Exercise 3 Cheat Sheet – RSA

Recognition

- **(a)** Given $p, q, e, c \to$ RSA decryption.
- **(b)** Given $n, e, d \to$ Factor n using $ed - 1$.
- **(c)** Count bases causing the factorization algorithm to stop at a given step.

Key Formulas

$$n = pq, \qquad \phi(n) = (p-1)(q-1),$$

$$ed \equiv 1 \pmod{\phi(n)},$$

$$m = c^d \pmod{n},$$

$$k = ed - 1 = 2^s t, \qquad t \text{ odd}.$$

$$\boxed{ed - 1 \text{ is a multiple of } \phi(n)}$$

A. RSA Decryption

$$\phi = (p-1)(q-1)$$

$$d = e^{-1} \pmod{\phi}$$

$$m = c^d \pmod{n}$$

GAP

```
phi := (p-1)*(q-1);
InverseMod(e,phi);
PowerMod(c,d,n);
```

B. Factoring n from d

1. Compute
$$k = ed - 1 = 2^s t.$$
2. Compute
$$x = a^t \pmod{n}.$$

   If $x = \pm 1$, the base fails.

3. Repeat

$$y = x^2 \pmod{n}.$$

If $y \neq 1$, set $x \leftarrow y$.

Stop when

$$y = 1 \quad \text{and} \quad x \neq \pm 1.$$

4. Recover

$$\boxed{p = \gcd(x-1, n), \qquad q = \gcd(x+1, n)}$$

Verify $pq = n$.

GAP

```
PowerMod(a,t,n);
PowerMod(x,2,n);

Gcd(x-1,n);
Gcd(x+1,n);

FactorsInt(n);
```

C. Count Bases Found at Step t

Let

$$k = 2^s m,$$

and define

$$E = 2^t m.$$

Suppose the desired factor is p and the other prime is q.

Modulo p:

$$x^{2E} \equiv 1, \qquad x^E \not\equiv 1.$$

$$\boxed{N_p = \gcd(2E, p-1) - \gcd(E, p-1)}$$

Modulo q:

$$x^{2E} \not\equiv 1.$$

$$\boxed{N_q = (q-1) - \gcd(2E, q-1)}$$

By CRT,

$$\boxed{N = N_p N_q.}$$

Useful fact:

$$\boxed{\#\{x : x^r \equiv 1 \pmod{p}\} = \gcd(r, p-1)}$$

GAP

```
Gcd(2*E,p-1);
Gcd(E,p-1);

Gcd(2*E,q-1);

ChineseRem([a,b],[p,q]);
```

Remember

- $ed - 1 \neq \phi(n)$ in general.
- t must be odd.
- If $a^t = \pm 1$, choose another base.
- Stop at the *first* occurrence of $y = 1$.
- Always verify $pq = n$.