UNIVERSITY OF RAJSHAHI

Rajshahi, BANGLADESH.

Course Code:

ICE-4221

Course Title :

Cryptography and Network security

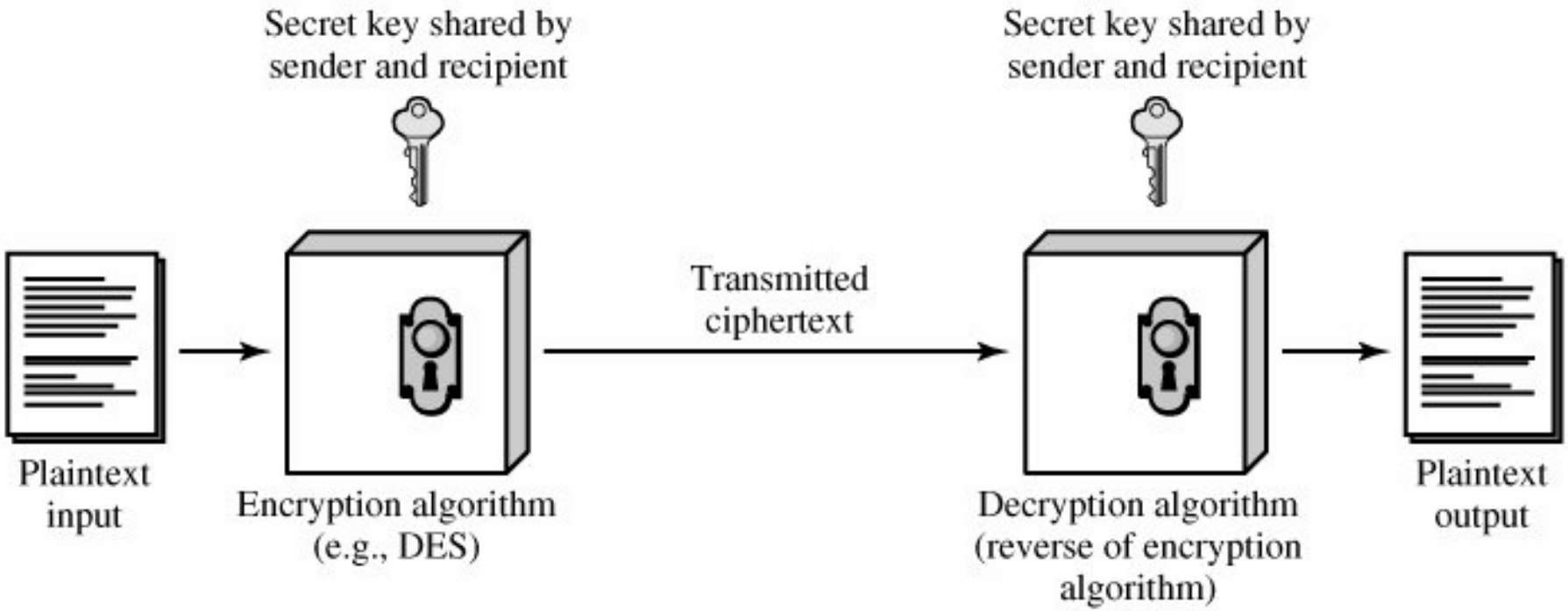
Classical Encryption Techniques

Key Points

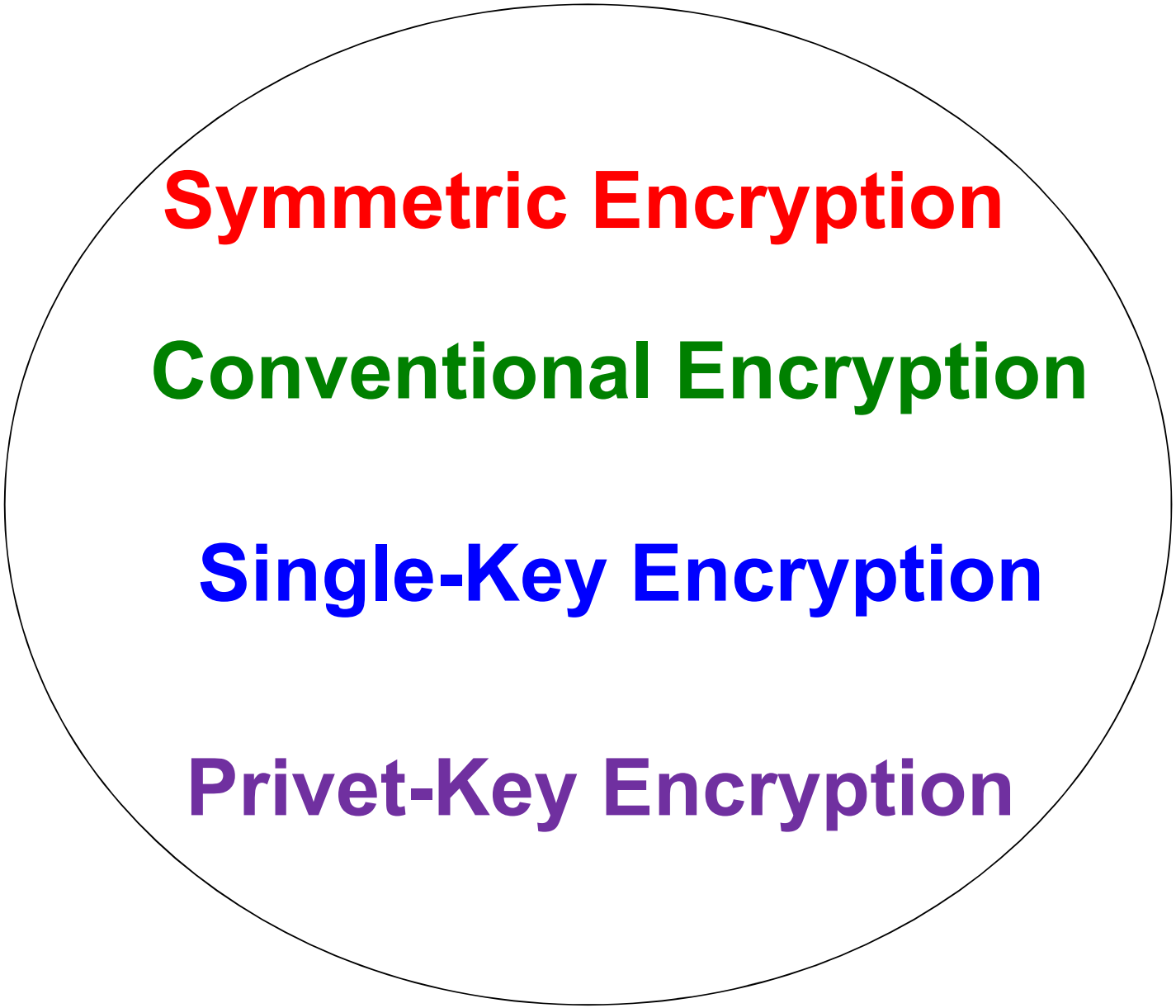
- ✓**Plaintext**,
- ✓**Ciphertext**.
- ✓**Enciphering** or **Encryption**;
- ✓**Decryption**.

Symmetric Cipher Model

A symmetric encryption has **FIVE** ingredients:



- Plaintext ,
- Encryption algorithm,
- Secret key,
- Ciphertext,
- Decryption algorithm:



Same Types

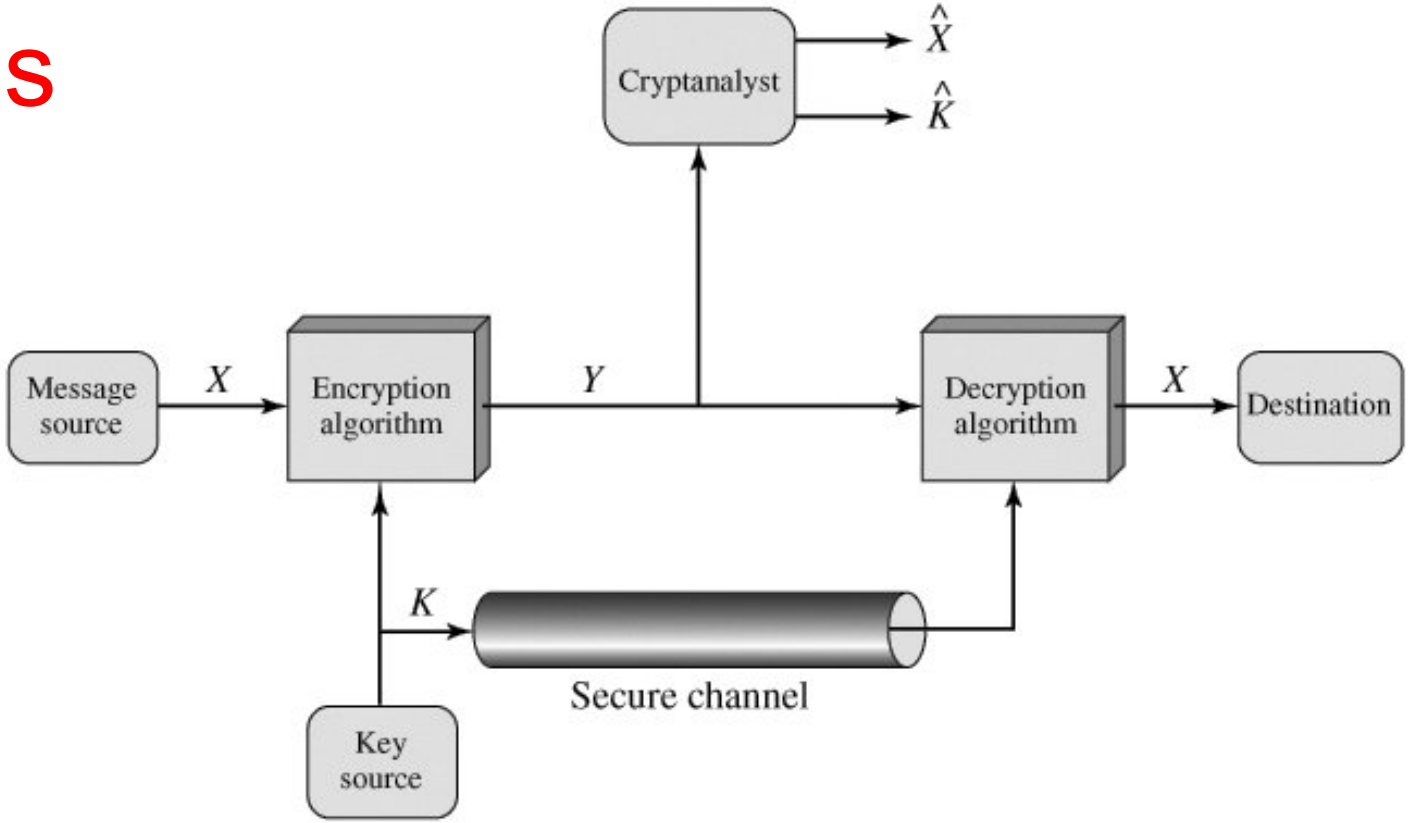
- ✓ **Later, during 1970, Public-Key Encryption system is developed.**

Requirements for Secure Use of Symmetric Encryption

✓Strong encryption algorithm is needed.

✓Sender and receiver must have obtained copies of the secret key in a **SECURE FASHION** and must keep the key secure.

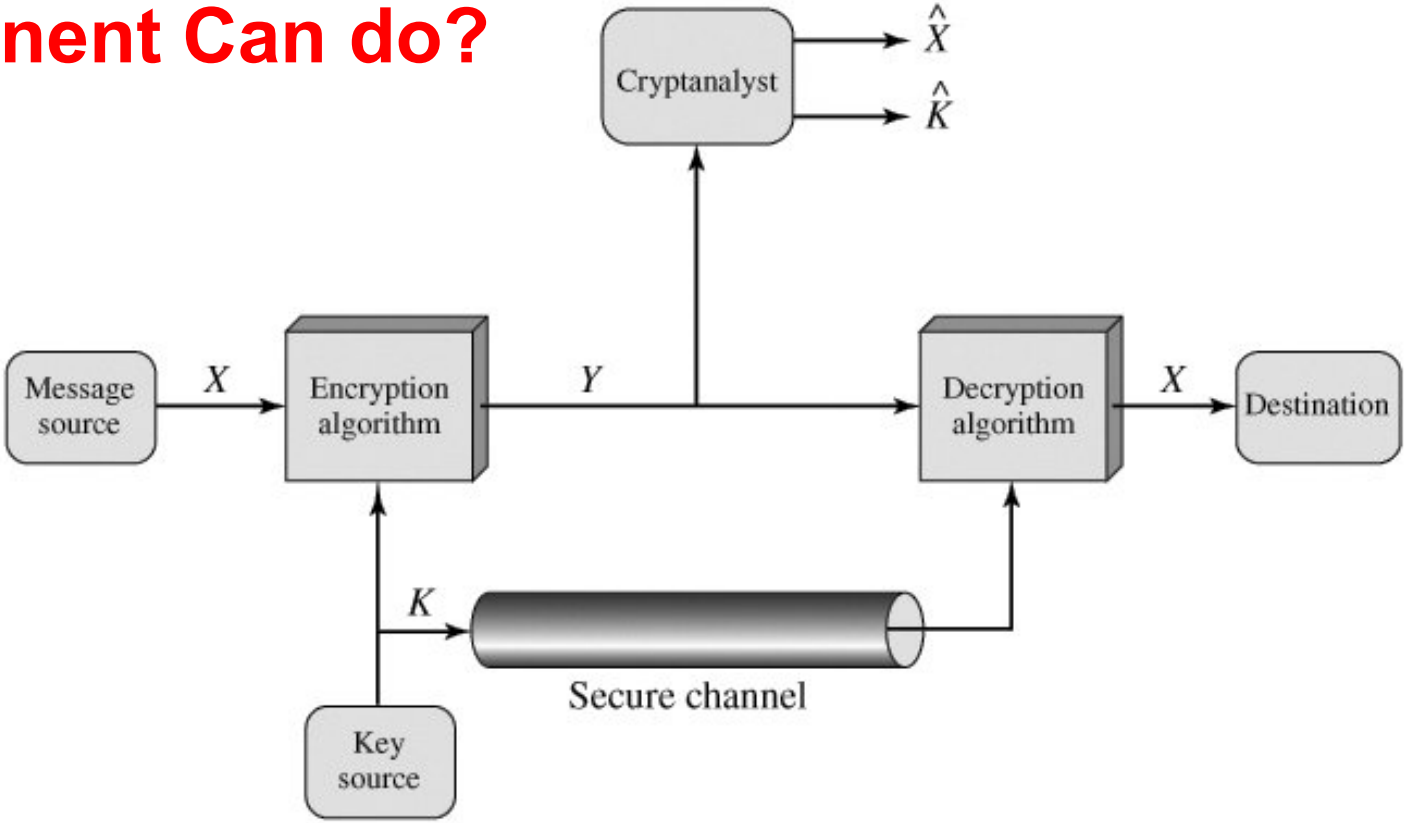
Examples



Model of Conventional Cryptosystem

- A source produces a message in plaintext, $\mathbf{X = [X_1, X_2, ..., X_M]}$.
- For encryption, a key of the form $\mathbf{K = [K_1, K_2, ..., K_J]}$ is generated.
- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext $\mathbf{Y = [Y_1, Y_2, ..., Y_N]}$. We can write this as $\mathbf{Y = E(K, X)}$

What Opponent Can do?



Model of Conventional Cryptosystem

An opponent,

- May observe **Y** but not having access to **K** or **X**,
- May attempt to recover X or K or both X and K.
- It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms.
- **If the opponent is interested in only this particular message**, then the focus of the effort is to recover X by generating a plaintext estimate.
- Often, however, **the opponent is interested in being able to read future messages as well**, in which case an attempt is made to recover **K** by generating an estimate.

Cryptography

Cryptographic systems are characterized along THREE independent dimensions:

1. **The type of operations used for transforming plaintext to cipher text.**
   - ✓ Substitution
   - ✓ Transposition
2. **The number of keys used.**
   - ✓ Single Key: **symmetric, single-key, secret-key, or conventional encryption.**
   - ✓ Different Key: **asymmetric, two-key, or public-key encryption**
3. **The way in which the plaintext is processed.**
   3. **Block Ciphering**
   4. **Stream Ciphering**

Cryptanalysis

Objective of attacking an encryption system is to recover the key in use rather then simply to recover the plaintext of a single ciphertext.

There are **TWO** general approaches to attacking a conventional encryption scheme:

✓**Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.

✓**Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	▪Encryption algorithm ▪Ciphertext
Known plaintext	▪Encryption algorithm ▪Ciphertext ▪One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	▪Encryption algorithm ▪Ciphertext ▪Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	▪Encryption algorithm ▪Ciphertext ▪Supposed ciphertext chosen by cryptanalyst, together with corresponding decrypted plaintext generated with the secret key.
Chosen text	▪Encryption algorithm ▪Ciphertext ▪Plaintext message chosen by cryptanalyst, together with corresponding ciphertext generated with the secret key ▪Supposed ciphertext chosen by cryptanalyst, together with corresponding decrypted plaintext generated with the secret key

An encryption scheme is……

- **Unconditionally secure**

  If the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. That is, no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext, simply because the required information is not there.

- **Computationally Secure**

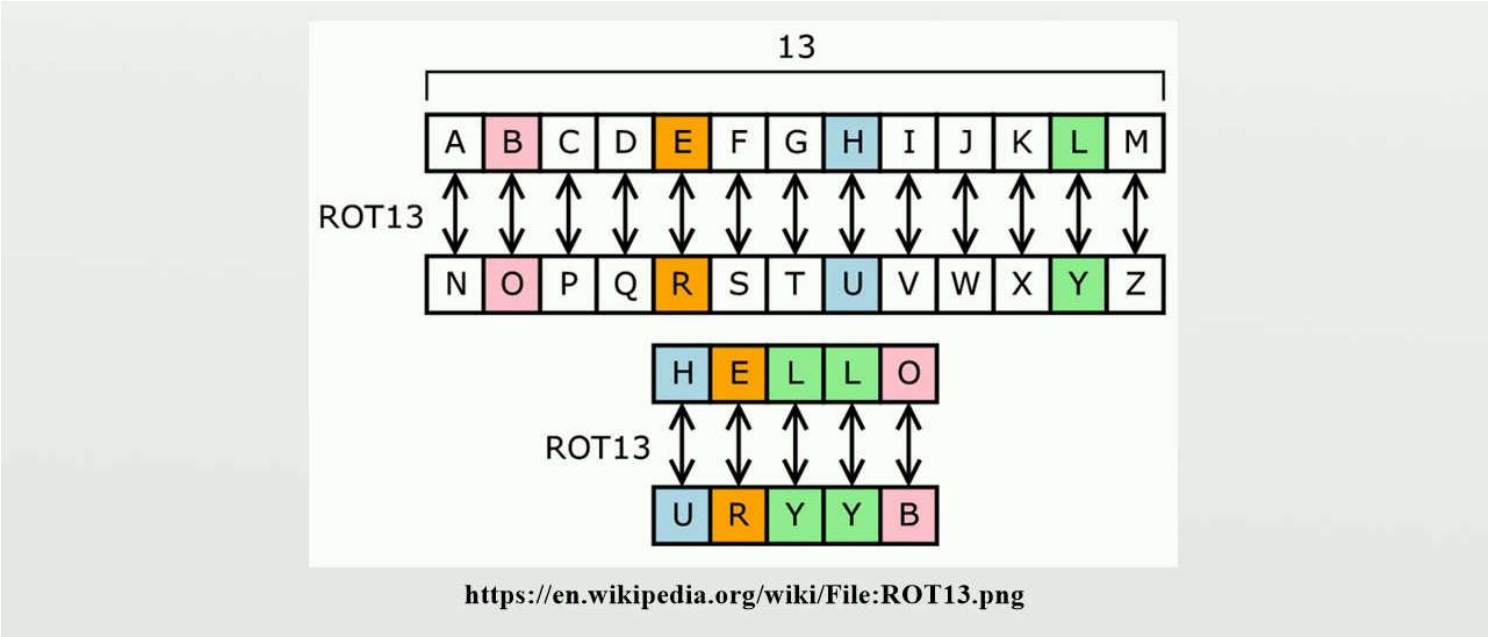
  If either of the following two criteria are meet….

i) The cost of breaking the cipher exceeds the value of the encrypted information.

ii)The time required to break the cipher exceeds the useful lifetime of the information

Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.



https://en.wikipedia.org/wiki/File:ROT13.png

Substitution Techniques

Caesar Cipher

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB ,

✓Note that the alphabet is **WRAPPED AROUND**, so that the letter following Z is A.

✓We can define the transformation by listing all possibilities, as follows:

plain: 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

cipher: 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

Caesar Cipher (cont')

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:

$$C = E(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is $C = E(k, p) = (p + k) \bmod 26$

where k takes on a value in the range 1 to 25.

The decryption algorithm is simply

$$p = D(k, C) = (C - k) \bmod 26$$

Caesar Cipher (cont')

If it is known that a given ciphertext is a Caesar cipher, then a **BRUTE-FORCE CRYPTANALYSIS** is easily performed: Simply try all the 25 possible keys.

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd

- ✓Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:
  - ➢The encryption and decryption algorithms are known.
  - ➢There are only 25 keys to try.
  - ➢The language of the plaintext is known and easily recognizable.

Substitution Techniques

Playfair Cipher

- The best-known **multiple-letter encryption cipher** is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- The Playfair algorithm is based on the use of a **5 x 5 matrix** of letters constructed using a keyword
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

SKIP

Substitution Techniques

Playfair Cipher

Preparing the plaintext

Prepare specific information
E.g. Shi Sherry loves Heath Ledger

Choose encryption key
E.g. Sherry

SKIP

Substitution Techniques

Playfair Cipher

Preparing the plaintext

- All the letters should be written
  - in capital letter,
  - in pairs,
  - without punctuation,
  - All Js are replaced with Is.

Plaintext: Shi Shasy lovs Heath Ledger

→SH IS HE RR YL OV ES HE AT HL ED GE R

- Double letters which occur in a pair must be divided by an X or a Z.

  E.g. LI TE RA LL Y→**LI TE RA LX LY**

→SH IS HE **RX RY** LO VE SH EA TH LE DG ER

SKIP

Substitution Techniques

Playfair Cipher

Preparing the Key

- present with an alphabet square
- 5*5
- No repeat letter
- No Js
- KEY: SHERRY→

SKIP

Substitution Techniques

Playfair Cipher

3 Rules to Prepare Ciphertext

- **Letters appear on the same row:** replace them with the letters to their immediate right respectively
- **Letters appear on the same column:** replace them with the letters immediately below respectively
- **not on the same row or column:** replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.
- **The order is important – the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter.**

SKIP

Substitution Techniques

Playfair Cipher

Plaintext:

SH IS HE RX RY LO VE SH LA TJ LE DG ER

Key Matrix:

S H E R Y

A B C D F

G I K L M

N O P Q T

U V W X Z

SKIP

Final ciphertext :

HEGHERDRYSIQWHHESCOYKRALRY

Substitution Techniques

Playfair Cipher

Decipher

- Shift up and left instead of down and right
- Drop extra X
- Locate any missing any “I”s that should be “J”s
- Back into the original readable message .

SKIP

Transposition Techniques

- All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol.
- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Transposition Techniques

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

For example, to encipher the message:

"meet me after the toga party" with a rail fence of depth 2, we write the following:

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

The encrypted message is:

MEMATRHTGPRYETEFETEOAAT

One-Time Pad

- Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.
- In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message. Such a scheme, known as a **one-time pad**, is unbreakable.
- It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

One-Time Pad (Cont')

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

✓There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.

✓Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.