Cryptography

Chapter-01

Content:

- CIA tried
- Security attacks
- Security services
- Security mechanisms
- Cryptography

CIA tried:

Confidentiality: preserving authorized restrictions on access and disclosure -

Integrity: data is complete, trustworthy and has not been modified and be modified by authorized users

Availability: it is available at 24 by 7 and not denied by authorized users

Confidentiality and privacy:

Confidentiality: be sure that private information is not made available

Privacy: involves your right to manage your personal information

System Integrity: it is designed, implemented and maintained to protect itself against unauthorized access

Authentication: assurance that the user who claims to be

Non-repudiation: assurance that participant cannot deny their actions

Access control: the ability to limit and control the access to user, systems and application and prevent misuse of resources

Security attacks:

- Passive attacks
- Active attacks

Passive attacks:

- The goal of the opponent is to learn the information
- System resources is not affected
- Very difficult to detect as there is no alteration of messages
- Emphasis is given to prevent passive attacks than to detect them

Decryption

Ciphertext= rjjy key= 5

For r, (17-5) mod 26= 12 mod26=12, m
For j, (9-5)mod 26= 4mod26=4,e
For y, (24-5)mod 26= 19, t

Plaintext= meet

Meet me - rjjy rj - monoalphabetic substitution

Meet me – xfwu hj- polyalphabetic

Mod Operator

5/4= Q=1 , Remainder=1

5 mod 4 = 1 6 mod 4=2 7 mod 4= 3 8 mod 4= 0 4mod4= 0 3 mod 4= 3 2mod4= 2
1mod4=1 35mod4=3 234mod4= 2 6574 mod 4=2 453421 mod 4=1

N mod 4 --→ 0,1,2,3

N mod 6-----→0,1,2,3,4,5

N mod 9 -----→ 0 ,1,2--- , 8

N mod 26--→ 0 to 25

625 mod 6= 1 12 mod 6= 0 15 mod 6= 3 26 mod 6= 2 1mod6=1 11mod6= 5 10 mod 6= 4 45678 mod 6= 0

l	11	T=(11*7)mod 26= 25	C=(25+2)mod26=1	B
l	11	T=(11*7)mod 26= 25	C=(25+2)mod26=1	B
o	14	T=(14*7)mod26=20	C=(20+2)mod26=22	W

Transposition cipher: rail fence technique: the plaintext is written down as a sequence of diagonals and read off as sequence of rows

Exp:

Plain Text= meet me after the toga party

m e m a t r h t g p r y

e t e f e t e o a a t

Ciphertext= MEMATRHTGPRYETEFETEOAAT

Playfair cipher:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as X, so that BALLOON would be treated as BA LX LO ON

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, AR is encrypted as RM.

3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, MU is encrypted as CM.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, HS becomes BP and EA becomes IM (or JM, as the encipherer wishes).

Example

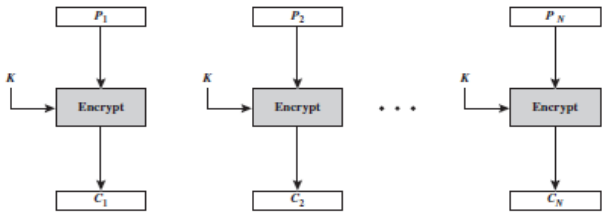
KEY=MONARCHY Plaintext = BALLOON

Step-1 Create matrix

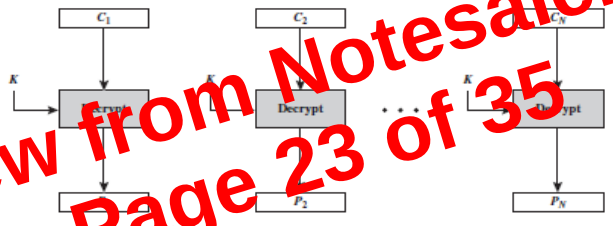
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

The difference between OFB and CTR: the input to encryption is different in OFB is nonce and it is fixed in all rounds and in CTR is counter which different in length which depends on plaintext length

EBC



(a) Encryption



(b) Decryption

Figure 6.3 Electronic Codebook (ECB) Mode

CFB

Authentication using public key encryption:

1. Encrypt the message using sender's private key
2. Transmit the message
3. Decrypt the message using sender's public key

Uses of public key encryption:

1. Encryption
2. Digital signature
3. Key exchange

Public key encryption using one way function: it is easy to implement but difficult to revers

Exp: integer factorization problem, Discrete logarithm Problem

Possible attacks:

- Brute force attack: large keys are used to defeat it
- Probable message attack (perform encryption of the entire possible key size)

Advantages and disadvantages of public key encryption:

Advantages:

- There is no need to share the private key because the key is used only by the owner
- Private and public key pair can remain unchanged for amount of time depend on the mode of usage
- In a network, number of keys to be managed is smaller than that of asymmetric encryption key scheme
- Public key encryption can be used to create digital signature mechanisms

Disadvantages:

- Public key encryption is slower than well-known symmetric key encryption
- Key size is larger than required for symmetric key encryption
- The security of public key encryption depends on the hardness of mathematical problems

Hybrid encryption scheme: merging two different encryption schemes to build stronger encryption scheme