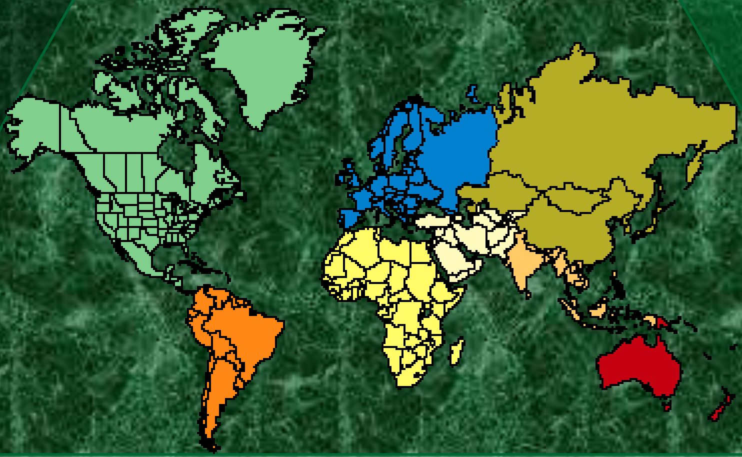
LECTURE 2



Introduction

- Plaintext – Message to be transformed.

- Ciphertext – Transformed message.

- Encryption – Plaintext → Ciphertext
- Decryption – Ciphertext → Plaintext

- Key – Information used in cipher known only to sender and receiver.
- Encryption & decryption are done using keys.

- Cipher – A particular encryption scheme.
- Cryptography – Study of algorithms used for encryption.
- Cryptanalysis – Techniques for deciphering the encrypted data without prior knowledge of which key has been used.
- Cryptology consists of the areas of cryptography and cryptanalysis together.

- Two general approaches for attacking a conventional encryption scheme.
  - Cryptanalysis
  - Brute-force attack – Tries every possible key on a piece of ciphertext.

- Cryptanalytic attacks are of four types:
  - Ciphertext only attack
  - Known plaintext attack
  - Chosen plaintext attack
  - Chosen ciphertext attack

- Ciphertext only attack
  - Attacker has access to a set of ciphertexts.
  - Attacker has the least amount of information to work with.
  - Attack is successful if the corresponding plaintexts and key can be deduced.

- Known plaintext attack
  - Attacker has samples of both the plaintext and the corresponding ciphertext.
  - Aim is to deduce the key using this information.

- Chosen plaintext attack
  - Attacker is able to define his own plaintext, feed it into the cipher & analyze the resulting ciphertext.
  - This attack requires the attacker to be able to send data to the encryption device & view the output from the device.
  - Impossible to attempt in most cases.
  - But it can happen if attacker gets access to the encryption device.

- Chosen ciphertext attack

  -Attacker choose the cipher text feed it to the cipher and get the plain text.

  - It can happen if he has the access to the cipher.

- Cipher text only attack < known plaintext attack < chosen plaintext attack < chosen cipher text attack

- Unconditionally secure :- If the ciphertext generated doesn’t contain enough information to decrypt.

- Computationally secure :-
  - The cost of breaking cipher exceeds the value of encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of information.

Classification of Cryptographic Algorithms

- Classification based on the number of keys.
- Symmetric Key Encryption
  - Same key is used for encryption & decryption.
  - Also termed as Private Key Cryptography.

- Asymmetric Key Encryption
  - Two different keys are used for encryption & decryption.
  - Also termed as Public Key Cryptography.

Conventional vs Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Classical cipher systems

- Classification based on the type of operations used for transforming.

- Two types:
  - Substitution Ciphers – Letters of plaintext are replaced by other letters.

  - Transposition Ciphers – Letters of plaintext are rearranged.

- Substitution ciphers are two types mono alphabetic and poly alphabetic.

- The relationship between a character in the plaintext to character in the ciphertext is always one to one.

- The relationship between a character in the plaintext to character in the ciphertext is always one to many.

Classical cipher systems

- Can also be classified as based on the way in which the plaintext is processed.
  - Stream Ciphers – Converts one symbol of plaintext immediately into a symbol of ciphertext.
  - Block Ciphers – Converts a block of plaintext symbols to blocks of ciphertext.

Monoalphabetic Substitution Ciphers

- Additive Cipher
  - Caesar Cipher or Shift Cipher – Each letter is replaced by a letter standing at a fixed number of places after it in the alphabet.
  - Plaintext: a b c d e ……………x y z

- We can assign numerical equivalent to each letter.
- Plaintext,ciphertext and key are integers in Z_{26}
- General Caeser algorithm
  - $C = E(p) = (p+k) \bmod 26$
- Decryption algorithm is
  - $p= D(C) = (C-k) \bmod 26$
- If we use a shift of 3 then
  - $C = E(p) = (p + 3) \bmod 26$

- Use the additive cipher with key = 15 to encrypt the message "hello".

Plaintext: h $\to$ 07	Encryption: $(07 + 15) \bmod 26$	Ciphertext: 22 $\to$ W
Plaintext: e $\to$ 04	Encryption: $(04 + 15) \bmod 26$	Ciphertext: 19 $\to$ T
Plaintext: l $\to$ 11	Encryption: $(11 + 15) \bmod 26$	Ciphertext: 00 $\to$ A
Plaintext: l $\to$ 11	Encryption: $(11 + 15) \bmod 26$	Ciphertext: 00 $\to$ A
Plaintext: o $\to$ 14	Encryption: $(14 + 15) \bmod 26$	Ciphertext: 03 $\to$ D

- Use the additive cipher with key = 15 to decrypt the message “WTAAD”.

Ciphertext: W $\rightarrow$ 22	Decryption: (22 − 15) mod 26	Plaintext: 07 $\rightarrow$ h
Ciphertext: T $\rightarrow$ 19	Decryption: (19 − 15) mod 26	Plaintext: 04 $\rightarrow$ e
Ciphertext: A $\rightarrow$ 00	Decryption: (00 − 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: A $\rightarrow$ 00	Decryption: (00 − 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: D $\rightarrow$ 03	Decryption: (03 − 15) mod 26	Plaintext: 14 $\rightarrow$ o

- Vulnerable to Ciphertext only attack using Bruteforce attack.
- There are only 25 keys to try.
- They are also vulnerable to statistical attacks.

Table : Frequency of characters in English

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Table : Frequency of diagrams and trigrams

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Eve has intercepted the following ciphertext

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on.

Corresponding plaintext

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Multiplicative Ciphers

- Encryption – multiplication of the plaintext by the key.
- $C = (P \times K) \bmod 26$

- Decryption – division of the ciphertext by the key.
- $P = (C \times K^{-1}) \bmod 26$

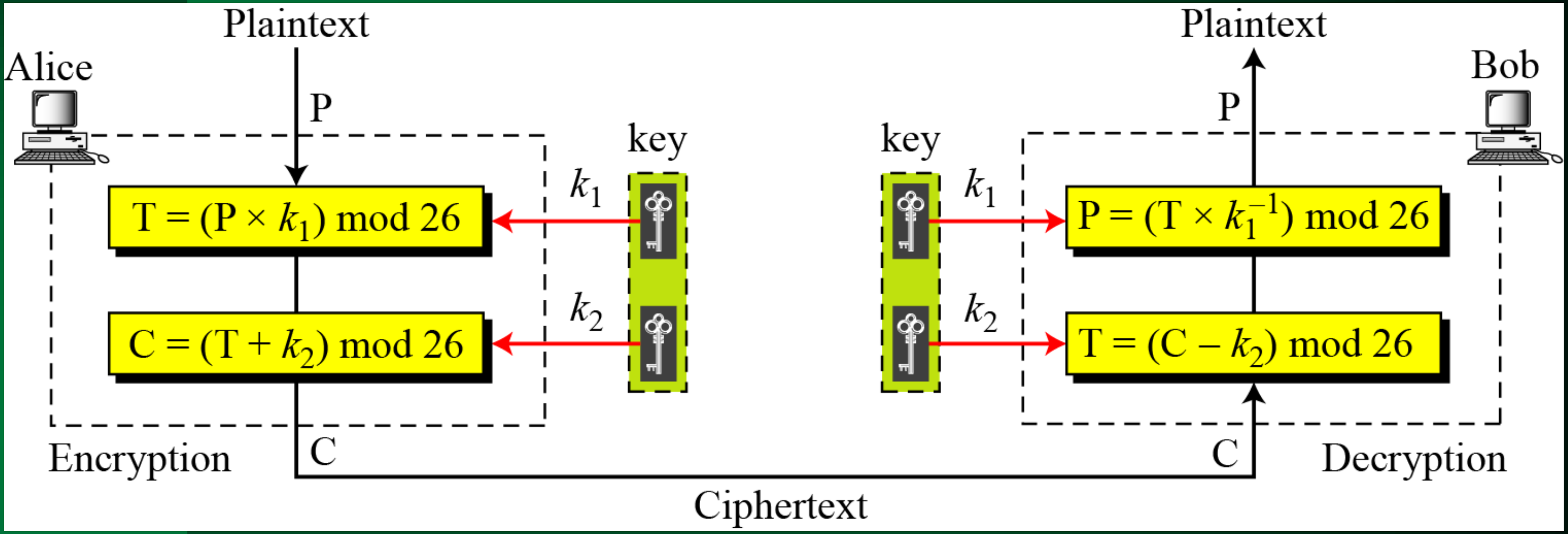
- Since the operations are in Z_{26} ,decryption is done by multiplying the multiplicative inverse of the key.
- Key domain ?

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

Affine Cipher

- It's a combination of additive and multiplicative cipher with a pair of keys.
- The first key is used with multiplicative cipher and the second one with the additive one.

Fig: Affine Cipher



$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

Size of the key domain ?

Use an affine cipher to encrypt the message “hello” with the key pair (7, 2).

P: h $\rightarrow$ 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 $\rightarrow$ Z
P: e $\rightarrow$ 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 $\rightarrow$ E
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: o $\rightarrow$ 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 $\rightarrow$ W

Corresponding decryption

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 $\rightarrow$ o

- Chosen plaintext attack

- Algorithm 1 : PT = et CT = WC
- Algorithm 2 : PT = et CT = WF
- Alg 1: 4 -> 22 and 19 -> 02
- $(04 \times k1 + k2) \equiv 22 \bmod 26$
- $(19 \times k1 + k2) \equiv 02 \bmod 26$

$$\begin{bmatrix} k1 \\ k2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 16 \\ 10 \end{bmatrix}$$

- k1 = 16 and k2 = 10

- Alg 2 : 4 -> 22 and 19 -> 05
- $(04 \times k1 + k2) \equiv 22 \mod 26$
- $(19 \times k1 + k2) \equiv 05 \mod 26$

- k1 = 11 and k2 =4
- Now using the inverse of these key values attacker is able to decrypt.

- Statistical attack

- Suppose the frequency of letters in CT is as follows R= 8,D= 7 ,E,H,K=5 , F,S,V = 4
- R <- e and D <- t
- 17 <- 4 and 03 <- 19
- $(04 \times k1 + k2) \equiv 17 \bmod 26$
- $(19 \times k1 + k2) \equiv 03 \bmod 26$
- k1 = 6 and k 2 = 19
- Since k1 doesn't have a multiplicative inverse we go for the next guess

- Next guess R -> e and E -> t , k1 = 13
- Next guess R -> e and H -> t , k1 = 8
- Next guess R -> e and K -> t , k1 = 3 and k2 = 5
- Now the message can be decrypted using the inverse of these key values.