ECE 471/571 Early ciphers.

Encryption

Sets: $\mathcal{P}$ (plaintext set)

$\mathcal{C}$ (ciphertext set)

$\mathcal{K}$ (key set)

$\mathcal{E}$ (Encryption rule set)

$\mathcal{D}$ (decryption rule set)

$x \in \mathcal{P}$ $y \in \mathcal{C}$ $k \in \mathcal{K}$

$y = E_k(x)$ $E_k(\cdot)$

$x = D_k(y)$ $D_k(\cdot)$

Affine cipher.

Enc: $y = E_k(x) = (a \cdot x + b) \bmod 26$

$a, b \in Z_{26}$ $a = 9$. $b = 3$

$x, y \in Z_{26}$ $x = 0$, $y = 3$

Dec: $x = a^{-1}(y-b) \bmod 26$.

$a^{-1} = 3$.

$= 3 \cdot (y-3) \bmod 26$.

$x=1,\ y=12$

$x=2,\ y=4$

how to select a, b? $[0, 1, \ldots 25]$

$b \in Z_{26}$.

$\gcd(a, 26) = 1$.

a : co-prime with 26.

---

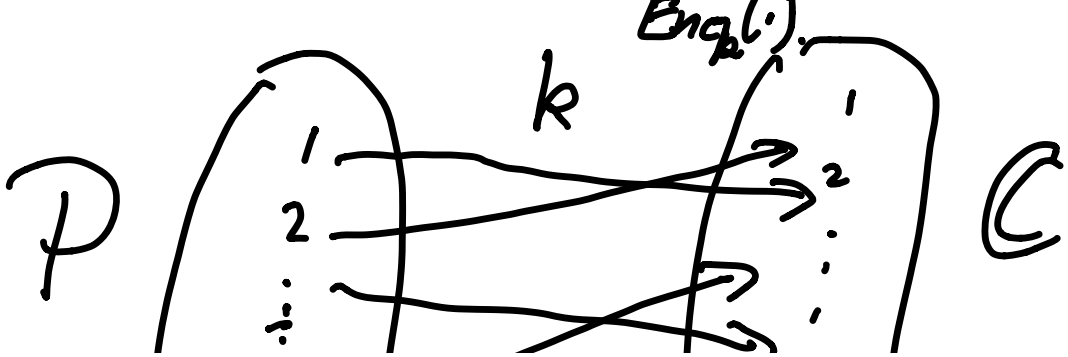
if $a = 2$. not co-prime ....

$b = 0$.

$y = 2x \bmod 26$. $x \in Z_{26}$

for $y = 0$. $x = ?$ 13. 0

ambiguous!



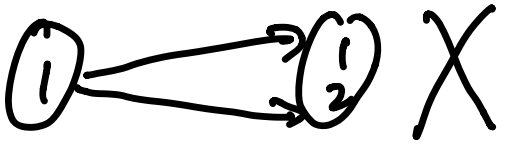
$\forall\ x_1, x_2 \in \mathbb{P}$

if $x_1 \neq x_2$ -

$E_k(x_1) \neq E_k(x_2)$

(injective function)

X



X

Euler's totient function

$\phi(n)$: # of integers $< n$

& coprime with n

if n is prime. e.g. $n=7$.

$\phi(n) = n-1$ $\quad$ 1, 2, 3, ... 6.

$n = p \times q$. $\quad$ p and q. primes

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

$\phi(26) = 1 \times 12 = 12$

$26 = 2 \times 13$ $\quad$ $n = 10 = 2 \times 5$

$\phi(10) = 4$ $\quad$ 1, 3, 7, 9

generally, $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$

$$\phi(n) = n \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)$$

e.g. $n = 4. = 2^2$

$\phi(4) = 4 \cdot \left(1 - \frac{1}{2}\right) = 2$

1, 3

e.g. $n = 24 = 4 \times 6 = 8 \times 3 = 2^3 \times 3$

$$\phi(24) = 24 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right)$$

$$= 24 \times \frac{1}{2} \times \frac{2}{3} = 8$$

Cardinality of key space of Affine cipher

$$n \times \phi(n) = 26 \times 12 = 312$$