gruppi ciclici

- Definizione
  Un gruppo G con n elementi tale esiste un elemento $g \in G$ con $o(g) = n$ si dice ciclico, e g si dice un generatore del gruppo
  - $U(\mathbb{Z}_9)$ è ciclico – p. es. $U(\mathbb{Z}_8)$ non lo è
  - i gruppi $U(\mathbb{Z}_p)$, p primo, sono gruppi ciclici
  - se $\mathbb{F}_{p^m}$ è un campo finito, il gruppo moltiplicativo $(\mathbb{F}_{p^m} - \{0\}, \cdot)$ è un gruppo ciclico
  - in questi due esempi, i generatori si chiamano radici primitive, o elementi primitivi

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 devessere 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

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

protocollo di scambio della chiave

- Alice e Bob non condividono informazioni segrete
- eseguono un protocollo, e alla fine hanno la stessa chiave
- Eve ascolta la comunicazione, ma non ottiene nessuna informazione sulla chiave

scambio della chiave di Diffie-Hellman

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

- Esempio: $p = 23$, $g = 5$
- Alice sceglie $a = 6$ $g^a = 5^6 \equiv 8 \mod 23$
- Bob sceglie $b = 15$ $g^b = 5^{15} \equiv 19 \mod 23$
- Alice calcola $(g^b)^a = 19^6 \equiv 2 \mod 23$
- Bob calcola $(g^a)^b = 8^{15} \equiv 2 \mod 23$

DH problem

- se Eve sa risolvere il problema del logaritmo discreto, sa ricavare la chiave comune di Bob e Alice
- dall'osservazione di g^a, g^b mod p ricava a e b, quindi calcola $k = g^{ab}$
- DH problem: dato un gruppo ciclico G, g un generatore e dati g^a, g^b trovare g^{ab}
- basta che sappia risolvere il DH problem per trovare la chiave
- equivalenza DH - DL?