9.2.1 Elgamal

- Parameter domains: g and p as in DH key agreement.
- $\mathsf{Gen}(\lambda)$: pick $A \in \{1, \cdots, p-1\}$ and compute $h = g^A$. Set $\mathsf{pk} = h$ and $\mathsf{sk} = A$.
- $\mathsf{Enc}_{\mathsf{pk}}(m)$ with $m \in \mathrm{GF}(p)$: pick RND $B \in \{1, \cdots, p-1\}$ and compute $C = (g^B, m \cdot h^B)$.
- $\mathsf{Dec}_{\mathsf{sk}}(C)$ with $C = (c_1, c_2)$: compute $m = c_2 / c_1^A$.

Exercise 9.2.4

Consider **Elgamal** with $p = 83$ and $g = 4$. Encipher $m = (011101)_2$ with $A = 37$.

$p = 83$ $\qquad$ $m = (011101)_2 = 29$

$g = 4$ $\qquad$ $C = ?$

$A = 37 \Rightarrow A = s_K$ (by definition)

computation below

$h = g^A \bmod p = \boxed{4^{37}} \bmod 83 = 12 \bmod 83$

h will be our P_K

For the encryption we choose an arbitrary (random) B s.t. $0 < B < p$

- $B = 1$

$\mathrm{Enc}_{P_K}(m) = C = (\overset{c_1}{g^B}, \overset{c_2}{m \cdot h^B}) \bmod p = (4^1, 29 \cdot 12^1) \bmod 83 =$

$= (4, 16)$

$\mathrm{Dec}_{sk}(C) = \frac{C_2}{C_1^A} \bmod p = \frac{16}{4^{37}} \bmod 83 = \frac{\cancel{16}^{\,4}}{\cancel{12}_{\,3}} \bmod 83 =$

$4 \cdot 3^{-1} \bmod 83 = 4 \cdot 28 \bmod 83 = 29 \bmod 83 = m$ ✓

computation below

COMPUTATION PART

- 4^{37} ?

$37_{10} = (100101)_2$

$1.\quad 1^2 \cdot 4^1 = 4 \bmod 83$
$0.\quad 4^2 \cdot 4^0 = 16 \bmod 83$
$0.\quad 16^2 \cdot 4^0 = 7 \bmod 83$
$1.\quad 7^2 \cdot 4^1 = 30 \bmod 83$
$0.\quad 30^2 \cdot 4^0 = 70 \bmod 83$
$1.\quad 70^2 \cdot 4^1 = \underline{12} \bmod 83$

- $3^{-1} \bmod 83$?

$83 = 27 \cdot 3 + 2 \qquad 1 = 3 - 2$

$3 = 2 + 1 \qquad = 3 - (83 - 27 \cdot 3) = \underline{28} \cdot 3 - 83$

$3^{-1} \bmod 83 = \underline{28} \bmod 83$

EXERCISE 2 (from math engineering exam)

In an Elgamal cryptosystem with p = 11 and generator element g = 6, Alice has a public key kp = 7.
If a hacker intercepts the ciphertext (10, 6) sent to Alice, they can trace back to the plaintext message.
Find the plaintext message.

$p = 11$ $\qquad K_p = h = 7$ $\qquad m = ?$

$g = 6$

$C = (c_1, c_2) = (10, 6)$

we know that $K_p = g^A \bmod p$:

$7 = 6^A \bmod 11$

BRUTE FORCE APPROACH:

$6^1 \bmod 11 = 6$	$6^6 \bmod 11 = 5$
$6^2 \bmod 11 = 3$	$6^7 \bmod 11 = 8$
$\boxed{6^3 \bmod 11 = 7}$ OK	$6^8 \bmod 11 = 4$
$6^4 \bmod 11 = 9$	$6^9 \bmod 11 = 2$
$6^5 \bmod 11 = 10$	$6^{10} \bmod 11 = 1$

You may want to check if there is a better way to solve this exercise.
Brute force was the only approach that came out of my mind.

$A = 3$

Once we have the A it is easy to compute m

$$m = \frac{c_2}{c_1^A} \bmod p = \frac{6}{10^3} \bmod 11 = 6 \cdot 10^{-1} \bmod 11 = 60 \bmod 11 = 5$$

REDUCED $10 \bmod 11$

EEA: $10^{-1} \equiv 10 \bmod 11$

The plaintext is $m = 5$

Another approach for this exercise would be:
Knowing that

$c_1 = g^B \bmod p$ AND $c_2 = m \cdot h^B \bmod p$

guess B (BRUTE FORCE APPROACH)

$c_1 = g^B \bmod p = 6^B \bmod 11 = 10 \Rightarrow B = 5$ (see table above)

HENCE

$$m = \frac{c_2}{h^B} \bmod 11 = \frac{6}{7^5} \bmod 11 = \frac{6}{10} \bmod 11 = 5 = m \checkmark$$