g is 12

① Recall: Order of $g \in \mathbb{Z}_n^*$ is $a \iff g^a = 1$ in $\mathbb{Z}_n^*$. Also, $a \underset{\text{divides}}{\mid} |\mathbb{Z}_n^*| = \underset{\text{Euler-phi function}}{\phi(N)}$

1. g has order 42. So, g generates $\mathbb{Z}_{43}^*$, i.e., $\mathbb{Z}_{43}^* = \{ g^i : i \in \{1, 2, \dots, 42\}\}$.

   Since $h \in \mathbb{Z}_{43}^*$, $\exists j \in \{1, 2, \dots, 42\}$ s.t. $g^j = h$, i.e., $11^j = 5$. In the worst case, one needs to try 41 multiplications.

2. g has order 42. So smallest power of g giving 1 in $\mathbb{Z}_{43}^*$ is 42.

   In particular, $x = 21$, $y = 14$, $z = 6$. Then smallest power of $g^x = g^{21}$ giving 1 in $\mathbb{Z}_{43}^*$ is 2, i.e., order of g^x is 2. Similarly, order of $g^y = g^{14}$ is and order of $g^z = g^6$ is 7.

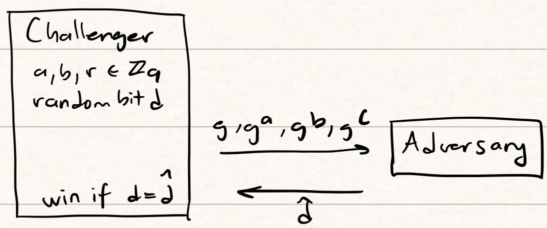
3. Discrete logarithm (DL) of h in $\mathbb{Z}_p$ for the base g is a, i.e., $g^a = h \bmod p$.

   $\Rightarrow (g^a)^x = h^x \bmod p \Rightarrow (g^x)^a = h^x \bmod p \Rightarrow a \bmod \underset{\text{order of } g^x}{2}$ is the DL of h^x for base g^x.

   Similarly, $a \bmod 3$ is the DL of h^y for the base g^y and $a \bmod 7$ is the DL of h^z for the base g^z. After finding
   $a = a_1 \bmod 2$
   $a = a_2 \bmod 3$
   $a = a_3 \bmod 7$, use Chinese Remainder Theorem to recover a. This is more efficient because a_1 can be found with at most 1 multiplication, a_2 with 2 mult., a_3 with 6 mult. In total, we need at most 9 multiplications.

4. Similar to 3, if $p = \prod_{i=1}^{\ell} p_i$ with $p_i < B$, we need at most $\sum_{i=1}^{\ell} (p_i - 1) < \ell(B-1)$ mult.

② Recall: DDH: p, q primes s.t. $q \mid p-1$. Fix $g \in \mathbb{Z}_p^*$ s.t. order of g is q.



$$c = \begin{cases} r & \text{if } d = 0 \\ a \cdot b & \text{if } d = 1 \end{cases}$$

1. Observe that g is a generator, so q is $p-1$. We need 2 observations:

1. a, b odd $\Rightarrow a \cdot b$ odd

2. $p-1$ even $\Rightarrow \frac{p-1}{2}$ is integer.

If a is even, then $a = 2 \cdot a'$ and $(g^a)^{\frac{p-1}{2}} = (g^{p-1})^{a'} = 1 \mod p$.

If a is odd, then $a = 2a'+1$ and $(g^a)^{\frac{p-1}{2}} = (g \cdot g^{2a'})^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \cdot \underbrace{(g^{p-1})^{a'}}_{1} \neq 1 \mod p$.

Similarly, we can check parity of b and c.

Notice that $a \cdot b$ is odd iff both a and b is odd, but c is is odd with prob. $\frac{1}{2}$. Given (g, g^a, g^b, g^c), adversary $\mathcal{A}$ computes $(g^{\frac{p-1}{2}}, (g^a)^{\frac{p-1}{2}}, (g^b)^{\frac{p-1}{2}}, (g^c)^{\frac{p-1}{2}})$

It checks if parities are consistent. If they are, it outputs $c = ab$, i.e., $L_{ddh\text{-}real}$.

$$\Pr[\mathcal{A} \text{ wins}] = \Pr[\mathcal{A} \Rightarrow L = L_{ddh\text{-}real} \mid L_{ddh\text{-}real}] \Pr[L_{ddh\text{-}real}]$$
$$+ \Pr[\mathcal{A} \Rightarrow L = L_{ddh\text{-}ideal} \mid L_{ddh\text{-}ideal}] \Pr[L_{ddh\text{-}ideal}]$$
$$= 1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

$$Adv(\mathcal{A}) = \left| \Pr[\mathcal{A} \text{ wins}] - \frac{1}{2} \right| = \frac{1}{4}.$$

3. 1. Given c_1, c_2, Bob computes $c_1^b = (g^a)^b = (g^b)^a = B^a \mod p$.

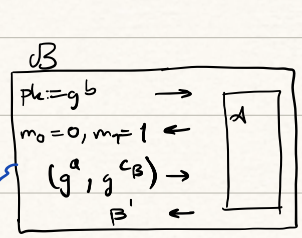
If c_1^b is equal to c_2, then $m=0$, otherwise $m=1$.

2. Let $\mathcal{A}$ be an adversary that wins the IND-CPA security game with prob. $P > \frac{1}{2}$.

Construct an adv. $\mathcal{B}$ that runs $\mathcal{A}$ as a subroutine to break DDH.

$c_0 := a \cdot b$
$c_1 \sim \mathbb{Z}_p^*$
$\beta \sim \{0,1\}$

$(g, g^a, g^b, g^{c_\beta}) \rightarrow$



we choose ctexts corresponding to encryption of one of the messages

- If $c_B = a \cdot b$, $\mathrm{Dec}(sk, (g^a, g^{c_B})) = 0$ indeed $g^{c_B} = g^{ab} = (g^b)^a = B^a$ with prob. p.

- If $c_B \sim \mathbb{Z}_p^*$, $\mathrm{Dec}(sk, (g^a, g^{c_B})) = 1$, with prob. $p\Big(1 - \underbrace{\frac{1}{p-1}}_{\text{prob. of random number being } ab.}\Big) \approx p$.

④ **Recall:** A group $(\underset{\text{set}}{G}, \underset{\text{operation}}{\cdot})$ is suitable for DH key exchange protocol if it is hard to compute $a \in \{1, \dots, \mathrm{ord}(G)\}$ given G, g, g^b where g is the generator.

1. If g is a generator, any elt. in $\mathbb{Z}_p$ can be written as $k \cdot g \bmod p$ for some $k \in \{0, \dots, p-1\}$.

   Given g, bg for some b, $b \cdot g \cdot g^{-1} = b \bmod p$. → modular inverse is easy.

2. Given $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^b = \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix}$ for some b, one can recover b by $b \cdot g \cdot g^{-1} = b \bmod p$.

3. Given g and g^b, observe that $g^i(1)$ is distinct for each $i \in \{1, \dots, n\}$. Apply brute-force on the power on the power of g and evaluate it at 1 (WLOG). When $g^i(1) = g^b(1)$, it means $i = b$. This has polynomial time complexity, namely $\underbrace{(n-1)}_{\le \# g^i(1)\text{'s}} \underbrace{\log n}_{\le \text{bits to represent } g^i(1)}$.