

Si distinguono:

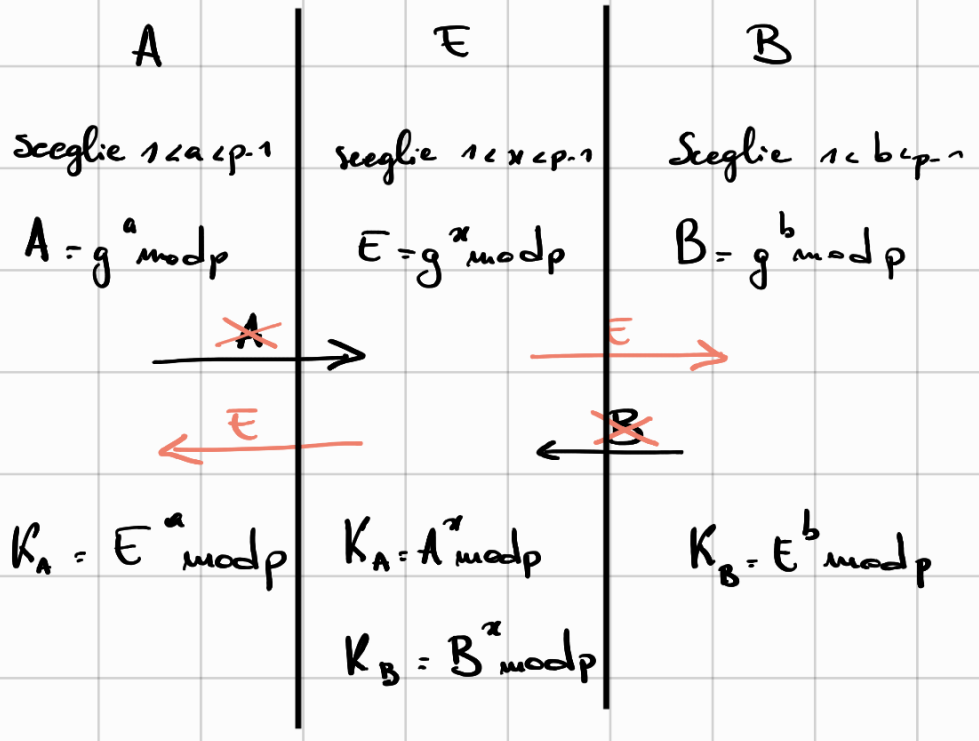
attacchi <u>passivi</u>: E conosce p. g. A, B

per calcolare k deve trovare a o b

$a = \log_g A$. $b = \log_g B$

è un problema difficile: usa il logaritmo discreto

<u>attivi</u>: è vulnerabile agli attacchi man in the middle



Se E resta attivo sul canale può intervenire decifrando e cifrando tutti i messaggi

CIFRARIO di ELGAMAL

1. Scelgo p primo e g generatore per $\mathbb{Z}_p^*$
2. Scelgo un intero casuale $x \in [2; p-2]$

3. Calcolo $y = g^x \bmod p$

$K_{pub} = (p, g, y)$

$K_{priv} = x$

CIFRATURA m è codificato come una sequenza binaria, $m < p$

Il mittente sceglie $r \in [2; p-2]$

Calcola $c = g^r \bmod p$, $d = m y^r \bmod p$

DECIFRAZIONE $m = c^{-x} \cdot d \bmod p$

Dim: $d \cdot c^{-x} \quad (p) =$

$= m \cdot y^r \cdot c^{-x} \quad (p) =$

$= m y^r \cdot (g^r)^{-x} \quad (p) =$

$= m \cdot (g^r)^x \cdot (g^r)^{-x} \quad (p) =$

$= m \bmod p = m.$

È può attaccare:

indovinando r: $d = y^r \cdot m \bmod p$

$m = d \cdot y^{-r} \bmod p$

forza bruta su x.

Cosa succede se si riusa r?

m_1, m_2 usano lo stesso r

$m_1 : (c = g^r \bmod p, d_1 = y^r m_1 \bmod p)$

$m_2 : (c = g^r \bmod p, d_2 = y^r m_2 \bmod p)$

E viene a conoscenza di m_1:

E calcola $y^r = d_1 \cdot m_1^{-1} \pmod p$

$m_2 = d_2 \cdot (y^r)^{-1} \pmod p$ si calcola in tempo polinomiale

CRITTOGRAFIA SU CURVE ELLITTICHE

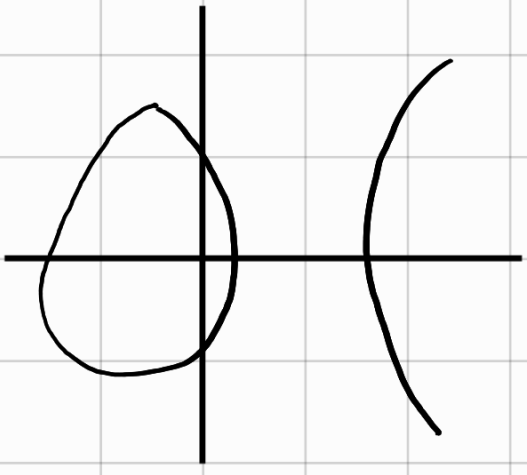
$$E(a,b,c,d,e) = \{(x,y) \in \mathbb{K}^2 : y^2 + axy + by = x^3 + cx^2 + dx + e\} \cup \{O\}$$

con $\mathbb{K}$ campo, $a,b,c,d,e \in \mathbb{K}$,

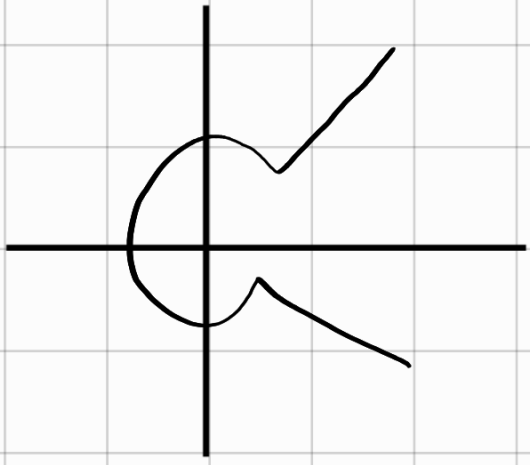
O punto a infinito (elemento neutro per l'addizione)

Se $\text{char}(\mathbb{K}) \neq 2$ e $\text{char}(\mathbb{K}) \neq 3$ allora si può scrivere in forma normale di Weierstrass

$$E(a,b) = \{(x,y) : \mathbb{K}^2 : y^2 = x^3 + ax + b\}$$



tre radici reali



una radice reale, due complesse coniugate

Per le applicazioni crittografiche si assume

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

- altrimenti che il polinomio cubico non abbia radici multiple
- la curva sia priva di cuspidi o nodi dove la tangente non sarebbe univoca

Presentano simmetria orizzontale

Sia $P := (x, y)$, definisco $-P = (x, -y)$; $-P$ appartiene alla curva.

ovv. $-O := O$

Si definisce l'addizione:

ovv. una retta interseca una curva al più 3 volte

Dati 3 punti $P, Q, R \in E$, se P, Q, R sono allineati allora vale che $P + Q + R = O$