ordine di un gruppo

- G un gruppo finito: ordine di $G = o(G) =$ numero di elementi di G
- l'insieme degli invertibili di $\mathbb{Z}_n$ è un gruppo rispetto al prodotto
- si denota con $U(\mathbb{Z}_n)$ e ha ordine $\phi(n)$
- esempio: $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$, ha $\phi(9) = 6$ elementi
- per $n = p$ primo, si ha $U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\} = \mathbb{Z}_p^*$, con $p - 1$ elementi

ordine di un elemento

- $(G, \cdot)$ un gruppo moltiplicativo di ordine n
- l'ordine di un elemento $g \in G$, $o(g)$, è il minimo intero positivo m tale che

$$g^m = 1$$

- (se $(G, +)$ è un gruppo additivo, l'ordine di un elemento $g \in G$ è il minimo intero positivo m tale che $mg = 0$)

- in $U(\mathbb{Z}_9)$, calcoliamo $o(2)$
  $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 7, 2^5 = 2 \cdot 7 = 14 = 5,$
  $2^6 = 2 \cdot 5 = 10 = 1$ quindi l'ordine di 2 è 6
- $o(2) = o(U(\mathbb{Z}_9)) = 6$
- ogni elemento di $U(\mathbb{Z}_9)$ si ottiene come una potenza dell'elemento 2
- si dice che 2 genera $U(\mathbb{Z}_9)$

gruppi ciclici

- Un gruppo G con n elementi, e tale che c'è un $g \in G$ con $o(g) = n$ si dice ciclico, e g si dice un generatore del gruppo
- i gruppi $U(\mathbb{Z}_p)$, p primo, sono gruppi ciclici
- se $GF(p^m)$ è un campo finito, il gruppo moltiplicativo $(GF(p^m) - \{0\}, \cdot)$ 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

$$g^x = y$$

- l'intero x si chiama il logaritmo discreto di y in base g, e si denota con $\log_g y$

logaritmo discreto come funzione unidirezionale

- in generale, lavoreremo con il gruppo $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$
- 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)

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

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?

- per implementare il protocollo, bisogna essere in grado di produrre numeri primi grandi
- e dato un tale primo p, di trovare una radice primitiva g modulo p
- sicurezza: p almeno 1024 bit, $p-1$ con un fattore primo grande
- si cerca anche un $p-1$ a fattorizzazione nota (per trovare facilmente g)
- spesso si sceglie $p = 2q+1$, q un primo
- la fattorizzazione è $p - 1 = 2q$
- un numero primo q tale che anche $2q+1$ è primo si chiama primo di Sophie Germain
- osservazione: la funzione unidirezionale $x \to g^x \pmod p$ non ha una trapdoor