Ch-4.6 Cryptography

modern

(*) Classical Cryptography

(1) Caesar's Cipher → key value → p = 3

msg → [Encoder] → encrypted msg → [Decoder] → msg

Encoder: $f(p)$; Decoder: $f^{-1}(p)$

$$f(p) = (c+p) \bmod 26$$

$$f^{-1}(p) = (c-p) \bmod 26$$

$0 \le r < d$

Ex

M E E T Y O U

12 4 4 19 24 14 20

$f(p)$

15 7 7 22 1 17 23

P H H W B R X

10th letter → J → (10-1) → 9

13th " → M → 12

$f^{-1}(p)$ → C

(*) p = 3 → CC

p ≠ 3 → public key shifting

Ch-4.6 Cryptography

modern

(*) Classical Cryptography

(1) Caesar's Cipher → key value → p = 3

msg → [Encoder] → Encrypted msg → [Decoder] → msg

Encoder: $f(p)$; Decoder: $f^{-1}(p)$

$$f(p) = (c+p) \bmod 26$$

$$f^{-1}(p) = (c-p) \bmod 26$$

$$0 \le r < d$$

Ex: MEET YOU

C	12	4	4	19	24	14	20
f(p)	15	7	7	22	1	17	23
	P	H	H	W	B	R	X

$f^{-1}(p)$ → C

10th letter → J → (10-1) → 9

13th " → M → 12

(*) p = 3 → CC

p ≠ 3 → public key shifting

(2) Block cipher

- Divide msg into blocks of (m) letters.
- if # of letters is not divisible by m, then add letters randomly at the end such that # of letters is divisible by m
- A transposition function (σ) for transposing.

Ex "PIRATES ATTACK"

$|msg| = 13$

$m = |\sigma| = 4$

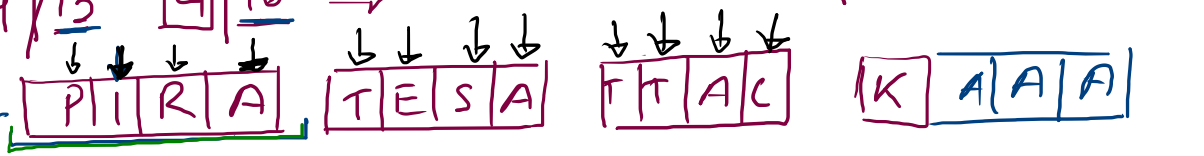
$\sigma = \{1, 2, 3, 4\}$

$\sigma(1) = 3$ $\quad \sigma(3) = 4$

$\sigma(2) = 1$ $\quad \sigma(4) = 2$

$\sigma(i) = m$

4 | 13 | 4 | 16

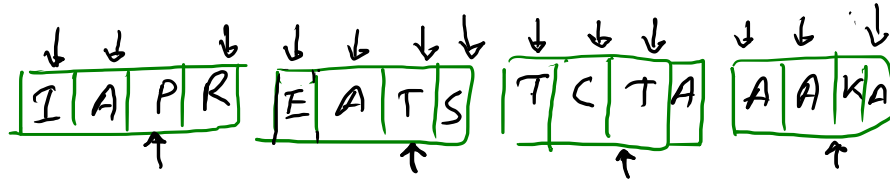


$\sigma(2) = 1$

$\sigma(4) = 2$

$\sigma(1) = 3$

$\sigma(3) = 4$



$\sigma^{-1}(1) = 2$

$\sigma^{-1}(2) = 4$

$\sigma^{-1}(3) = 1$

$\sigma^{-1}(4) = 3$