Crittosistemi basati su logaritmi discreti

Trapdoor famose

La crittografia asimmetrica è stata introdotta negli anni Settanta grazie alla scoperta di trapdoor matematiche basate su due problemi principali (difficili):

- Difficoltà della fattorizzazione di grandi numeri interi
- Difficoltà del calcolo dei logaritmi discreti su grandi campi finiti.

Logaritmo discreto

- Dato un **primo** p e due interi non nulli (mod p) α e β tali che:

$$\beta \equiv \alpha^x \pmod{p}$$

- Il problema di trovare x è noto come **problema del logaritmo discreto**.

- Se n è il più piccolo intero positivo tale che $\alpha^n \equiv 1 \pmod{p}$, si ha $0 \leq x < n$ e possiamo scrivere:

$$x = L_\alpha(\beta)$$

- $L_\alpha(\beta)$ si dice logaritmo discreto di β in base α.

Logaritmo discreto (ctd.)

- L'esponenziazione modulare è quindi un esempio di funzione unidirezionale: è facile calcolare $\alpha^x \pmod p$ ma trovare x da $\beta \equiv \alpha^x \pmod p$ è difficile.

Scambio di chiave di Diffie-Hellman

- Whitfield Diffie e Martin Hellman nel 1976 hanno formulato la prima proposta di un crittosistema asimmetrico per lo scambio di una chiave segreta su un canale pubblico.

- La sua sicurezza si basa sulla difficoltà del calcolo dei logaritmi discreti.

W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976.

Scambio di chiave di Diffie-Hellman

HP: Ogni comunicazione tra Alice e Bob avviene su un canale pubblico.

1. Alice sceglie un primo grande e sicuro p e una radice primitiva α (mod p). I valori di p e α sono resi pubblici.

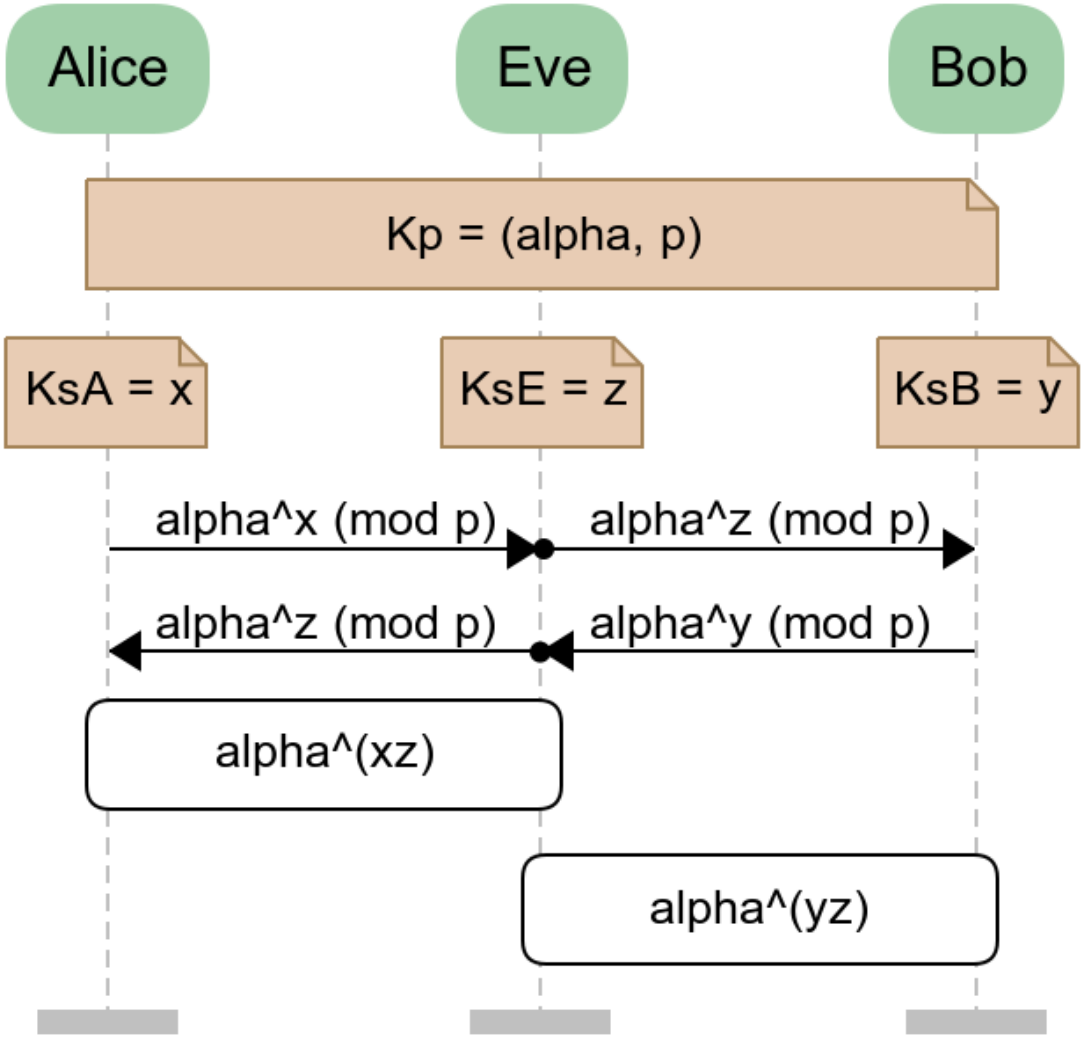
2. Alice sceglie casualmente x, with $1 \leq x \leq p - 2$, e Bob sceglie y, con $1 \leq y \leq p - 2$.

3. Alice manda $\alpha^x \pmod p$ a Bob e Bob manda $\alpha^y \pmod p$ a Alice.

4. Usando i messaggi ricevuti, possono calcolare entralbi la stessa chiave K: Alice $K \equiv (\alpha^y)^x \pmod p$ e Bob $K \equiv (\alpha^x)^y \pmod p$.

Man-in-the-middle (MITM) attacks

Attacco MITM contro Diffie-Hellman



Crittosistema di ElGamal

- Crittosistema asimmetrico proposto nel 1985 da Taher ElGamal.
- La sua sicurezza si basa sulla difficoltà di risolvere i logaritmi discreti.
- Insieme dei possibili testi in chiaro: numeri interi (mod p).
- Insieme dei possibili testi cifrati: coppie di numeri interi (r, t) (mod p).

Crittosistema di ElGamal – Generazione della chiave

- Bob sceglie un primo grande p e una radice primitiva α.
- Bob sceglie un intero segreto a e calcola $\beta \equiv \alpha^a \pmod{p}$

- Bob's **private key**: a
- Bob's **public key**: (p, α, β)

Crittosistema di ElGamal - cifratura

- Alice vuole mandare un messaggio $0 \leq m < p$ a Bob.
- Alice ottiene la chiave pubblica di Bob (p, α, β).
- Alice sceglie k e calcola:
  $r \equiv \alpha^k \pmod{p}$.
  $t \equiv \beta^k m \pmod{p}$.
- Il testo cifrato associato a m è (r, t).
- Va evitato $m = 0$

Crittosistema di ElGamal - decifratura

- Bob decifra (r, t) calcolando:

$$tr^{-a} \equiv \beta^k m\left(\alpha^k\right)^{-a} = \left(\alpha^a\right)^k m\alpha^{-ak} \equiv \alpha^{ak} m\alpha^{-ak} \equiv m \pmod{p}.$$