

logaritmo discreto

- sia G un gruppo ciclico di ordine n , sia g un generatore di G
- dato $y \neq 1 \in G$
- bisogna determinare l'unico intero x con $1 \leq x \leq n - 1$ tale che

$$g^x = y$$

- ex: in $U(\mathbb{Z}_9)$ con $g = 2$, se $y = 7$ si ha $x = 4$, perché $2^4 = 7$.
- l'intero x si chiama il **logaritmo discreto** di y in base g , e si denota con $\log_g y$
- ex: in $U(\mathbb{Z}_9)$, $4 = \log_2 7$

logaritmo discreto come funzione unidirezionale

- in generale, lavoreremo con il gruppo \mathbb{Z}_p^* o più in generale con \mathbb{F}_q^* , $q = p^m$, p primo
- dati g generatore di \mathbb{Z}_p^* e x tale che $1 \leq x \leq p - 1$, calcolare $y = g^x$ è computazionalmente facile
- ($y \equiv g^x \pmod{p}$) – si usa l'algoritmo square-and-multiply)
- si ritiene che, dati g generatore di \mathbb{Z}_p^* e $y \in \mathbb{Z}_p^*$, determinare $x = \log_g y$ sia difficile (sotto opportune ipotesi su p)
- in particolare, p dev'essere grande (2048 bit), $p \approx 2^{2047}$
- dati g e y posso trovare x tale che $g^x = y$ per tentativi – calcolando g^x per tutti gli x , $1 \leq x \leq p - 1$
- ma il numero di tentativi è enorme

cifratura RSA e logaritmo discreto

- nella cifratura RSA, la funzione è del tipo

$$x \longrightarrow x^e \pmod{N}$$

- nel problema del logaritmo discreto, la funzione è del tipo

$$x \longrightarrow g^x \pmod{p}$$

scambio della chiave di Diffie-Hellman

- Alice e Bob scelgono pubblicamente un primo p e un elemento primitivo $g \pmod{p}$
- Alice sceglie casualmente $a \in \{2, \dots, p-2\}$; calcola $g^a \pmod{p}$ e invia il risultato a Bob
- Bob sceglie casualmente $b \in \{2, \dots, p-2\}$; calcola $g^b \pmod{p}$ e invia il risultato a Alice
- Alice calcola $(g^b)^a \pmod{p}$
- Bob calcola $(g^a)^b \pmod{p}$
- la chiave è $k = g^{ab}$

crittosistema Elgamal (ca 1985)

- sia p un primo, g un elemento primitivo mod p
- $\mathcal{P} = \mathbb{Z}_p^*$
- $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
- Lo spazio delle chiavi è

$$\mathcal{K} = \{(p, g, a, \beta) \mid \beta \equiv g^a \pmod{p}\}.$$

- p , g e β sono la **chiave pubblica** – a è la **chiave privata**

crittosistema Elgamal

- **prima** di cifrare il messaggio $x \in \mathcal{P}$, Alice **sceglie un numero casuale (segreto) $h \in \{2, \dots, p-2\}$**
- $e_k(x, h) = (y_1, y_2)$
- con $y_1 = g^h$, $y_2 = x\beta^h \pmod{p}$
- Bob riceve $(y_1, y_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ – **non conosce h** ma conosce a
- calcola $y_1^a = (g^h)^a = (g^a)^h = \beta^h \pmod{p}$
- calcola $(\beta^h)^{-1} \pmod{p}$ e ottiene $x = y_2(\beta^h)^{-1}$
- $d_k((y_1, y_2)) = y_2(y_1^a)^{-1} \pmod{p}$
- notare la somiglianza con DH – non si inverte la funzione $x \rightarrow g^x \pmod{p}$
- Alice sceglie un nuovo h a ogni trasmissione (randomized encryption)

esempio

- Bob sceglie $p = 83$, $g = 2$ e la chiave privata $a = 30$
 - $\beta = 2^{30} \equiv 40 \pmod{83}$
 - la chiave pubblica di Bob è $(83, 2, 40)$
 - il messaggio di Alice è $x = 54$ – il numero scelto per la cifratura è $h = 13$
 - Alice invia $(g^h, x\beta^h) = (2^{13}, 54 \cdot 40^{13}) \equiv (58, 71) \pmod{83}$
 - per decifrare, Bob calcola $(g^h)^a = 58^{30} = 9$
 - l'inverso di $9 \pmod{83}$ è 37 – il messaggio è quindi $37 \cdot 71 = 54 \pmod{83}$
-
- la “cifratura” è una moltiplicazione: $x \rightarrow xg^{ha}$
 - si può invece usare un cifrario a blocchi (AES) e cifrare $x \rightarrow e_{g^{ha}}(x)$
 - anche per Elgamal, si usa p di almeno 2048 bit, $p - 1$ con un fattore primo grande e a fattorizzazione nota
 - anche per violare Elgamal, basta che Eve sappia risolvere il DH problem
 - se dati g^h e $\beta = g^a$ sa trovare $g^{ah} = \beta^h$, può leggere il messaggio
 - se Eve sa risolvere il logaritmo discreto può ricavare l'esponente h e quindi ricavare direttamente x
 - oppure ricavare a e decifrare come Alice (conviene – h cambia in ogni trasmissione)

in un gruppo ciclico arbitrario

- sia lo scambio della chiave di Diffie-Hellman che il crittosistema di Elgamal possono essere implementati utilizzando un **gruppo ciclico arbitrario**
- per esempio, il gruppo moltiplicativo di un campo finito, $\mathbb{F}_{p^m}^*$, in particolare con $p = 2$
- o il gruppo di una curva ellittica su un campo finito (un suo sottogruppo ciclico)

crittosistema Elgamal

- G un gruppo ciclico di ordine n moltiplicativo, g un generatore
- $\mathcal{P} = G$; $\mathcal{C} = G \times G$
- Lo spazio delle chiavi è $\mathcal{K} = \{(G, g, a, \beta) \mid \beta = g^a\}$.
- G, g e β sono la **chiave pubblica** – a è la **chiave privata**
- **prima** di cifrare il messaggio $x \in G$, Alice **sceglie un numero casuale (segreto) $h \in \{2, \dots, n-1\}$**
- $e_k(x, h) = (y_1, y_2)$
- con $y_1 = g^h$, $y_2 = x\beta^h$
- Bob riceve $(y_1, y_2) \in G \times G$ – **non conosce h** ma conosce a
- calcola $y_1^a = (g^h)^a = (g^a)^h = \beta^h$
- calcola $(\beta^h)^{-1}$ e ottiene $x = y_2(\beta^h)^{-1}$
- $d_k((y_1, y_2)) = y_2(y_1^a)^{-1}$
- Alice sceglie un nuovo h a ogni trasmissione (randomized encryption)