Exercise 4 Cheat Sheet
ElGamal + Pohlig–Hellman

1. Problem Recognition

Given

$$(p, \alpha, A), \quad A \equiv \alpha^x \pmod{p}$$

This is an ElGamal / discrete log setting.
Typical tasks:

- Encrypt / decrypt messages
- Recover secret exponent x (Pohlig–Hellman)

2. ElGamal Basics

Public key:

$$(p, \alpha, A) \quad \text{with } A = \alpha^x \bmod p$$

Secret key:

$$x$$

Encryption:

$$B = \alpha^b \bmod p, \quad C = mA^b \bmod p$$

Ciphertext: (B, C)

Decryption:

$$m = C \cdot (B^x)^{-1} \bmod p$$

Inverse:

$$(B^x)^{-1} \equiv (B^x)^{p-2} \bmod p$$

3. Fast ElGamal Procedures

Encryption

Input: m, b, p, α, A

1. $B = \alpha^b \bmod p$
2. $K = A^b \bmod p$
3. $C = mK \bmod p$
4. Output (B, C)

Decryption

Input: $(B, C), x$

1. $K = B^x \bmod p$
2. Compute K^{-1}
3. $m = CK^{-1} \bmod p$

4. Pohlig–Hellman (Discrete Log)

Goal:

$$\alpha^x \equiv A \pmod{p}$$

Use:

$$p - 1 = \prod q_i^{e_i}$$

Solve $x \bmod q_i^{e_i}$, then combine via CRT.

5. Core Algorithm

Step 1: Factor group order

$$p - 1 = \prod q_i^{e_i}$$

GAP:

```
FactorsInt(p-1);
```

Step 2: Work modulo one prime power q^e

Compute:

$$g = \alpha^{(p-1)/q}, \quad h = A^{(p-1)/q}$$

Table:

$$g^0, g^1, \ldots, g^{q-1}$$

Step 3: First digit

Find:

$$h = g^{x_0} \Rightarrow x_0$$

GAP:

```
PowerMod(alpha,(p-1)/q,p);
PowerMod(A,(p-1)/q,p);
```

Step 4: Remove digit

$$A \leftarrow A \cdot \alpha^{-x_0}$$

GAP:

```
A := A * InverseMod(PowerMod(alpha,x0,p),p);
```

Now:

$$A = \alpha^{q(x_1 + x_2 q + \cdots)}$$

Step 5: Next digits

For digit x_i:

$$h = A^{(p-1)/q^{i+1}} \quad \Rightarrow \quad h = g^{x_i}$$

Then remove:

$$A \leftarrow A \cdot \alpha^{-x_i q^i}$$

Repeat until all digits are found.

Step 6: Reconstruct solution

$$x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}$$

This gives:

$$x \bmod q^e$$

Step 7: Combine with CRT

After computing all residues:

$$x \equiv a_i \pmod{q_i^{e_i}}$$

GAP:

```
ChineseRem([a1,a2,...],[m1,m2,...]);
```

Final result:

$$x \bmod (p-1)$$

6. Exam Strategy (Optimized)

- Factor $p-1$ first
- Solve one q^e fully before moving on
- Always reuse the same g-table
- Let GAP handle powers + CRT
- Never brute-force full log in $(\mathbb{Z}/p\mathbb{Z})^*$

Key Insight

Each step projects the problem into a subgroup of order q, isolating one digit of x at a time.