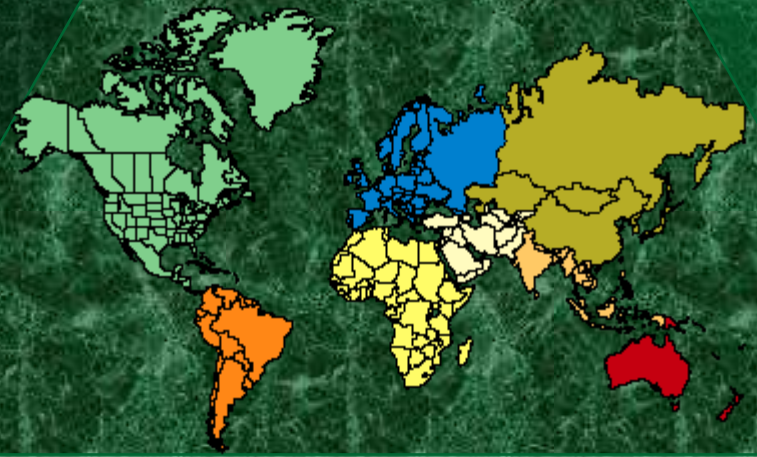
LECTURE 2



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.

- 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 → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

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

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → 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.
- $P = (C \times K^{-1}) \bmod 26$

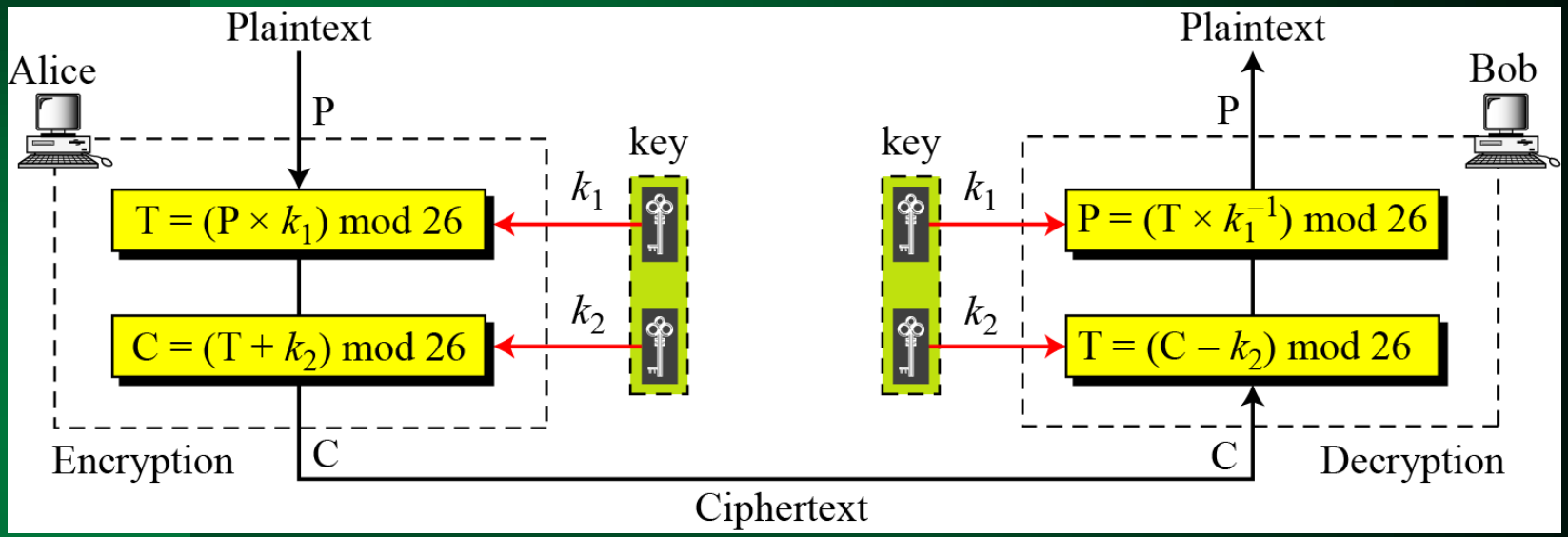
- Since the operations are in Z_{26} ,decryption is done by multiplying the multiplicative inverse of the key.
- Key domain ?

Plaintext: h → 07	Encryption: (07 × 07) mod 26	ciphertext: 23 → X
Plaintext: e → 04	Encryption: (04 × 07) mod 26	ciphertext: 02 → C
Plaintext: l → 11	Encryption: (11 × 07) mod 26	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: (11 × 07) mod 26	ciphertext: 25 → Z
Plaintext: o → 14	Encryption: (14 × 07) mod 26	ciphertext: 20 → 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 → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 → W

Corresponding decryption

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

- Chosen plaintext attack

- Algorithm 1 : PT = et CT = WC
- Algorithm 2 : PT = et CT = WF
- Alg 1: 4 -> 22 and 19 -> 02
- (04 ×k1 + k2) ≡ 22 mod 26
- (19 × k1 + k2) ≡ 02 mod 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
- $(04 \times k1 + k2) \equiv 22 \bmod 26$
- $(19 \times k1 + k2) \equiv 05 \bmod 26$

- 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 ×k1 + k2) ≡ 17 mod 26
- (19 × k1 + k2) ≡ 03 mod 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.

Polyalphabetic Ciphers

- Polyalphabetic cipher - Different substitution alphabets are used for the same alphabet in plaintext based on a key value.
- Playfair Cipher
- Multiple letter encryption cipher.
- Treats digrams in the plaintext as single units.
  - Encryption is done based on the use of a 5X5 matrix of letters constructed using a keyword.

- The matrix is constructed by filling in the letters of the keyword from left to right & from top to bottom.
- Then fill the remainder of the matrix with the remaining letters in alphabetic order.
- Letters I & J are counted as one letter.

- If the no of plaintext characters is odd insert bogus character.
- Plaintext is encrypted two letters at a time as follows:

  - If a pair is a repeated letter, insert bogus character like ‘X’.

  - If both letters fall in the same row, replace each with letter to right (wrapping back to start from end) .

- If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)

- Else, each letter is replaced by the letter in the same row and in the column of the other letter of the pair.

- Ex:- Keyword is MONARCHY

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

- Ex:- Keyword is MONARCHY

- AR is encrypted as RM.
- MU is encrypted as CM.
- HS is encrypted as BP.
- EA is encrypted as IM or JM.

Encrypt the following

- MEET ME HERE TODAY
- The digrams are, ME ET ME HE RE TO DA YX, ciphertext will be, CL KL CL CF MK PR BR BW

- Bruteforce attack is difficult (size of the key domain is 25!)
- Encipherment hides frequency of single characters.
- Ciphertext only attack based on the diagram frequency is possible.

Substitution Ciphers (contd.)

- Vigenere Cipher
  - It’s a combination of m additive ciphers.
  - Key stream is a repetition of initial key stream of length m where $1 \leq m \leq 26$

- Encryption

$$C_i = (P_i + K_i) \bmod 26$$

- Decryption

$$P_i = (C_i - K_i) \bmod 26$$

- Eg:We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P’s values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C’s values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

- Encryption is done with the help of Vigenere table as follows:
  - Locate the plaintext letter on the top row.
  - Locate the key letter on the side column.
  - Encrypt the letter using the letter at the intersection of the row & column.
  - To encrypt the key needed is as long as the message.
  - Usually key will be repeating keyword.

- Decryption

- Key letter identifies the row.
- The position of the ciphertext letter in that row determines the column.
- Plain text letter is on top of that column.

Vigenere Table

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

- Strength : Multiple cipher text letters for each plaintext letter.
- Do not preserve the frequency of characters.
- Repeated sequence of cipher text because of periodic nature of the keyword.

- Cryptanalysis consist of two parts

- Find the length of the key
- Finding the key

- Key length is found using kasiski test.

- Based on the observation that two identical PT segments will be encrypted to the same ciphertext if they are ‘d’ positions apart in PT where m | d .

- If more segments can be found within distances d1,d2,d3….dn then m | (d1,d2,…..dn) .
- Once keylength has been found , CT is divided into m pieces.
- They can be cryptanalyzed separately

- Assume that the following is the intercepted cipher text

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQH-
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVWVWJWIXGFWLTSHGJOUEEHH-
VUCFVGOWICQLTJSUXGLW

- The kasiski test is as follows

String	*First Index*	*Second Index*	*Difference*
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

- The greatest common divisor of differences is 4.
- Try m = 4.

```
C1: LWGWCRAOKTEPGTQCTJVUEGVGUQGECVPRPVJGTJEUGCJG
P1: jueuapymircneroarhtsthihytrahcieixsthcarrehe
C2: IGGGQHGWGKVCTSOSQSWVWFVYSHSVFSHZHWWFSOHCOQSL
P2: usssctsiswhofeaeceihcetesoecatnpntherhctecex
C3: OFDHURWQZKLZHGVVLUVLSZWHWKHFDUKDHVIWHUHFWLUW
P3: lcaerotnwhiwedssirsiirhketehretltiideatrairt
C4: MEVHCWILEMWVVXGETMEXLMLCXVELGMIMBWXLGEVVITX
P4: iardysehaisrrtcapiafpwtethecarhaesfterectpt
```

Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher. It is an additive cipher with the key set to three. Each character in the plaintext is shifted three characters to create ciphertext.

Vernam Cipher

- It’s a symmetrical stream cipher
- System works on binary data other than letters.
- The key used is random key as long as the message .

- Ci = Pi (XOR) Ki
- Pi = Ci (XOR) Ki

- It’s breakable if the key is repeated
- If PT_1 and PT_2 encrypted using the same key, then CT_1 (XOR) CT_2 = PT_1 (XOR) PT_2

One-Time Pad

- An improvement to Vernam cipher.
- Use a random key as long as the message with no repetitions.
- Each new message requires a new key as long as the message.
- Ideal cipher
- Produces random output that has no statistical relationship with the plaintext.

- Advantages
- Easy to compute
- Secure iff the key sequence is random

- Fundamental Difficulties
- Practical problem of making large number of random keys.
- Problem of key distribution and protection.

Hill Cipher

- PT is divided into equal size blocks.
- Key is a square matrix of m × m size where m is the size of the block.
- Substitution is determined by m linear equations.
- Each character is assigned a numerical equivalent.
  - Uses matrix multiplication to generate the ciphertext.

- Encryption is done as, C = KP mod 26 where K is an ***mXm*** matrix representing the encryption key & C and P are column vectors of length ***m***.

- For hill cipher to work K should have an inverse

- Eg:-Plaintext: HATS , m=2
- Key matrix: $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$$K \begin{bmatrix} 7 \\ 0 \end{bmatrix} = \begin{bmatrix} 21 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 21 \\ 14 \end{bmatrix} = VO$$

- Finally, ciphertext will be VOHY

- Theorem : K has an inverse iff det K is invertible in Z_{26} ie (det K, 26) = 1.

- $K^{-1} = (\det K)^{-1} \begin{bmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{bmatrix}$

- $\det K = 3 \times 5 - 3 \times 2 = 9$
- $(\det K)^{-1}$, $9 \times X \equiv 1 \bmod 26$ which is equal to 3.
- $$3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$ Decryption key

- CT : “VOHY “
- $$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 21 \\ 14 \end{bmatrix} = \begin{bmatrix} 553 \\ 546 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 \\ 0 \end{bmatrix}$$

- It completely hides single letter frequency information.
- Use of large matrix hides more frequency information.
- Strong against ciphertext only attack.
- Cannot defend known plaintext attack.

- Eve should know the value of m and PT<->CT pairs for at least m blocks.
- Eve can create two m × m matrices of PT and CT.
- $K = P^{-1} C$ if P is invertible.

Transposition (Permutation) Ciphers

- Rail fence technique (Keyless Transposition Cipher)
  - Arrange the plaintext charatcters as a sequence of diagonals.
  - Read off as a sequence of rows.
  - No of rows is fixed.

Transposition Ciphers (contd.)

- Eg:-

  Plaintext : MEET ME HERE

  M E M H R

  E T E E E

  Ciphertext: MEMHR ETEEE

Encrypt the following

- COME HOME TOMORROW
- CMHM TMRO OEOE OORW

Transposition Ciphers (contd.)

- Columnar Transposition
  - Write the characters of plaintext in rows.
  - Form the ciphertext by reading down the column.
  - If the message length is not a multiple of the chosen no, a special character or alphabets can be used to fill in any short column.

Transposition Ciphers (contd.)

- Eg:
  - Plaintext: THIS IS A SAMPLE MESSAGE
  - Choose number to be 5.

    T H I S I

    S A S A M

    P L E M E

    S S A G E
  - Ciphertext: TSPS HALS ISEA SAMG IMEE

Encrypt the following

- COME HOME TOMORROW
- Choose number to be 4.

  C O M E

  H O M E

  T O M O

  R R O W

- CHTR OOOR MMMO EEOW

- Keyed Transposition Ciphers
- Write the message row wise.
- Read the message column wise, but can change the order of the columns.
- The order of columns then became the key value.

- COME HOME TOMORROW
- Key is 4, 6, 1, 2, 5, 3

  4 6 1 2 5 3

  C O M E H O

  M E T O M O

  R R O W $ $

- MTO EOW OO$ CMR HM$ OER