Basics of Cryptography

Ms. Swati Mali

swatimali@somaiya.edu

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya TRUST

Module 1

Introduction to Information Security & Cryptography		**07**	**CO 1**
1.1	Information Security and its goals, Vulnerability Threats and Attacks, Security services and security mechanisms		
1.2	Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Types of keys, Cryptanalysis methods		
1.3	Classical attacks on security and counter measures: Eavesdropping, Traffic Analysis attack, Replay attack, non-repudiation attack, Man-in-the-Middle attack, Data Tampering, Denial of Service (DoS) attack, Brute Force Attack, zero day exploit attack, Phishing and social engineering, Spoofing, Malware, session hijacking attack,		

Module 1.2

- Cryptography
- Word with Greek Origin
- Means “Secret Writing”
- Science & Art of transforming messages to make them secure and immune to attacks-Forouzan

Definitions

- **Plaintext-**An original message
- **Ciphertext-T**he coded message
- **Enciphering** or E**ncryption**- The process of converting from plaintext to ciphertext
- **Deciphering** or D**ecryption**- Restoring the plaintext from the ciphertext

Definitions

- **Cryptography –**
  - The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system** or a **cipher**.

- **Cryptanalysis-**
  - Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**.
  - Cryptanalysis is what the layperson calls “breaking the code.”

- **Cryptology -** The areas of cryptography and cryptanalysis together.

Stream Cipher Vs Block Cipher

- Stream Cipher :
  - stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
- Block Cipher :
  - block cipher converts the plain text into cipher text by taking plain text's block at a time

Stream Cipher Vs Block Cipher

Aspect	Stream Cipher	Block Cipher
Basic Concept	Encrypts data one bit or byte at a time.	Encrypts data in fixed-size blocks (e.g., 64 or 128 bits).
Processing	Continuous, works on data streams.	Discrete, processes data in chunks.
Speed	Generally slower, especially for real-time applications., discrete, exponential operations	Faster due to block-wise operations, Ex-OR operations
Complexity	Simpler implementation.	More complex design and implementation.
Mode of Operation	Doesn't require padding as it works bit-by-bit.	Requires padding if data size is not a multiple of block size.
Key Usage	Often uses a single key and generates a pseudorandom keystream.	Uses keys in conjunction with specific modes like ECB, CBC, etc.
Suitability	Best for applications needing real-time or streaming encryption (e.g., voice, video).	Best for encrypting files or data at rest.
Error Propagation	Errors affect only the bit/byte in question.	Errors can propagate throughout the block.
Security	Potential vulnerability to pattern attacks if the keystream is not truly random.	More robust due to structured modes of operation.
Examples	RC4, RSA, ECC	AES, DES, Blowfish.

Stream Cipher Vs Block Cipher

- Datasize?
  - 8 bits Vs 64, 128 bits?
- Technique?
  - stream cipher uses only confusion.
  - Block cipher Uses confusion as well as diffusion
- Applications?
  - Short data
  - Large data?
- Strength?

Stream Cipher Vs Block Cipher

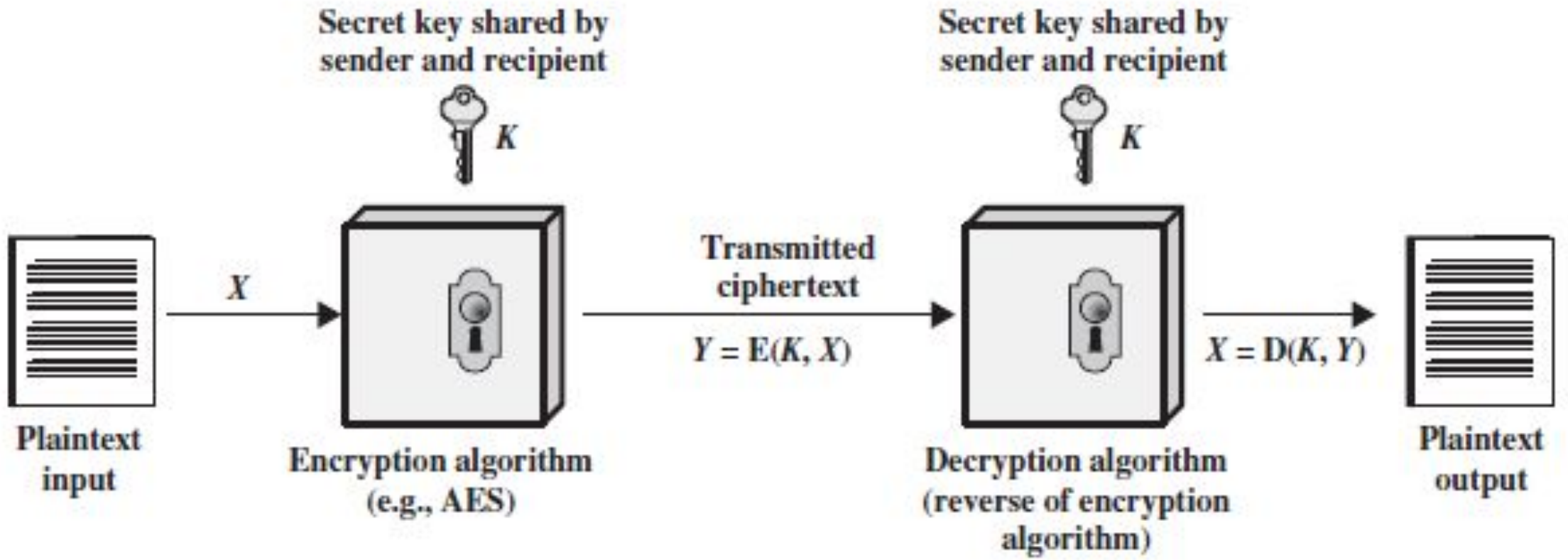
- Block ciphers are More secure than stream ciphers when the same key is used multiple times; Stream ciphers are less secure than block ciphers when the same key is used multiple times

Symmetric Encryption

A symmetric encryption scheme has five ingredients

- **Plaintext**
- **Encryption algorithm**
- **Secret key**
- **Ciphertext**
- **Decryption algorithm**

Symmetric Encryption



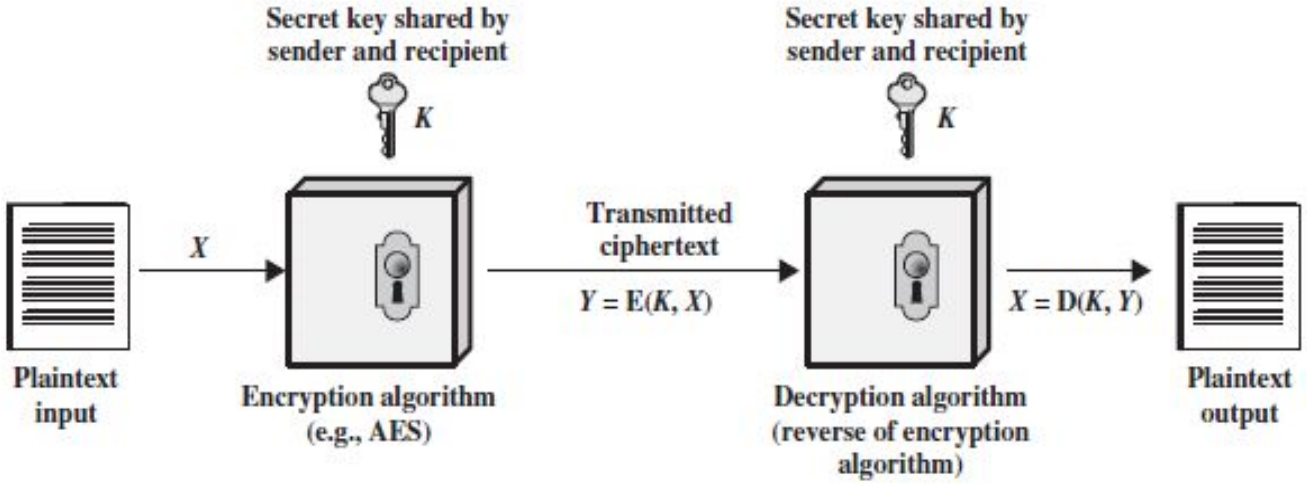
Symmetric Encryption

Plaintext

- This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm

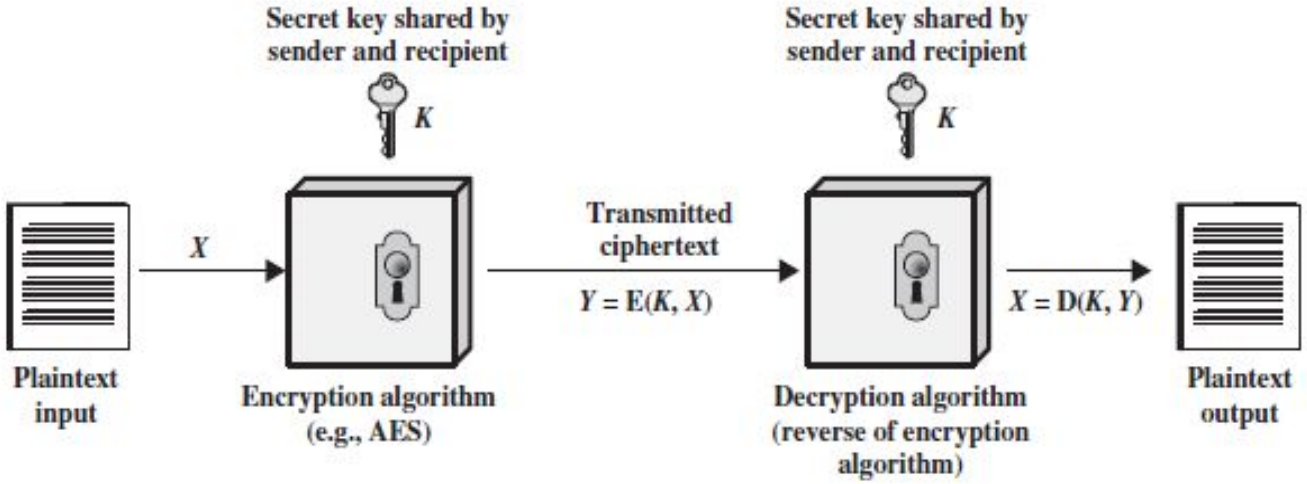
- The encryption algorithm performs various substitutions and transformations on the plaintext.



Symmetric Encryption

Secret key:

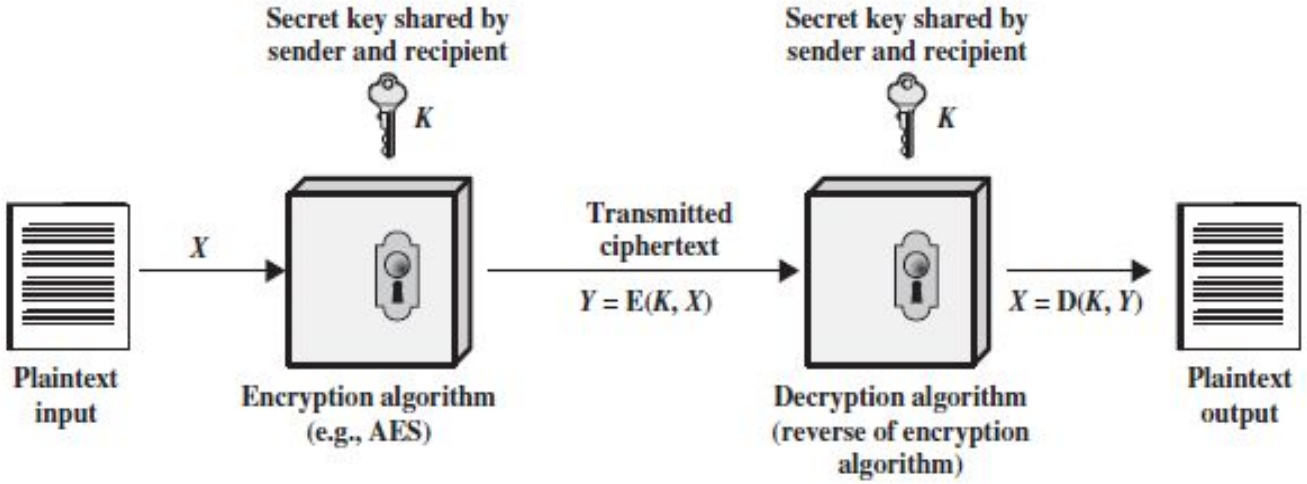
- The secret key is also input to the encryption algorithm.
- The key is a value independent of the plaintext and of the algorithm.
- The algorithm will produce a different output depending on the specific key being used at the time.
- The exact substitutions and transformations performed by the algorithm depend on the key.



Symmetric Encryption

Cipher text

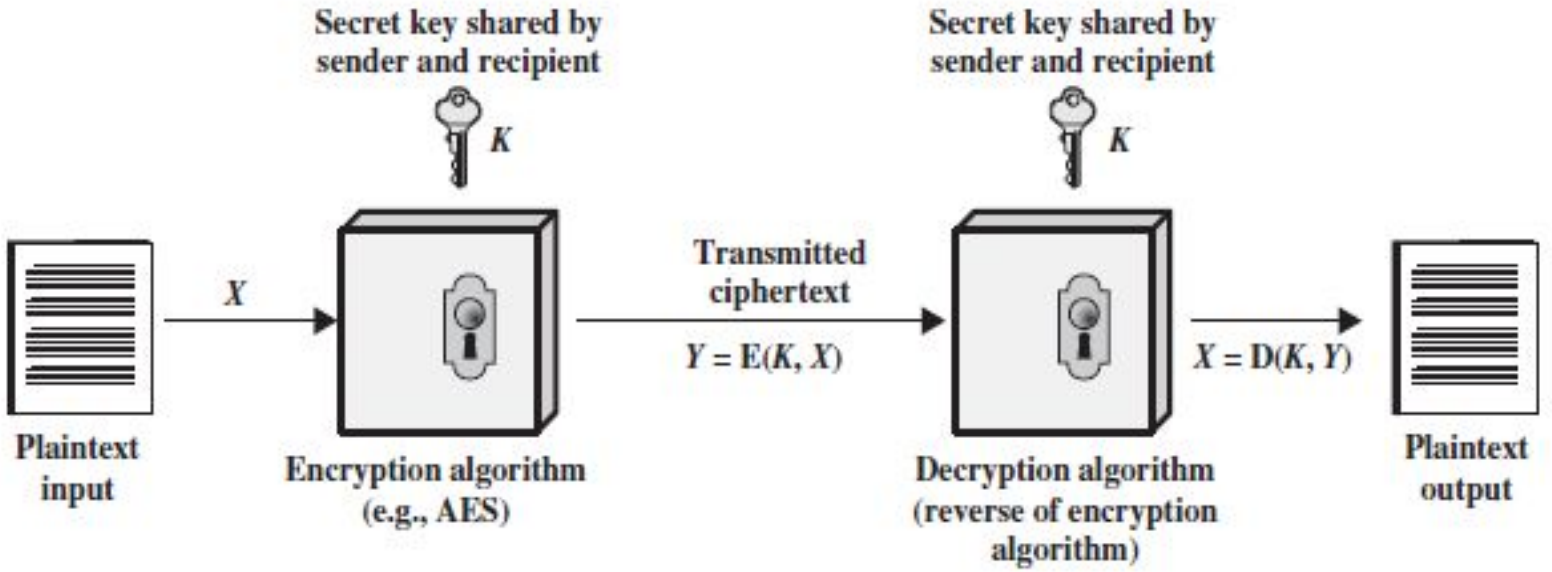
- This is the scrambled message produced as output.
- An apparently random stream of data and, as it stands, is unintelligible.
- It depends on the plaintext and the secret key.
- **<u>For a given message, two different keys will produce two different cipher texts.</u>**



Symmetric Encryption

Decryption algorithm

- This is essentially the encryption algorithm run in reverse.
- It takes the cipher text and the secret key and produces the original plaintext.



Symmetric Encryption

Requirements for secure use of conventional/Symmetric encryption:

- A strong encryption algorithm.
- Secure Secret Key

Symmetric Encryption

A strong encryption algorithm.

- Even if the opponent knows the algorithm and has access to one or more ciphertexts, Still would be unable to decipher the ciphertext or figure out the key.
- The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

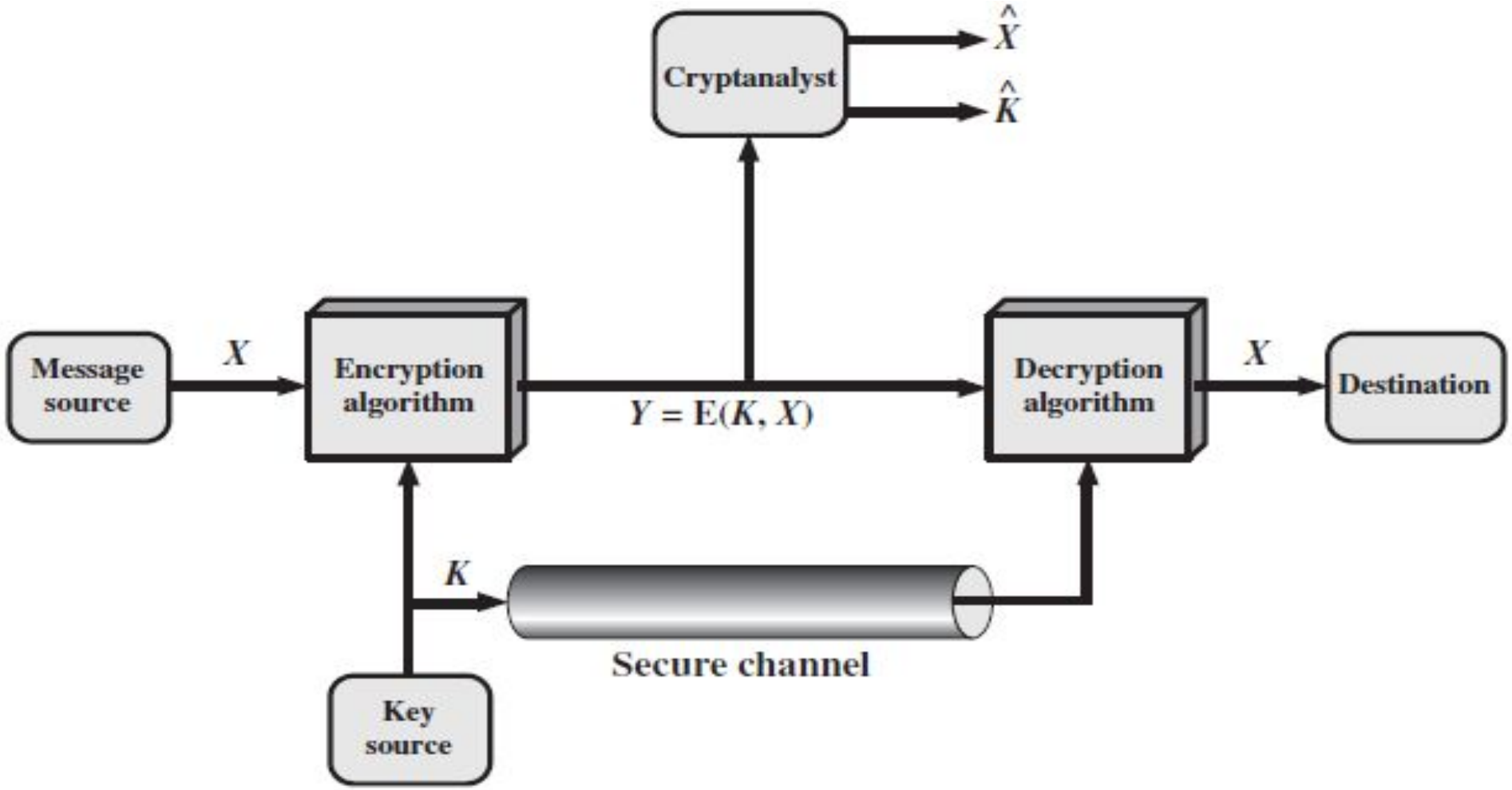
Symmetric Encryption

Secure Secret Key-

- Sender and receiver must have
  - obtained copies of the secret key in a secure fashion and
  - must keep the key secure.

- If someone can discover the key and knows the algorithm, all communication using this key is readable.

Model of Symmetric Cryptosystem



SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya TRUST

Model of Symmetric Cryptosystem

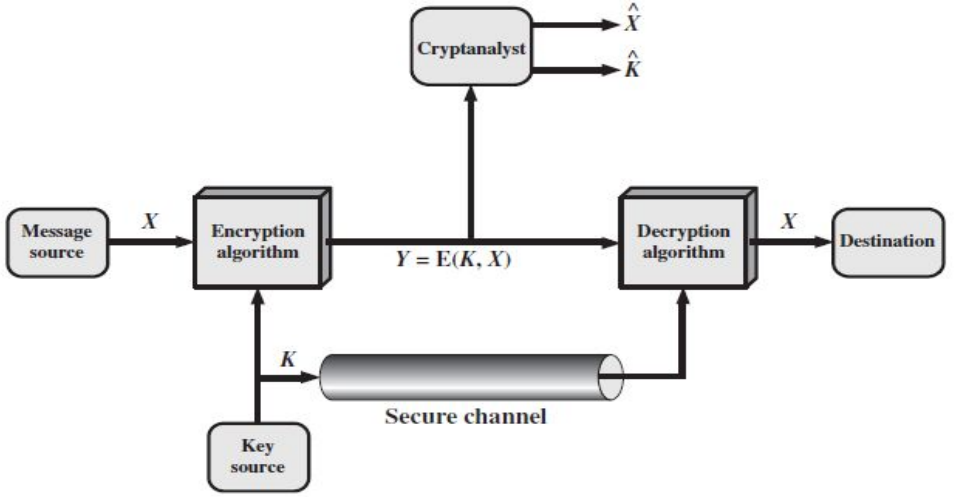
- A source produces a message in plaintext,

  $X = [X1, X2, \ldots\ldots\ldots\ldots, XM]$.

- The M elements of X are letters in some finite alphabet(26 Capital letters or {0,1})
- Key generation

  $K = [K1, K2, c, KJ]$

- If the key is generated at the Message source or Third Party, delivered to the destination by means of some secure channel.



Model of Symmetric Cryptosystem

- Cipher text generation

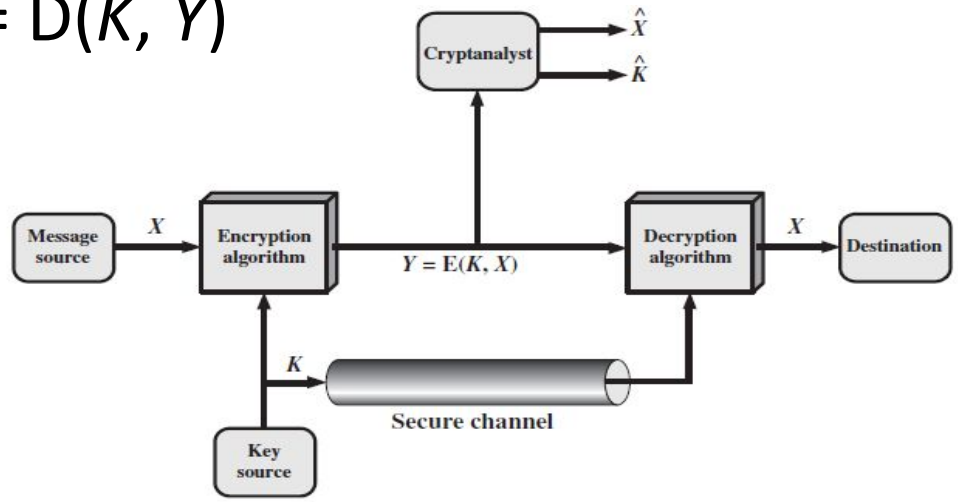
$$Y = [Y1, Y2, \ldots\ldots, YN].$$

$$Y = \mathrm{E}(K, X)$$

- Y is produced by using encryption algorithm E as a function of the plaintext X, the value of the key K.

- The intended receiver, in possession of the key, is able to invert the transformation:

$$X = \mathrm{D}(K, Y)$$



Categories of Cryptographic System

Characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to cipher text.**

2. **The number of keys used.**

3. **The way in which the plaintext is processed.**

Categories of Cryptographic System

The type of operations used for transforming plaintext to cipher text-

All encryption algorithms are based on two general principles:

- Substitution
- Transpositions

Categories of Cryptographic System

Substitution

- Each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element

Transposition

- Elements in the plaintext are rearranged.

- The fundamental requirement is that no information be lost (i.e., that all operations are reversible).
- Most systems involve multiple stages of substitutions and transpositions.

Categories of Cryptographic System

The number of keys used-

- If both sender and receiver use the same key, the system is referred to as **symmetric, single-key, secret-key, or conventional encryption.**

- If the sender and receiver use different keys, the system is referred to as **asymmetric, two-key, or public-key encryption.**

Categories of Cryptographic System

The way in which the plaintext is processed-

- **A *block cipher*** processes the input one block of elements at a time, producing an output block for each input block.

- **A *stream cipher*** processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack

The objective of attacking an encryption system is

- To recover the key in use rather than simply to recover the plaintext of a single ciphertext.
- Why?

Cryptanalysis and Brute-Force Attack

- There are two general approaches to attacking a conventional encryption scheme:
  - **Cryptanalysis**
  - **Brute-force attack**

Cryptanalysis and Brute-Force Attack

Cryptanalysis:

- Cryptanalytic attacks rely on
  - the nature of the algorithm or
  - the general characteristics of the plaintext or
  - even some sample plaintext–ciphertext pairs.

- This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Cryptanalysis and Brute-Force Attack

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.
- Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.
- That is, if there are *X* different keys, on average an attacker would discover the actual key after *X*/2 tries

Cryptanalysis and Brute-Force Attack

- If either type of attack succeeds in deducing the key, the effect is catastrophic
- All future and past messages encrypted with that key are compromised.

Cryptanalysis and Brute-Force Attack

- Summary of the various types of **cryptanalytic attacks** based on the amount of information known to the cryptanalyst.

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 • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cryptanalysis

- Cryptanalysis is the study and process of analyzing and decrypting ciphers, codes, and encrypted text without using the real key.
- Alternately, we can say it's the technique of accessing a communication's plain text content when you don't have access to the decryption key.

- Put simply, cryptanalysis is the practice, science, or art of decrypting encrypted messages.

Cryptanalysis

- Cryptanalysis experts study ciphers, cryptosystems, and ciphertext to understand their functions.
- Then, they use that knowledge to find or improve techniques to weaken or defeat them.
- Cryptographer : one who writes encryption code used in cybersecurity,
- Cryptoanalyst : one who tries to crack those encryption codes.
- Two opposing sides of the cybersecurity coin, locked in conflict, trying to one-up the other, constantly inventing new measures and countermeasures.

Who Uses Cryptanalysis?

- Hackers use cryptanalysis.
- Would-be hackers use cryptanalysis to root out cryptosystem vulnerabilities rather than a brute force attack.
- Governments use cryptanalysis to decipher the encrypted messages of other nations.
- Companies specializing in cybersecurity products and services use cryptanalysis to test their security features.
- Even the world of academia gets in on the action, with researchers and academicians looking for weaknesses in cryptographic algorithms and protocols.
- Black-hat hackers use it to commit cybercrimes, and white-hat hackers use it to conduct penetration testing as directed by organizations that hire them to test their security.

Cryptanalysis Attacks and Techniques

1. Ciphertext-Only Attack

The attacker only has access to :

- at least one encrypted message
- but does not know the plaintext data, any cryptographic key data used, or the encryption algorithm being employed.
- Intelligence agencies often face this challenge when they've intercepted encrypted communications from a target.
- However, this is a formidable attack to pull off, thanks to the lack of target data.

Ciphertext-Only Attack (COA)

- **Problem:** cryptanalyze : **"DQG D FKLOG UHQWLQJ."**
  Assume the cipher is a Monoalphabetic substitution cipher. Decrypt the message.
- **Solution:**
- Since only the ciphertext is given, try all possible cipher shifts (brute force).
- Shifting letters by 3 (common Caesar cipher key):
  - 'D' → 'A', 'Q' → 'N', 'G' → 'D', etc.
- Decrypted text: **"AND A CHILD RENTING."**
- Success with a shift of 3.

Cryptanalysis Attacks and Techniques

2. Known Plaintext Attack
   - This attack is easier to implement, compared to the ciphertext-only attack.
   - analyst most likely has access to some or all the ciphertext's plaintext.
     - E.g. Hello in beginning or Regards in the end of message
   - The goal is to discover the key the target uses to encrypt the message and use the key to decrypt the message.
   - Once the key is discovered, the attacker can decrypt every message encrypted with that specific key.
   - Known plaintext attacks rely on the attacker finding or guessing all or part of an encrypted message, or alternately, even the original plaintext's format.

Known Plaintext Attack (KPA)

- **Problem:**
  You know the plaintext **"HELLO"** maps to the ciphertext **"KHOOR"** using a Caesar cipher.
  Decrypt **"ZRUOG."**
- **Solution:**
- Calculate the shift:
  - 'H' → 'K' (shift of 3).
- Use this shift to decrypt **"ZRUOG"**:
  - Z → W, R → O, U → R, L → I, G → D.
- Decrypted text: **"WORLD."**

Known Plaintext Attack (KPA)

- **Problem:** You know the plaintext **"ATTACK"** maps to ciphertext **"DWWDFN"** using a substitution cipher. Decrypt **"FDWDWDFNHUV."**
- **Solution:**
- Determine the shift:
  - A → D (shift of 3).
- Decrypt **"FDWWDFNHUV"** by reversing the shift:
  - F → C, D → A, W → T, etc.
- Decrypted text: **"CAT ATTACKERS."**

Cryptanalysis Attacks and Techniques

3. Chosen Plaintext Attack

- Analysts using a chosen plaintext attack either already knows the encryption or can use the device used for encryption.
- The cryptanalyst can then encrypt the chosen plaintext using the targeted algorithm to gather information regarding the key.

Chosen Plaintext Attack (CPA)

- **Problem:** You suspect a substitution cipher, as **“CAT"** = **“FDW."** Decrypt the ciphertext **"LQIRUPDWLRQ"** using the known plaintext.
- **Solution:**
- Map plaintext to ciphertext:
  - C → F, A → D, T → W
- Use the substitution mapping to decode other ciphertext messages.
- For "LQIRUPDWLRQ", apply the reverse mapping:

- Decrypted text: "INFORMATION."

Chosen Plaintext Attack (CPA)

- **Problem:** You suspect a transposition cipher with **"HELLO" = "LEHLO."**
  Decrypt the ciphertext **"LEHLO"** using the pattern observed.

- Solve it..

Chosen Plaintext Attack (CPA)

- **Problem:** You suspect a transposition cipher with **"HELLO" = "LEHLO."**
  Decrypt the ciphertext **"LEHLO"** using the pattern observed.
- **Solution:**
- Analyze how plaintext maps to ciphertext:
  - "HELLO" → "LEHLO" (swap positions 1↔2, 4↔5).
- Apply the same swaps in reverse:
  - Ciphertext **"LEHLO"** → Plaintext **"HELLO."**

Cryptanalysis Attacks and Techniques

4. A chosen-ciphertext attack

- cryptanalyst can analyse any chosen ciphertexts together with their corresponding plaintexts.
- the goal is to acquire a secret key or to get as many information about the attacked system as possible.
- The attacker has capability to make the victim (who obviously knows the secret key) decrypt any ciphertext and send him back the result.
- By analysing the chosen ciphertext and the corresponding received plaintext, the intruder tries to guess the secret key which has been used by the victim.
- Chosen-ciphertext attacks are usually used for breaking systems with public key encryption.
- For example, early versions of the RSA cipher were vulnerable to such attacks. They are used less often for attacking systems protected by symmetric ciphers. Some self-synchronizing stream ciphers have been also attacked successfully in that way.

Chosen Ciphertext Attack (CCA)

- **Problem:** You submit **"KHOOR"** (Caesar cipher) for decryption and receive **"HELLO.“**
- Decrypt **"FRQJUDWXODWLRQV."**
- **Solution:**
- From the given decryption, the cipher uses a Caesar shift of 3 (reverse each letter by 3).
- Decrypt **"FRQJUDWXODWLRQV"**:
  - F → C, R → O, Q → N, G → D, etc.
- Decrypted text: **"CONGRATULATIONS."**

Summary

- **Ciphertext-only attack:** Attacker only has access to ciphertext. This is the most challenging scenario.
- **Known-plaintext attack:** Attacker has access to both ciphertext and corresponding plaintext.
- **Chosen-plaintext attack:** Attacker can choose plaintext and obtain corresponding ciphertext.
- **Chosen-ciphertext attack:** Attacker can choose ciphertext and obtain corresponding plaintext

Cryptanalysis of Classical Ciphers

- **Caesar Cipher**
  - **Brute-force attack:** try all 25 possible key shifts.
  - **Frequency analysis**
- **Rail Fence Cipher**
  - **Brute-force attack:** test different numbers of "rails" until a meaningful plaintext emerges.
  - **Visual inspection:** For short ciphertexts, visual inspection and rearranging the characters can sometimes reveal the plaintext

- **Columnar Transposition Cipher**
  - **Anagramming and Columnar Transposition:** Explain the process.
  - **Brute-force attack:** Discuss brute-forcing different key lengths and permutations. Mention the increasing complexity with longer keys.
  - **Frequency analysis:** digraph and trigraph frequencies can aid in identifying column order
- **Playfair Cipher**
  - **Frequency analysis:** digraph frequencies can be used to identify common digraphs and infer the Playfair square structure.
  - **Known-plaintext attack:** a small amount of plaintext-ciphertext pairs can be very effective in deducing the Playfair square.
  - **Brute-force attack:** brute-forcing a Playfair cipher is significantly harder compared to the previous ciphers due to the larger key space (possible arrangements of the 5x5 grid).

Cryptanalysis Tools

- **Cryptol:** This tool is an open-source license initially designed to be used by the Nation Security Agency (NSA), the United States intelligence agency, targeting cryptographic algorithms. Cryptol allows users to monitor how algorithms operate in programs that specify the ciphers or algorithms.
- **CrypTool:** CrypTool is another open-source offering that creates elearning programs, plus a web portal designed to help users learn about cryptographic algorithms and cryptanalysis.
- **Ganzua:** Ganzua is the Spanish term for a skeleton key or lockpick. It's an open-source, multi-platform Java-based tool that allows analysts to define almost totally arbitrary cipher and plain alphabets. In addition, this function will enable users to crack non-English cryptograms.

Cryptanalysis

- **Problem:**
  The ciphertext is **"BMODZBXDNABEKUDMUIXMMOUVIF"**, and you know the keyword is **"MONARCHY"**. Decrypt the message.

Solution

- **Construct the Playfair Matrix:**
  Using the keyword **"MONARCHY"** (no repeated letters), fill a 5x5 grid:

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

- **Decrypt Digraphs:**
  Ciphertext digraphs are **BM, OD, ZB, XD, NA, BE, KU, DM, UI, XM, MO, UV, IF**.

- For each pair, locate letters in the grid:
  - **BM**: 'B' (row 2, col 4) and 'M' (row 1, col 1). They form a rectangle. Swap columns: **AN**.
  - **OD**: 'O' (row 1, col 2) and 'D' (row 2, col 5). Rectangle swap: **RY**.
  - Continue for all pairs.

- **Final Decrypted Text:**
  Result: **"AN INSTRUCTION IS IMPORTANT."**

Cihertext-Only Attack

- **Problem:**
  The ciphertext is **"WECRLTEERDSOEEFEAOCAIVDEN"**. The number of rails is unknown. Decrypt the message.

- **Test Different Rails:**
  Use trial and error to reconstruct plaintext by arranging the ciphertext in a zig-zag pattern.

W . . . E . . . C . . . R . . . L

. E . R . D . S . E . E . F . A .

. . O . . . C . . . A . . . I . V

- Read horizontally: **"WEAREDISCOVEREDFLEEATONCE"**
- Final Plaintext: **"WE ARE DISCOVERED FLEE AT ONCE."**

Columnar Transposition Cipher Cryptanalysis

- **Problem:**
  Ciphertext: **"HWEOLRLLDO"**
  Key: **"312“**

- **Solution:**
- Arrange Ciphertext in Columns Based on Key:
  Key: **3 1 2**

3	1	2
W	H	E
O	L	L
D	O	R

- Rearrange Columns by Key Order:
  Key Order: **1 2 3**

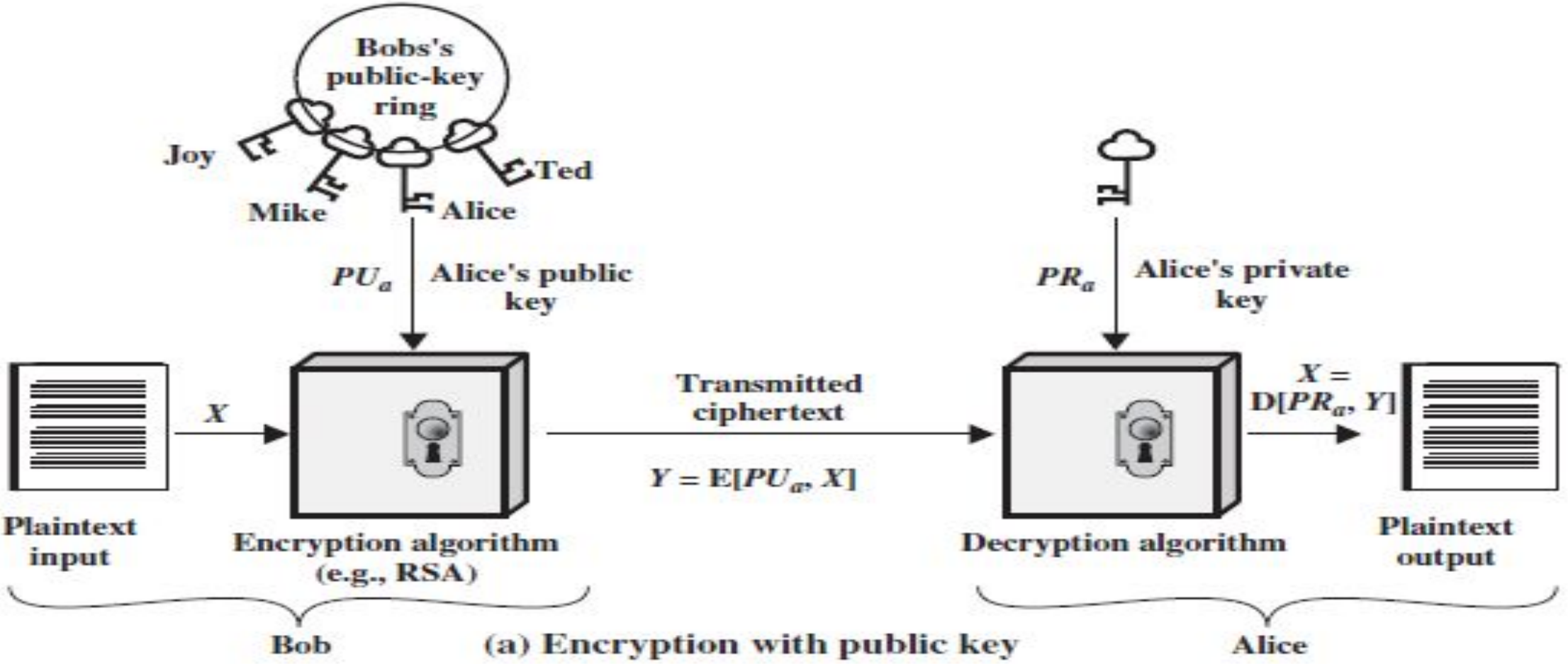
H	**E**	**W**
L	**L**	**O**
O	**R**	**D**

- **Read Row by Row:**
  Plaintext: **"HELLO WORLD."**

Asymmetric cryptography

- Public-key cryptography
- Asymmetric cryptography,
- A cryptographic system that uses pairs of keys
- Public keys (which may be known to others),
- Private keys (which may never be known by any except the owner).

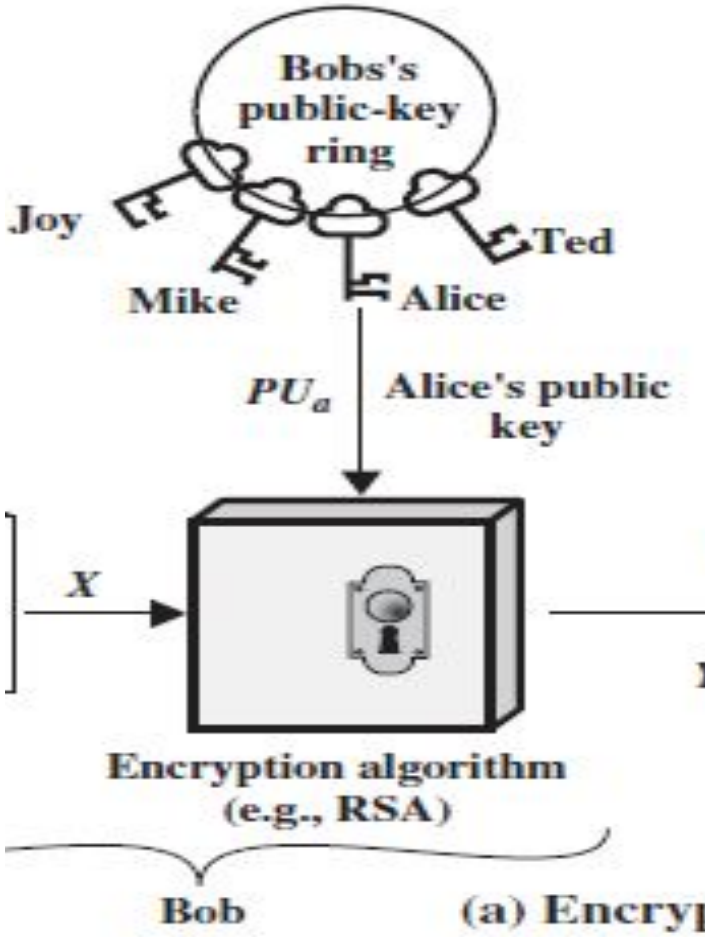
Asymmetric cryptography



Asymmetric cryptography

The essential steps are the following.

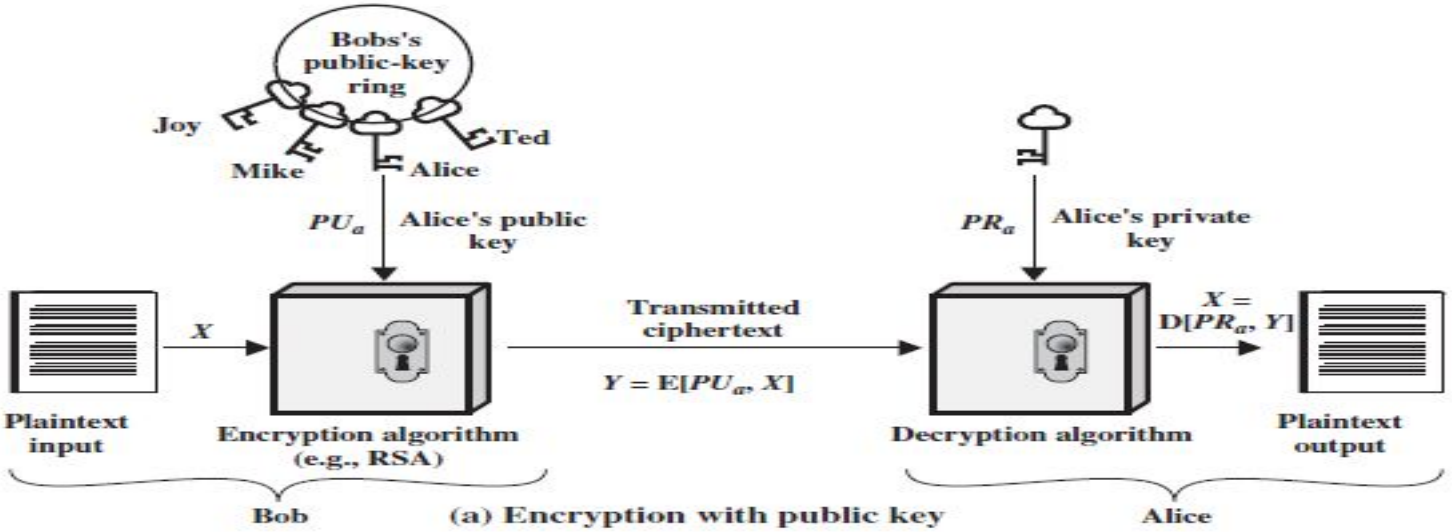
- Each user generates a pair of keys to be used for the encryption and decryption of messages.
- Each user places one of the two keys in a public register or other accessible file. This is the public key.
- The companion key is kept private.
- Each user maintains a collection of public keys obtained from others.



Asymmetric cryptography

The essential steps are the following.

- If Bob wishes to send a confidential message to Alice
- Bob encrypts the message using Alice's public key.
- When Alice receives the message, she decrypts it using her private key.
- No other recipient can decrypt the message because only Alice knows Alice's private key.



Difference between Symmetric and Asymmetric Encryption

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

Classical Encryption Techniques

- Basic approaches to symmetric encryption

- The two basic building blocks of all encryption techniques are-
  - Substitution
  - Transposition

Classical Encryption Techniques

Substitution Techniques:

- **Monoalphabetic Cipher: Caesar Cipher**
- **Playfair Cipher**

Transposition Techniques

- **Rail Fence**
- **Rectangle Transposition**

Transposition Techniques

- Substitution-All the techniques involve the substitution of a ciphertext symbol for a plaintext symbol.

Transposition cipher-

- **A very different kind of mapping achieved by performing some sort of permutation on the plaintext letters.**

Transposition Techniques-Rail fence

- **<u>The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.</u>**
- 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

- Trivial to cryptanalyze

Transposition Techniques

A more complex scheme:

1) **Write the message in a rectangle, row by row**

2) **Read the message off, column by column**

3) **Permute the order of the columns**

4) **The order of the columns then becomes the key to the algorithm**

Transposition Techniques

For example,

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Transposition Techniques

- **The key is 4312567.**
- **To encrypt, start with the column that is labeled 1, in this case column 3. Write down all the letters in that column.**
- **Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.**

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Transposition Techniques

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- Cryptanalysis is fairly straightforward
- Involves laying out the ciphertext in a matrix and playing around with column positions.
- Digram and trigram frequency tables can be useful.

Transposition Techniques

- The transposition cipher can be made significantly more secure
- By performing more than one stage of transposition.
- The result is a more complex permutation that is not easily reconstructed.

Transposition Techniques

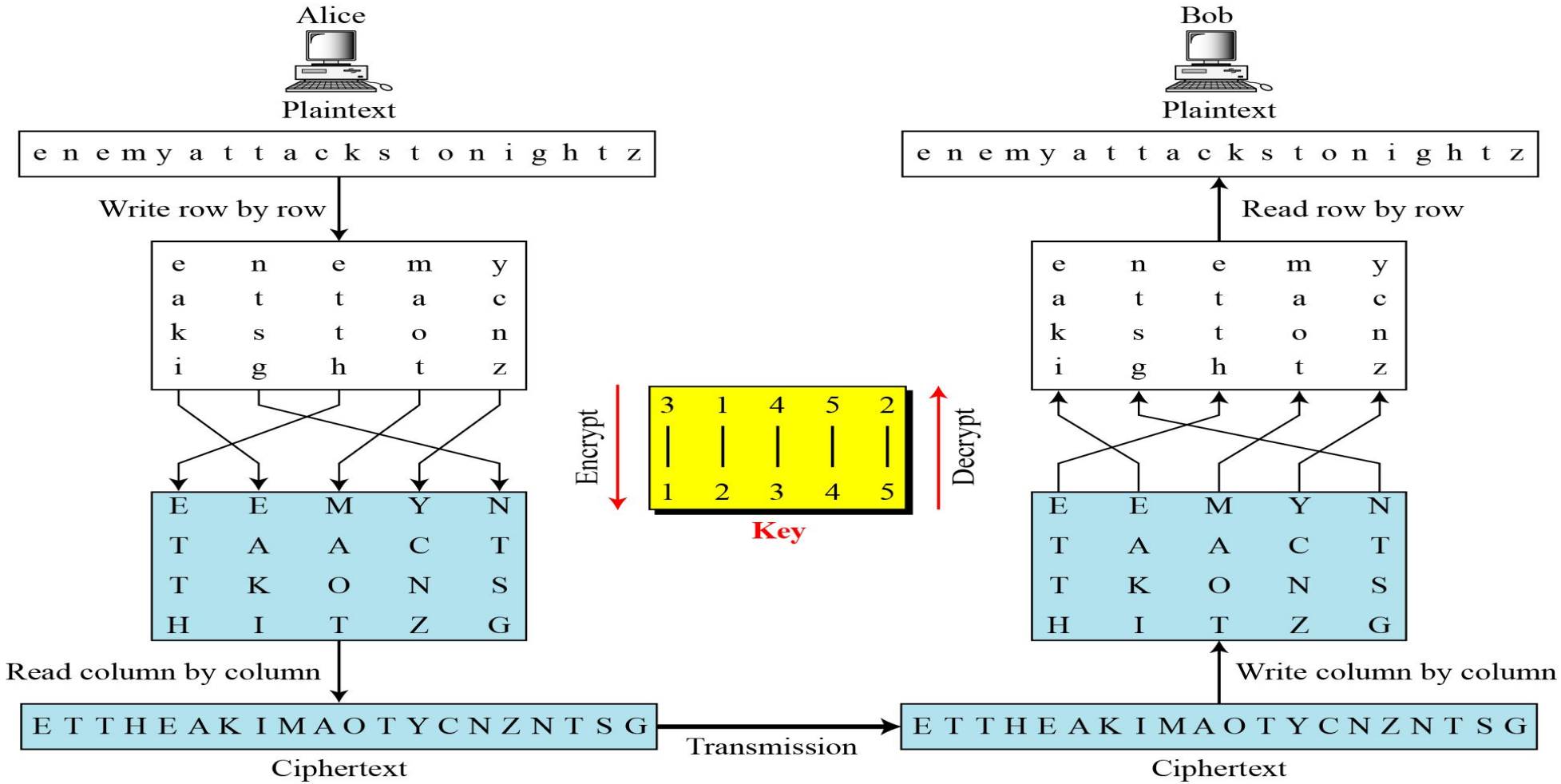
- If the foregoing message is re-encrypted using the same algorithm

```
Key:      4 3 1 2 5 6 7
Input:    t t n a a p t
          m t s u o a o
          d w c o i x k
          n l y p e t z
Output:   NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Combining Two Approaches

Example

Figure



Classical Encryption Techniques

Substitution

- **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.**

Caesar Cipher

- **The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.**
- **The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,**

Caesar Cipher

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

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

Caesar Cipher

- 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

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

- If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.

Brute-Force Cryptanalysis of Caesar Cipher

- The results of applying this strategy to the example ciphertext.
- In this case, the plaintext leaps out as occupying the third line.

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
25	qiix	qi	ejxiv	xli	xske	tevxc

Brute-Force Cryptanalysis of Caesar Cipher

Caesar Cipher

- 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

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

- If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.

Caesar Cipher

- With only 25 possible keys, the Caesar cipher is far from secure.
- A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.
- Permutation!!

Caesar Cipher

- A **permutation** of a finite set of elements *S* is an ordered sequence of all the elements of *S*, with each element appearing exactly once.

- For example,

S = {a, b, c}, there are six permutations of *S*:

abc, acb, bac, bca, cab, cba

- There are *n*! permutations of a set of *n* elements,
  - The first element can be chosen in one of *n* ways,
  - The second in *n* - 1 ways,
  - The third in *n* – 2 ways, and so on.

Caesar Cipher

- Caesar Cipher-

```
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
```

- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys.

- Such an approach is referred to as a monoalphabetic substitution cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

Playfair Cipher

- Playfair, treats **digrams** in the plaintext as single units
- Translates these units into ciphertext digrams

- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

- In this case, the 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

Playfair Cipher

- 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.

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

Playfair Cipher

Plaintext is encrypted two letters at a time, according to the following rules:

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.

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

Playfair Cipher

Plaintext is encrypted two letters at a time, according to the following rules:

1) 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, st=TL

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

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

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya TRUST

Playfair Cipher

Plaintext is encrypted two letters at a time, according to the following rules:

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, me=CL

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

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

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya TRUST

Playfair Cipher

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).

Diagraph: "nt" **Encrypted Text:** rq

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

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

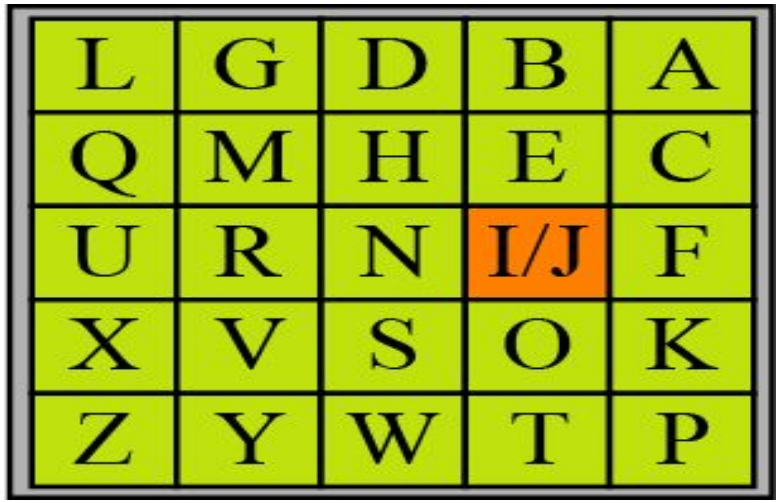
SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya TRUST

Playfair Cipher

Figure An example of a secret key matrix in the Playfair cipher

Secret Key =



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

Example

Let us encrypt the plaintext "hello" using the key in given Figure

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

Cryptanalysis of Playfair Cipher

- Brute force is difficult
- Size of key domain 25!
- Hides single letter frequency of characters
- Still leaves much of the structure of the plaintext language intact.
- A few hundred letters of ciphertext are generally sufficient
- Cryptanalyst can have ciphertext only attack based on digram frequency test to find the key

Polyalphabetic Cipher

- Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.

- Called as polyalphabetic substitution cipher.

- All these techniques have the following features in common:

1) A set of related mono alphabetic substitution rules is used.
2) A key determines which particular rule is chosen for a given transformation.

Monoalphabetic vs Polyalphabetic Cipher

Monoalphabetic cipher-

- The cipher alphabet for each plain alphabet is fixed throughout the encryption process.

- For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.

Polyalphabetic Cipher –

- The cipher alphabet for the plain alphabet may be different at different places during the encryption process.

Monoalphabetic vs Polyalphabetic Cipher

SR.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
1	Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
3	Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto 'm' alphabetic characters of a cipher text.

Monoalphabetic vs Polyalphabetic Cipher

Note

In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Monoalphabetic vs Polyalphabetic Cipher

Example

The following shows a plaintext and its corresponding ciphertext. The cipher is probably monoalphabetic because both l's are encrypted as O's.

Plaintext: hello **Ciphertext:** KHOOR

Example

The following shows a plaintext and its corresponding ciphertext. The cipher is not monoalphabetic because each l is encrypted by a different character.

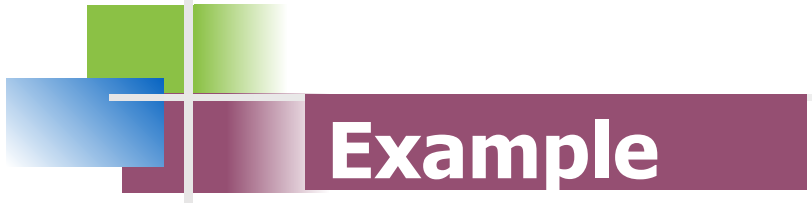
Plain Text; hello Cipher text: ABNZF

Eg of Monoalphabetic Cipher

The simplest mono alphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature.

Figure Plaintext and ciphertext in Z_{26}

Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



Example

Use the additive cipher with key = 15 to encrypt the message “hello”.

Example

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

Solution

We apply the encryption algorithm to the plaintext, character by character:

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

Example

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Example

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution

We apply the decryption algorithm to the plaintext character by character:

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

Example

Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the Caesar cipher.

Example

Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use a brute-force attack to break the cipher.

Solution

Eve tries keys from 1 to 7. With a key of 7, the plaintext is "not very secure", which makes sense.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

GATE | GATE-IT-2004 | Question 25

A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?

(A) Sender encrypts using receiver's public key

(B) Sender encrypts using his own public key

(C) Receiver decrypts using sender's public key

(D) Receiver decrypts using his own public key

GATE | GATE-IT-2004 | Question 25

A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?

(A) Sender encrypts using receiver's public key

(B) Sender encrypts using his own public key

(C) Receiver decrypts using sender's public key

(D) Receiver decrypts using his own public key

Answer: (A)

TYPES OF KEYS

- Public key
- Private key
- Symmetric key
- Session key
- keystream
- Passphrase
- Key protection/encryption keys
- Access keys/granting keys
- Data encryption keys

Symmetric Key (Secret Key)

- **Used in:** Symmetric encryption
- **Key characteristic:** Same key used for encryption and decryption
- **Examples:**
- **AES key (Advanced Encryption Standard)** – 128, 192, or 256 bits
- **DES key (Data Encryption Standard)** – 56 bits (now obsolete)
- **3DES key** – 112 or 168 bits
- **RC4, RC5, RC6 keys**

Asymmetric Key (Public/Private Key Pair)

- **Used in:** Asymmetric encryption, digital signatures, key exchange
- **Key characteristic:** Public key for encryption or signature verification; private key for decryption or signing
- **Examples:**
  - **Public Key** – Used to encrypt data or verify digital signatures
  - **Private Key** – Used to decrypt data or create digital signatures
  - **RSA Key** – Common in email and secure web communication
  - **ECC Key** – Elliptic Curve Cryptography (e.g., P-256, Ed25519)
  - **DSA Key** – Digital Signature Algorithm
  - **ElGamal Key** – Often used for encryption based on Diffie–Hellman

Public Key

- **Used in:** Encryption or signature verification
- **Key characteristic:** Can be shared openly

Private Key

- **Used in:** Decryption or digital signing
- **Key characteristic:** Must be kept secret; compromise means full access

Session Key

- **Used in:** Temporary communication sessions
- **Key characteristic:** Ephemeral symmetric key generated for a single session
- **Often used with:** TLS, VPNs, secure messaging

Key Exchange / Derivation / Wrapping

- **Pre-shared Key (PSK)** – Shared in advance, used in VPNs, Wi-Fi (WPA2-PSK)
- **Key Derivation Key (KDK)** – Used in key derivation functions (KDFs)
- **Key Encryption Key (KEK)** – Encrypts other keys, not data directly
- **Master Key / Root Key** – Base key used to derive or sign other keys

Application-Specific Keys

- **Data Encryption Key (DEK)** – Specifically used to encrypt data (e.g., in databases, cloud storage)
- **Authentication Key (Auth Key)** – Used in MACs (Message Authentication Codes), HMACs, and digital signatures
- **Passphrase / Password Key** – A human-memorable string often turned into a cryptographic key via a KDF (like PBKDF2, scrypt, Argon2)

Passphrase

- A passphrase is a **human-readable string** (often multiple words) used to derive a cryptographic key. It's similar to a password but typically **longer and more secure**.
- **Usage:**
  - Protect private keys (e.g., PGP or SSH keys)
  - Used in key derivation functions (KDFs) like PBKDF2, scrypt, Argon2
  - Encrypt files, devices, or secure messages
- **Example:**
  "correct horse battery staple" → used to generate a 256-bit

Keystream

- **Definition:**
  A **keystream** is a sequence of bits or bytes **generated by a stream cipher**, which is **combined (usually XORed)** with plaintext to produce ciphertext.
- **Usage:**
  - Core component in stream ciphers like **RC4**, **ChaCha20**, **Salsa20**
  - Ensures data is encrypted **bit by bit or byte by byte**
- **Properties:**
  - Must be **random-looking** and **synchronized** between sender and receiver
  - Should never be reused with the same key (to avoid attacks)
- **Example:**
  Plaintext: 10110100
  Keystream: 01001110
  text XOR Keystream = 11111010

Question

- What is salt?
- How passwords are stored in databases?