Cryptography

Monday, February 21, 2022 12:54 PM

Recall: FLT

if p is prime, $a^{p-1} \equiv 1 \pmod{p}$

for a coprime to p

* Primality Test
* reducing exponent e.g. $3^{50} \bmod 13 \equiv 3^{2} \pmod{13}$
* Pseudoprimes

  if $a^{n-1} \equiv 1 \pmod{n}$ for composite n

  then n is pseudoprime to base-a.
* Carmichael numbers.

  e.g. 561

Oh Quiz 1

1] Hash functions

$$h(k) = d$$

k : is the key of arbitrary length (size)

d : is the hash value of a fixed length (size)

h : is a one-way function

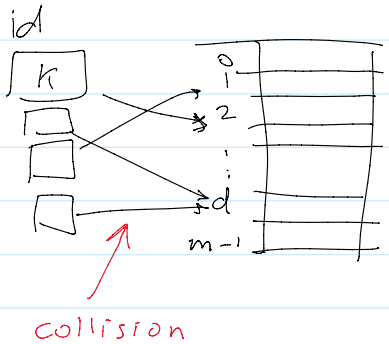
Format:

$$h(k) = k \bmod m$$

e.g.

$$h(k) = k \bmod 31$$

of length 5-bit



can be used to map student ID. to a month calender

e.g. $20173613_{0} \bmod 31 = 3$

$= 8 \times 2$

$= 10$

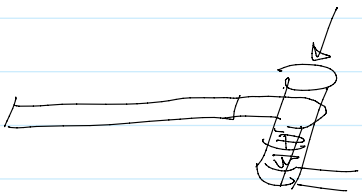
$= 17$

$= 16 \times 2$

$= 20$

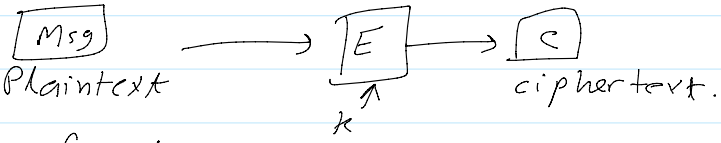
$= 15 \times 2$

2] Cryptography (§4.6)

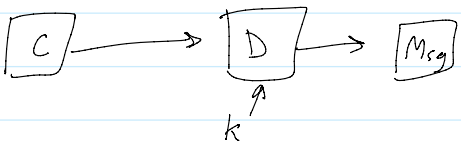


Crypto = secret
graphy = writing

- Encryption function : to encrypt the msg.



- Decryption function : to decrypt the ciphertext.



3] Caesar Method (shift-cipher)

$a - z \longrightarrow 0 - 25$ (mod 26)

A $\xrightarrow{+3}$ D
B $\xrightarrow{+3}$ E
⋮
X $\xrightarrow{+3}$ A
Y $\xrightarrow{+3}$ B

Encryption function:

$k \in \{0, \ldots, 25\}$

$$c = E(p) \equiv p + k \pmod{26}$$

Decryption:

$$D(c) \equiv c - k \pmod{26} = p$$

$c = p \cdot k$
$p = c \cdot k^{-1}$

a	b	c	d	e	f	g
0	1	2	3	4	5	6

h	i	j	k	l	m	n
7	8	9	10	⋮		13

o	p	q	r	s	t	u
14	⋮	⋮	⋮	18		

4] Affine cipher

key = (a, b)

$$c = E(p) \equiv a \cdot p + b \pmod{26}$$

e.g. Encrypt : Msg = "ok" with k = (3, 2)

Sol. "ok" $\longrightarrow$ (14, 10)

$$O = 14 \xrightarrow{E} 3 \times 14 + 2 \equiv 18 \pmod{26} \rightarrow S$$
$$K = 10 \xrightarrow{E} 3 \times 10 + 2 = 6 \pmod{26} \rightarrow G$$

$$\text{"OK"} \xrightarrow{E} \text{"SG"}$$

The decryption function:

$$D(c) = (c - b) \cdot \bar{a}^{1} \pmod{26}$$

5] How many keys are there in affine cipher?

$$k = (a, b) \qquad a \in \mathbb{Z}_{26}^{*}, \; b \in \mathbb{Z}_{26}$$

$$|\mathbb{Z}_{26}| = 26$$

$$|\mathbb{Z}_{26}^{*}| = \Phi(26) = \Phi(2 \cdot 13) = 1 \cdot 12 = 12$$

The size of the key space $|K| = 26 \cdot 12 = 312$ keys.