Defn: Let G be a group and $g \in G$. The order of g is minimum i such that $g^i = e$

$g^i = \underbrace{g \cdot g \cdot \ldots \cdot g}_{i \text{ times}}$

Result 1: Let G be a group and $g \in G$ of order i. Then for any x, $g^x = g^{(x \bmod i)}$

Result 2: Let G be a group and $g \in G$ of order i. Then for any x and y, $g^x = g^y \iff x \equiv y \bmod i$

Result 3: Let G be a finite group of order m. and $g \in G$ of order i. Then $i \mid m$.

Defn: A finite group G of order m is called a cyclic group if $\exists$ at least one $g \in G$ such that the order of g is m. g generator of G.

Corollary: If G is a group of prime order p, then G is cyclic and every non-identity element of G is generator of G.

Result: Any subgroup of a cyclic group is cyclic

Thm: If p is prime, then $\mathbb{Z}_p^*$ is cyclic

where, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Fact: For any integer n, $(\mathbb{Z}_n, +)$ is a cyclic group of order n. where 1 is the generator of the group.

Let G be a cyclic group of order n. Then $G \cong \mathbb{Z}_n$.

Mapping $f(i) = g^i$

Example: $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^*$ for p being prime

Suppose G is a cyclic group and $G = \langle g \rangle$

Therefore for every $h \in G$ $\exists$ x such that

$h = g^x$ → Discrete logarithm of h base g.

$x = \log_g h$

Adversary A will be given the description of the cyclic group G, along with its generator g and a random group element h. Adversary A needs to find x.

Discrete Logarithm problem.

$DLOG_{A,G}(1^n)$

- Run $G(1^n)$ to obtain the o/p (G, q, g). where cyclic group.
  $|G| = q$, $\|q\| = n$ and $G = \langle g \rangle$
- Choose an element $x \xleftarrow{\$} \mathbb{Z}_q$ and compute $h = g^x$
- A is given (G, q, g, h) and outputs $x \in \mathbb{Z}_q$.
- Return 1 if $x = x'$

We say that discrete logarithm problem is hard if $\forall$ PPT alg. A, $\exists$ a G_1 and a negl fn such that.

$$Pr[DLOG_{\mathcal{A},\mathcal{G}}(1^n) = 1] \leq negl(n)$$ for all sufficiently large n.

Diffie-Hellman problem:

We consider a cyclic group $\mathcal{G}$ of order q and its generator g. Let $x_1, x_2 \in \mathbb{Z}_q$

$$DH(g^{x_1}, g^{x_2}) = g^{x_1 x_2} = (g^{x_1})^{x_2} = (g^{x_2})^{x_1}$$

$h_1 = g^{x_1}$; $h_2 = g^{x_2} \in \mathcal{G}$. $DH(h_1, h_2) = h_1^{x_2} = h_2^{x_1}$

Computational Diffie-Hellman:

Given $(G, q, g, g^{x_1}, g^{x_2})$, it is infeasible for any PPT alg. A to compute $g^{x_1 x_2}$

$CDF_{A,G}(1^n)$:

- Run $G(1^n)$ to get (G, q, g) s.t. $|G| = q$ & $G = \langle g \rangle$.
- Choose $x_1, x_2 \xleftarrow{\$} \mathbb{Z}_q$ and compute $h_1 = g^{x_1}$, $h_2 = g^{x_2}$; $h = g^{x_1 x_2}$.
- A is given (G, q, g, h_1, h_2) & return $y \in G$.
- Return 1 when $y = h$.

Computational Diffie-Hellman is hard if $\forall$ PPT alg. A, $\exists$ G and a negligible fn negl such that:

$Pr[CDH_{\mathcal{A},G}(1^n) = 1] \leq negl(n)$ for all sufficiently large n.

Claim: $CDH \leq_p DLOG$

$A \leq_p B$

$A(G, q, g, g^{x_1}, g^{x_2})$

A has to compute $g^{x_1 x_2}$

Decisional Diffie-Hellman problem

$DDH_{A,G}(1^n)$

- On input 1^n, $G(1^n)$ returns (G, q, g) where $|G| = q$, $\|q\| = n$ and $G = \langle g \rangle$
- Randomly samples $x_1, x_2 \leftarrow\$ \mathbb{Z}_q$.
- Computes $h_1 = g^{x_1}$, $h_2 = g^{x_2}$
- Samples a bit $b \leftarrow\$ \{0,1\}$
  - if $b = 0$, then $y \leftarrow\$ \mathbb{Z}_q$, $h_3 = g^y$.
  - if $b = 1$, then $h_3 = g^{x_1 x_2}$

- A is given (G, q, g, h_1, h_2, h_3)
- A outputs b'
- Return 1 if $b = b'$

We say that DDH is hard if $\forall$ PPT alg. A, $\exists$ a G and a negligible fn negl such that

$$Pr[DDH_{A,G}(1^n) = 1] \leq \frac{1}{2} + negl(n)$$ for all sufficiently large n.

$$\left| Pr[A(G, q, g, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1] - Pr[A(G, q, g, g^{x_1}, g^{x_2}, g^{y}) = 1] \right| \leq negl(n).$$

Fact 2: $DDH \leq_p CDH$.

From Fact 1 and Fact 2:

$$DDH \leq_p CDH \leq_p DLOG_2$$

There are groups in which DDH problem is easy, but CDH and DLOG are believed to be hard.

Using prime order group:

A necessary condn for DDH problem to be hard is that $DH_g(h_1, h_2)$ by itself should be indistinguishable from a random group element.

It seems that it would be best if $DH_g(h_1, h_2)$ actually were a random group element when h_1, h_2 are randomly chosen from the group.

Lemma: Let G be a group of prime order q such that $G = \langle g \rangle$. If $x_1, x_2 \leftarrow\$ \mathbb{Z}_q$, then

(i) $\Pr[DH_g(g^{x_1}, g^{x_2}) = 1] = \frac{2}{q} - \frac{1}{q^2}$

and for any $y \neq 1$

(ii) $\Pr[DH_g(g^{x_1}, g^{x_2}) = y] = \frac{1}{q} - \frac{1}{q^2}$

Pf: (i) $\Pr[DH_g(g^{x_1}, g^{x_2}) = 1] = \Pr[g^{x_1 x_2} = g^0]$

$= \Pr[x_1 x_2 \bmod q = 0] = \Pr[x_1 = 0] + \Pr[x_2 = 0]$

$- \Pr[x_1 = 0 \wedge x_2 = 0]$

$= \left(\frac{2}{q} - \frac{1}{q^2}\right)$

(ii) $P[x_1 x_2 \equiv \alpha \bmod q]$

$P[x_1 x_2 \equiv \alpha \bmod q]$

$= P[x_1 x_2 \equiv \alpha \bmod q \wedge x_1 \neq 0]$.

$+ P[x_1 x_2 \equiv \alpha \bmod q \wedge x_1 = 0]$.

$\underbrace{\qquad\qquad}_{0}$

$= P[x_1 x_2 \equiv \alpha \bmod q \mid x_1 \neq 0] \cdot \underbrace{P[x_1 \neq 0]}_{\frac{q-1}{q}}$

$= \frac{1}{q}$.

$= \frac{1}{q}\left(1 - \frac{1}{q}\right) = \frac{1}{q} - \frac{1}{q^2}$.

the error bound that $DH_g(h_1, h_2)$ is $\frac{1}{q} \pm \frac{1}{q^2}$ away from uniform distⁿ.

We work in $\mathbb{Z}_p^*$ for p is a prime number.
But the order of $\mathbb{Z}_p^* = p-1$ which is not prime.
One can show that if p is a prime number then DDH is easy in $\mathbb{Z}_p^*$.
If p is a strong prime $\Rightarrow p = 2q+1$, where q is prime, then $|\mathbb{Z}_p^*| = (p-1)$. Subgroups which are the quadratic

residues modulo p will have the cardinality

$$\frac{p-1}{2} = q$$

El-gamal Encryption:

Lemma: Let G be a finite group and $m \in G$ be an arbitrary group element. Then for any $\hat{g} \in G$.

$$P[m \cdot g = \hat{g}] = \frac{1}{|G|}$$

$g \leftarrow\$ G$

$$\Downarrow$$

$$P[g = m^{-1} \cdot \hat{g}] = \frac{1}{|G|}$$

El-Gamal

$Gen(1^n)$: Runs $G(1^n)$ to obtain (G, q, g), where $|G| = q$, $\|q\| = n$ and $G = \langle g \rangle$. Choose a random $x \leftarrow\$ \mathbb{Z}_q$.

$$PK = (G, q, g, g^x)$$

$$SK = (G, q, g, x)$$

$Enc_{PK}(m)$: Let $pk = (G, q, g, h)$.

Sample $y \leftarrow\$ \mathbb{Z}_q$.

Computes $c_2 = (h^y \cdot m)$

$$\hat{c} = \begin{pmatrix} c_1 \\ \| \\ g^y \end{pmatrix}, c_2)$$

Receiver receives the ciphertext

$\hat{C} = (c_1, c_2)$

$c_1 = g^y$

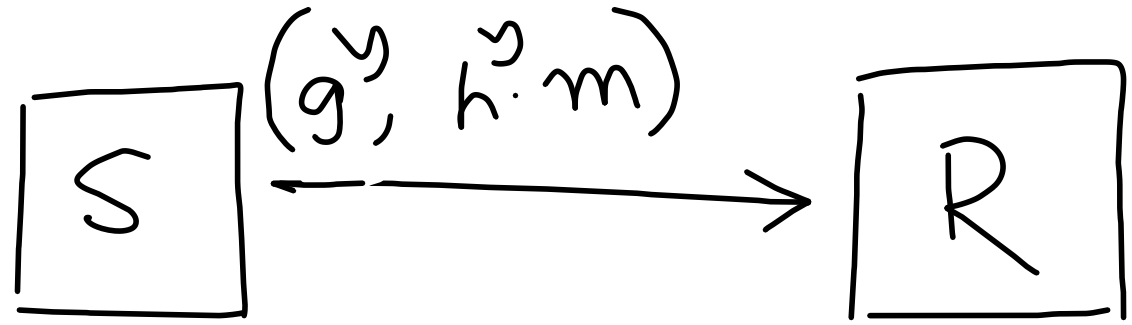
$c_2 = h^y \cdot m$

$= g^{xy} \cdot m$

c_1 = g^y, c_2 = $g^{xy} \cdot m$

$(g^y, g^{xy} \cdot m)$

$(c_1^x)^{-1} \cdot c_2 = (g^{xy})^{-1} \cdot g^{xy} \cdot m = m$.



$y \leftarrow \$ \mathbb{Z}_q$.

$x \leftarrow$ secret

$h \leftarrow$ public

Adversary knows:

(i) g^y

(ii) g^x . $g^{xy} \cdot m$.