1. Introduction to Network Security & cryptography

Page No.
Date

- The information Security Triad
  - Confidentiality
  - Integrity
  - Availability

- Techniques used to achieve the security goals
  (1) Cryptography (Generalized)
  (2) Steganography (Specific)

- Cryptography
  - Some Security mechanisms listed in the previous section can be implemented using cryptography. Cryptography a word with Greek origin, means "secret writing". However we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Although in the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms: Symmetric-key encipherment, asymmetric-key encipherment and hashing.
  - It is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" and the suffix "-graphy" stands for "writing"
  - Parts:
    - Encryption
    - Decryption

- Techniques of cryptography
  - Symmetric

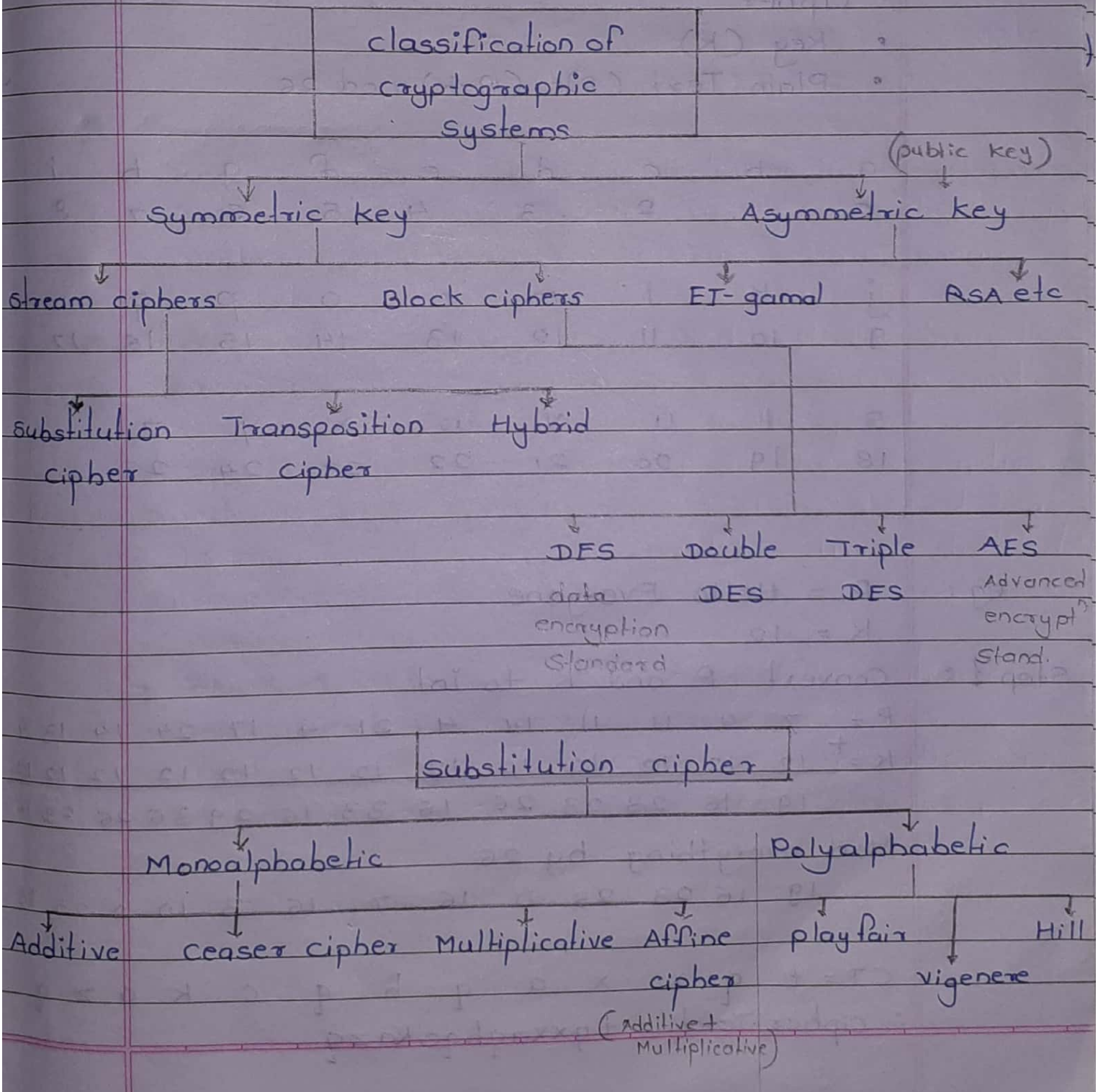
In Symmetric encipherment, an entity say Alice can send a message to other entity, say Bob, over an insecure channel with the assumption that an adversary, say Eve cannot understand the contents of the message by simply dropping over the channel. Alice encrypts the message using an encryption algorithm. Bob decrypt the ~~encryption~~ message using a decryption algorithm. Symmetric-key encipherment uses a single secret key for both encryption and decryption. Encryption/decryption can be thought of as electronic locking system. In symmetric-key enciphering. Alice puts the message in a box and locks the box using shared secret key. Bob unlocks the box with the same key and takes out the messages.

- asymmetric

In Symmetric encipherment, we have the same situation as the symmetric-key encipherment with a few exceptions. First there are two keys instead of one is public key and one private key. To send a secure message to Bob. Alice firsts encrypts the message using Bob's public key. To decrypts the message, Bob uses his own private key.

- **Hashing**

In hashing, a fixed-length message digest is created out of a variable-length message. The digest is normally much smaller than the message. To be useful, both the message and the digest must be sent to Bob. Hashing is used to provide check values.



mod:(26) → No. of unique char possible

Page No.
Date

- **Additive Cipher (shift cipher)**

$x = (P+K) \bmod 26$

$P+K = a, 26 = b$

$x = a \bmod b$

$x = a - (int(a/b) * b)$

Encryption

- Plain text (P) (message)
- Key (K)
- Cipher (C) = (P+K) mod 26

Decryption

- Cipher
- Key (K)
- Plain Text (P) = (C-K) mod 26

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

eg: P = Hello Everyone

K = 12

Step 1: Convert P and K to int

P = 7 4 11 11 14 4 21 4 17 24 14 13 4

K = + 12 12 12 12 12 12 12 12 12 12 12 12 12

19 16 23 23 26 16 33 16 29 36 26 25 16

Mod everything by 26

19 16 23 23 0 16 7 16 3 10 0 25 16

CT = t q x x a q h q c k a z q

∴ Cipher Text = tqxxaqhqckazq

a mod N = (a+N) mod N

Page No.
Date

Decryption:

	19	16	23	23	0	16	7	16	3	10	0	25	16
−	12	12	12	12	12	12	12	12	12	12	12	12	12
	7	4	11	11	-12	4	-5	4	-9	-2	-12	13	4

mod everything by 26

	7	4	11	11	14	4	21	4	17	24	14	13	4

PT: helloeveryone

- Ceaser Cipher
  - In this cipher the value of key is not given, it is fixed to 3
  - key = 3

16/7 • Multiplicative Cipher

Encryption

- Plain text (P)
- Key (K)
- cipher (C) = (P * K) mod 26

Decryption

- Cipher
- key (K)
- plain Text (P) = $\left(\frac{C}{K}\right) \bmod N$

$= (C \times K^{-1}) \bmod N$

eg. P = Hello Everyone
Key = T = 19

— Encryption:

step 1: Convert P and K to integer

h	e	l	l	o	e	v	e	r	y	o	n	e
7	4	11	11	14	4	21	4	17	24	14	13	4

step 2: (P * K) mod 26

- h = (7 * 19) mod 26
  = 133 mod 26
  = 3
- e = (4 * 19) mod 26
  = 76 mod 26
  = 24
- l = (11 * 19) mod 26
  = 209 mod 26
  = 1
- l = (11 * 19) mod 26
  = 209 mod 26
  = 1
- o = (14 * 19) mod 26
  = 6
- r = (17 * 19) mod 26
  = 11
- n = (13 * 19) mod 26
  = 13
- y = (24 * 19) mod 26
  = 14

mode → decimal

calculator $(a - a/b \times b) = a \bmod b$

Page No.
Date

b	e	l	l	o	e	v	e	r	y	o	n	e
7	4	11	11	14	4	21	4	17	24	14	13	4
3	24	1	1	6	24	9	24	11	14	6	13	24

step 3: convert the integer back to char

3	24	1	1	6	24	9	24	11	14	6	13	24
d	y	b	b	g	y	j	y	l	o	g	n	y

∴ cipher : dybbgyjylognyy

— Decryption

$d = (3/19) \bmod 26$

$= 19^{-1} * 3 \bmod 26$

Forward

$19 * x = 1 \bmod 26$

$26 = 19(1) + 7$

$19 = 7(2) + 5$

$7 = 5(1) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

Reverse

$1 = 5 + 2(-2)$

$1 = 5 + [7 + 5(-1)](-2)$

$1 = 5(3) + 7(-2)$

$1 = [19 + 7(-2)](3) + 7(-2)$

$1 = 19(3) + 7(-8)$

$1 = 19(3) + [26 + 19(-1)](-8)$

$1 = 19(11) + 26(-8)$

Taking mod 26 on both the sides

$1 \bmod 26 = (19(11) + 26(-8)) \bmod 26$

$1 = (19(11) \bmod 26 + 26(-8) \bmod 26) \bmod 26$

- Property

$a = b$

(1) $a \bmod n = b \bmod n$

(2) $(a \pm b) \bmod n = (a \bmod n \pm b \bmod n) \bmod n$

(3) if $a \bmod n = b$

then

$(((a \bmod n) \bmod n) \bmod n \cdots)_{m\text{ times}} = b$

(4) $(b \times a) \bmod n \neq 0$

$1 = (19\,(11) \bmod 26 + 0)_{\bmod 26}$

$1 = (19\,(11) \bmod 26) \bmod 26$

$1 = 19\,(11) \bmod 26$

$\because 1 = 19 \times k^{-1} \bmod 26$

$\therefore \underline{k^{-1} = 11}$

Plain Text $(P) = C \times k^{-1} \bmod 26$

$d = (3 \times 11) \bmod 26 = 33 \bmod 26 = 7 \rightarrow h$

$y = (24 \times 11) \bmod 26 = 264 \bmod 26 = 4 \rightarrow e$

$b = (1 \times 11) \bmod 26 = 11 \bmod 26 = 11 \rightarrow l$

$b = (1 \times 11) \bmod 26 = 11 \bmod 26 = 11 \rightarrow l$

$g = (6 \times 11) \bmod 26 = 66 \bmod 26 = 14 \rightarrow o$

$y = (24 \times 11) \bmod 26 = 264 \bmod 26 = 4 \rightarrow e$

$j = (9 \times 11) \bmod 26 = 99 \bmod 26 = 21 \rightarrow v$

$y = (24 \times 11) \bmod 26 = 264 \bmod 26 = 4 \rightarrow e$

$l = (11 \times 11) \bmod 26 = 121 \bmod 26 = 17 \rightarrow r$

$o = (14 \times 11) \bmod 26 = 154 \bmod 26 = 24 \rightarrow y$

$g = (16 \times 11) \bmod 26 = 176 \bmod 26 = 14 \rightarrow o$

$n = (13 \times 11) \bmod 26 = 143 \bmod 26 = 13 \rightarrow n$

$y = (24 \times 11) \bmod 26 = 264 \bmod 26 = 4 \rightarrow e$

$\therefore P = \text{hello everyone}$

2017

Q Decrypt : abcdefgh , K=9 using multiplicative cipher

→

$C = (P * K) \bmod N$

$P = (C * K^{-1}) \bmod N$

$K * K^{-1} \bmod N = 1$

$g * x \bmod 26 = 1$

Forward

$26 = 9(2) + 8$

$9 = 8(1) + 1$

$8 = 1(8) + 0$

Reverse

$1 = 9 + 8(-1)$

$1 = 9 + [26 + 9(-2)](-1)$

$1 = 9(3) + 26(-1)$

taking mod 26 on both side

$1 \bmod 26 = 9(3) \bmod 26 + 26(-1) \bmod 26$

$1 = 9(3) \bmod 26$

Comparing with

$1 = 9 \times K^{-1} \bmod 26$

$\therefore K^{-1} = 3$

$PT = C \times K^{-1} \bmod 26 = C \times 3 \bmod 26$

a =

b =

c =

d =

e =

f =

g =

h =

Plain Text:

for small alphabet = 26 char
alpha numberic = 10 char

Page No.
Date

Q Decrypt:
C = otsfp2oz612jq
K = 7
PT ?

→

$PT = C \times K^{-1} \bmod N$

$K \times K^{-1} \bmod N = 1$

$7 \times x \bmod 36 = 1$

Forward

$36 = 7(5) + 1$

$7 = 1(7) + 0$

Reverse

$1 = 36 + 7(-5)$

mod 36 on both side

$1 = 7(-5) \bmod 36$

$x = -5$

Negative not take

$= -5 + 36$

$x = 31$

$\therefore K^{-1} = 31$

$PT = C \times K^{-1} \bmod 36$

o = (14 × 31) mod 36 = 2 = c
t = (19 × 31) mod 36 = 13 = n
s = (18 × 31) mod 36 = 18 = s
f = (5 × 31) mod 36 = 11 = l
2 = (27 × 31) mod 36 = 4 = e
o = (14 × 31) mod 36 = 2 = c
z = (25 × 31) mod 36 = 19 = t
6 = (30 × 31) mod 36 = 20 = u
l = (11 × 31) mod 36 = 17 = r
2 = (27 × 31) mod 36 = 4 = e
j = (9 × 31) mod 36 = 27 = 1
q = (16 × 31) mod 36 = 28 = 2

∴ Plain Text (P) = cnslecture12

Q Decrypt: 560xbdq using multiplicative cipher
N = 36
key = 11
PT = ?

- Affine cipher
  - It is a combination of (Additive + Multiplicative)
  - Encryption
    - Plain Text (P)
    - Key (a, b)
    - cipher (c) = (P * a + b) mod 26
  - Decryption

eg: P = Hello Everyone
K = (11, 3)

step 1: convert P and K to integer

h	e	l	l	o	e	v	e	r	y	o	n	e
7	4	11	11	14	4	21	4	17	24	14	13	4

step 2: cipher = (P * a + b) mod 26
h = (7 * 11 + 3) mod 26 = 80 mod 26 = 2

h	e	l	l	o	e	v	e	r	y	o	ne
7	4	11	11	14	4	21	4	17	24	14	13 4
2	21	20	20	1	21	0	21	8	7	1	16 21

Step 3: Convert integer back to char

2	21	20	20	1	21	0	21	8	7	1	16 21
c	v	u	u	b	v	a	v	i	h	b	q v

∴ cipher Text = cvuubvavihbqv

— Decryption