# TW 314 Lecture 33 (Mo 8 May 2017)

## The ElGamal cipher

- **The keys for user A**

A chooses a large prime number $n$, $\alpha \in \mathbb{Z}_n - \{0\}$, an integer $a$ $(1 < a < n)$, and then calculates $\beta \equiv \alpha^a \pmod{n}$.

A keeps the key $a$ secret, but makes the keys $\alpha$, $\beta$ and $n$ public.

- **Encryption**

If you want to send the message $x \in \mathbb{Z}_n$ to A, you encrypt $x$ by the rule

$$e(x, k) = \left(\alpha^k \pmod{n},\ x\beta^k \pmod{n}\right),$$

where the mask $k$ is a randomly chosen integer, $1 < k < n$.

## Decryption

A receives the cipher $(y_1, y_2)$ and decrypts by the rule

$$d(y_1, y_2) = y_2 (y_1^a)^{-1} \pmod{n}.$$

We need to prove that $d(y_1, y_2) = x$, that is, that $d(e(x, k)) \equiv x \pmod{n}$.

Proof: $d(e(x, k)) = d(\alpha^k \pmod{n}, x\beta^k \pmod{n})$

$$= x\beta^k ((\alpha^k)^a)^{-1} \pmod{n}$$

$$\equiv x\beta^k ((\alpha^a)^k)^{-1} \pmod{n}$$

$$\equiv x\beta^k (\beta^k)^{-1} \pmod{n}$$

$$\equiv x \pmod{n}.$$

∎

Example :

User A chooses $n = 557$, $\alpha = 123$, $a = 45$

and calculates $\beta \equiv 123^{45} \equiv 330 \pmod{557}$.

A keeps the key $a \equiv 45$ secret, and publish the keys $n = 557$, $\alpha = 123$, $\beta = 330$.

You need to send the message GO (i.e. 0715) to A, using "block length protocol" 2 digits:

You encrypt

$$e(07,29) = \left(123^{29} \pmod{557},\ 7 \times 330^{29} \pmod{557}\right) = (64,285)$$

$$e(15,31) = \left(123^{31} \pmod{557},\ 15 \times 330^{31} \pmod{557}\right) = (190,190)$$

A receives (64,285), (190,190) and decrypts...

$$d(64,285) = 285 \times 64^{-45} \equiv 7 \pmod{557}$$

$$d(190,190) = 190 \times 190^{-45} \equiv 15 \pmod{557}$$

which gives the message 0715, or GO.

---

As an exercise, check the calculations using the Euclidean algorithm and the square-and-multiply algorithm.