

APPROFONDIMENTO: CRITTOGRAFIA ELLITICA

Problema generale: trasmettere un messaggio da Alice a Bob evitando che un terzo, eve, si intrometta.
Il messaggio è crittografato da una linea crittografica. Se nopo di eve i rischia alle diverse.

CRITTI: SIA CHE ALICE E BOB CONDIVIDANO LA CHIAVE (UNICA) CHE È IN grado DI DESCRIFARE IL MESSAGGIO. ES. AES
PROBLEMA: Prendere保障 la linea crittografica sicura e mantenuta regola.

CRITTI ASIMMETRICO: ALICE E BOB CONDIVIDONO DUE CHIAVI:

- 1) UNA CHIAVE PUBBLICA UTILIZZATA PER DESCRIFARE;
- 2) UNA CHIAVE PRIVATA UTILIZZATA PER ENTRIFARE.

ESEMPIO: ELGAMAL

PROBLEMA: gli algoritmi sono molto più complessi

ALGORITMO ELGAMAL

- 1) Bob sceglie la chiave pubblica indicata con:

$$(G, q, g, h)$$

gruppo \downarrow generatore di G \rightarrow elemento di $G \rightarrow \{1, \dots, q\}$ in g
 \rightarrow elementi di g

CASUALE

La $(*)$ non viene comunicata. Il problema è che per inserire a^{-1} all'interno di un gruppo è molto complicato e richiede molta computazione.

- 2) Alice cifra il messaggio con la chiave pubblica di Bob. Per fare ciò Alice

- 1) Alice sceglie a caso $y \in \{1, \dots, q\}$
- 2) Alice calcola $c_1 = g^y$ e $c_2 = H \cdot h^y$
- 3) Alice manda (c_1, c_2) a Bob

Per decrittare l'affare H , Bob fa: $H \cdot c_2 \cdot (h^y)^{-1} = c_2 \cdot ((g^y)^{-1})^{-1} = c_2 \cdot ((g^y)^{-1})^{-1} = c_2 \cdot (c_1)^{-1} = c_2 \cdot c_1^{-1}$

perché c_1 è la chiave pubblica di Alice

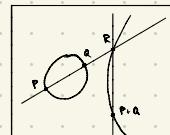
Tutto funziona se si prende G abbastanza grande \Rightarrow si sceglie il gruppo dei punti di una curva ellittica

CURVE ELLITTICHE

Una curva ellittica è una curva algebrica piana non singolare (non è auto-intersezione) descritta da $y^2 = x^3 + ax + b$ in un dato sistema di riferimento affine.

GRUPPO SU UNA CURVA

È possibile definire con operazioni sul insieme dei punti di una curva ellittica le stesse proprietà della struttura di gruppo: i associativo, commutativo, con un elemento neutro e con inverso.

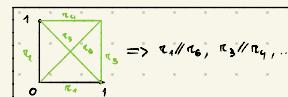


I punti che condividiamo li prendiamo con coordinate invece in modo da poter definire un campo su cui scrivere finito.

GEOMETRIA AFFINE SU CAMPO FINITO

Condividiamo $\mathbb{Z}_2 = \{0, 1\}, +, \cdot$ con $\begin{array}{c|cc|c} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ e $\begin{array}{c|cc|c} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$

Nello spazio $\mathbb{A}^2 = \{\mathbb{Z}_2^2, (\mathbb{Z}_2^2, \mathbb{Z}_2, +, \cdot), \Psi_V\}$ esistono 6 rette distinte:



Per poter far funzionare ELGAMAL dobbiamo scegliere una struttura più complessa, tipo $\mathbb{A}_{2,0}^2 = \{\mathbb{Z}_{2,0}, (\mathbb{Z}_{2,0}, \mathbb{Z}_{2,0}, +, \cdot), \Psi_V\}$. Su $\mathbb{A}_{2,0}^2$ definiamo la nostra curva ellittica e , e dopo aver scelto da i punti della curva ellittica formate un gruppo e usandolo per crittografare i messaggi. Ogni algoritmo ha il suo campo e la sua curva conosciuta a tutti.