PRIVACY:

TP. 1.0

TP1: (20) $G = \mathbb{Z}^*_{17} \Rightarrow n = 17$

1) $|G| = |\{1, 2, \dots, 14, 15, 16\}| = \boxed{16}$

2) 3 is generator of if $\forall a \in G :: \exists l \mid a = g^l \% n$

$\Rightarrow G' = [3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]$

$\dots [3^1, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}, 3^{16}]$ (mod 17)

$\Rightarrow$ OK

3) $5 . 5^{-1} \% 17 = 1 \Leftrightarrow$ ~~$5^{n-1} \% n$ $a^{n-1} \% n = 1$~~ (

Fermat's Little $\Rightarrow a^{-1} = a^{n-2} \% n$

$\boxed{5^{-1} = 5^{17-2} \% 17 = 7}$ $\qquad (5.7 = 35) \% 17 = 1$

4) $3^5 \% 17 = 5$ $\qquad q = 16 = $ order

$g^l \% n = g^{l \% q} \% n \Leftrightarrow 3^{2021} \% 17 = 3^{2021 \% 16} \% 17 = 3^5 \% 17 = 5$

5) $\frac{4}{7} \% 17 = 4 . 7^{-1} \% 17 = 4.5 \% 17 = 20 \% 17 = 3$

$\boxed{7^{-1} = 7^{17-2} \% 17 = 5}$

Q1) TP.J.1

P0 → Discrete log DL : given $(g, h) \Rightarrow$ find $x \mid h = g^x$

P1 → Computational Diffie - Hellman : given $(g, a = g^x, b = g^y) \Rightarrow$ find $c \mid c = g^{xy}$

P2 → Decisional Diffie - Hellman : given $(g, a = g^x, b = g^y, c = g^z) \Rightarrow$ decide if $z = xy$

P0 : $x = \text{discrete\_log}_g(h) \Rightarrow$ NP-HARD

P1 : $c = g^{(\text{dl\_log}_g(a) \cdot \text{dl\_log}_g(b))}$

P2 : $\text{dl\_log}_g(c) = \text{dl\_log}_g(a) \cdot \text{dl\_log}_g(b)$

1) ~~As seen in P0, CDH is solvable if DL is solvable. Thus if~~

If CDH holds in a group $G = (g^1, g^2, g^3, \dots, g^{n-1}) \pmod{n}$, it can be easily computed as follow :

$a = g^x$, $b = g^y$: find indexes of a and b respectively in G so i, j

We know $\begin{cases} G_i = a = g^x = g^i \\ G_j = b = g^y = g^j \end{cases} \Leftrightarrow \begin{cases} x = i \\ y = j \end{cases}$

So $c = g^{ij} \% n$

DL in group G can be reduced to CDH with :

$DL(g, h) = \exists i \in [1; n-1] \mid h = CDH(g, g^i, g^1) = g^i \% n$

Then $x = i$

As CDH is easy in group G and DL can be easily solved using DL problem then ~~CDH~~ DL is easy (polynomial complexity $O(n^2)$).

HOLD = Ne peut pas être résolu sans les clés. TP. 1.2
C'est compliqué à résoudre NP-HARD

1) Prove CDH is hard => DL is hard

DL is easy => CDH is easy (P1) car le donne.

we can build CDH using DL. ~~thus if DL holds CDH has to to hold also.~~

If DL doesn't hold then CDH doesn't hold:

$$(\text{CDH hold} \Rightarrow F \Leftrightarrow T) \Rightarrow \text{CDH hold} = F$$

If DL holds then CDH could hold =>

$$((\text{CDH hold} \Rightarrow T \Leftrightarrow T) \Rightarrow \text{CDH hold} = T \vee \text{CDH hold} = F$$

2) Prove DDH hold => CDH hold
(is hard) (is hard)

∃ implem |

implem: $DDH(g, a = g^x, b = g^y, c = g^z) = a.b == CDH(g, a, b)$

∃ impl If CDH doesn't hold then DDH doesnt hold

In this world only problems DL, DDH, CDH, no magic algo to solve DDH and not CDH.

Q7) TP. 1.3

$P(p, x) \doteq \exists s \in \mathbb{Z}_p^* \mid s^2 = x \quad \in \{0;1\}$

```
DDH(g, a = g^x, b = g^y, c = g^z) =
    x = 1
    while a > g:
        if P(p, a) then a = √a ; x *= 2
        else a = a/g ; x += 1
    if a == g:   // else a == 1
        x += 1
    return b^x = c
```

On peut leak des infos :

$B_a = P(p, a)$

$B_b = P(p, b)$

$B_c = P(p, c)$

$B_a \vee B_b \Rightarrow B_c$ si c'est faux alors DDH = false

$\neg B_a \wedge \neg B_b \Rightarrow \neg B_c$

Pr(x is pair) = Pr(y is pair) = Pr(z is pair) = 1/2

B_a	B_b	B_c	S	Pr
0	0	0	?	50%
0	0	1	F	100%
0	1	0	F	100%
0	1	1	?	50%
1	0	0	F	100%
1	0	1	?	50%
1	1	0	F	100%
1	1	1	?	50%

50% des cas on sait dire non

50% des cas on répond random

Pr(avoir bon avec réponses random) $= 1 \cdot 50\% + \frac{1}{2} \cdot 50\% = 75\%$

~~Half the elements of $\mathbb{Z}_p^*$ are square, other half not because if x is even then g^x is~~

Q7) TP.1.4

Client | **Server**

Server:

Select G, generator g and modulo p

Order $|G| = p$

Secret $x \in \mathbb{Z}_p$ and $h = g^x \% p$

Server → Client: (G, p, g, h)

Client:

$q = |G|$

$m \equiv \text{message} \in \mathbb{Z}_p$

$r = \text{rand}(\mathbb{Z}_p)$

$$Enc_h(m) = \begin{cases} c_1 = g^r \% p \\ c_2 = m \cdot h^r \% p \end{cases}$$

Client → Server: $Enc_h(m) = (c_1, c_2)$

Server:

$s = c_1^{x} \% p$

$s' = s^{-1} = s^{p-2} \% p$

$m = c_2 \cdot s' \% p \equiv Dec_x(c_1, c_2)$