INFORMATION AND NETWORK SEURITY

INTRODUCTION

What is????????

------ Information

-------Network

-------Security

Information is the processed data on which decisions and of **computer** systems and information from harm, theft, and unauthorized use.
A **computer network** is a group of **computers** that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the **network** nodes.

Computer security, The protection of **computer** systems and information from harm, theft, and unauthorized use.

What security is about in general?

- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley
- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, burglar alarms, closed circuit TV
- Reaction
  - attack on burglar (not recommended 😊), call the police, replace stolen items, make an insurance claim

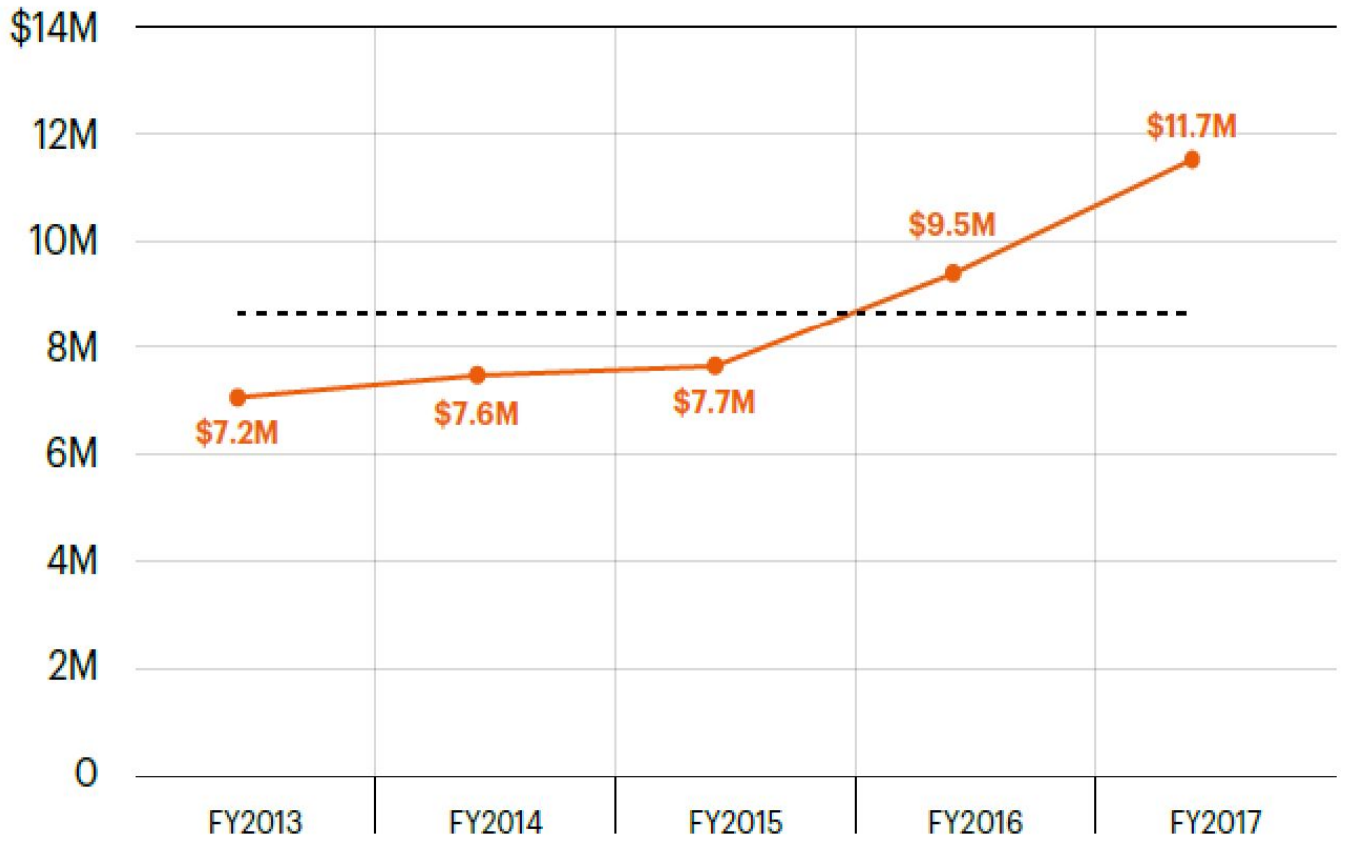
Internet shopping example

- **Prevention**
  - encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don't send card number via Internet
- **Detection**
  - an unauthorized transaction appears on your credit card statement
- **Reaction**
  - complain, dispute, ask for a new card number, sue (if you can find of course 😊)
  - Or, pay and forget (a glass of cold water) 😊

Information security in past & present

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - in general: physical and administrative mechanisms
- Modern World
  - Data are in computers
  - Computers are interconnected

The global average cost of cyber crime/attacks

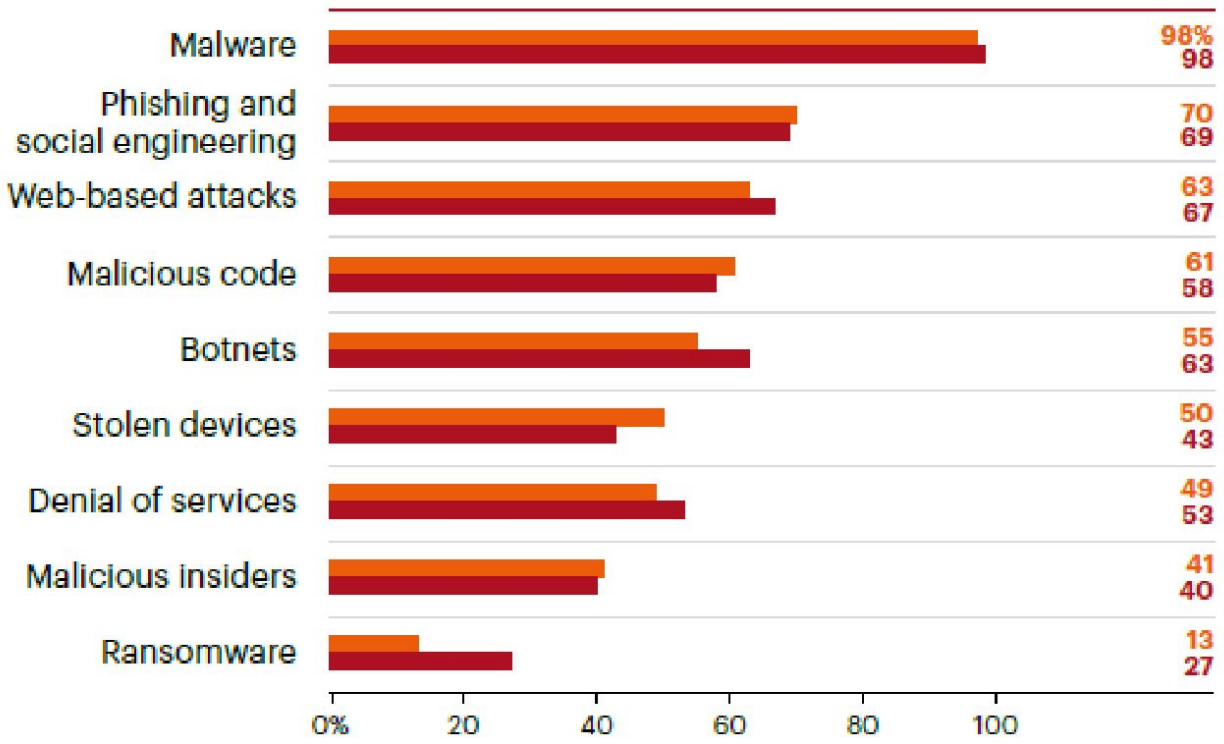


2017 Cost of Cyber Crime Study by Accenture*

Steeper increasing trend in the recent years

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Types of cyber attacks experienced



2017 Cost of Cyber Crime Study by Accenture*

- Percentage of the respondents experienced
- Ransomware doubled

* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Module–I

Introduction

Pillars of information security systems, mathematical background for cryptography – modulo arithmetic, the greatest common divisor, useful algebraic structures, Chinese remainder theorem, cyber-attacks, basics of cryptography preliminaries, elementary substitution ciphers, elementary transport ciphers, secret key cryptography , product ciphers

Cyberattacks

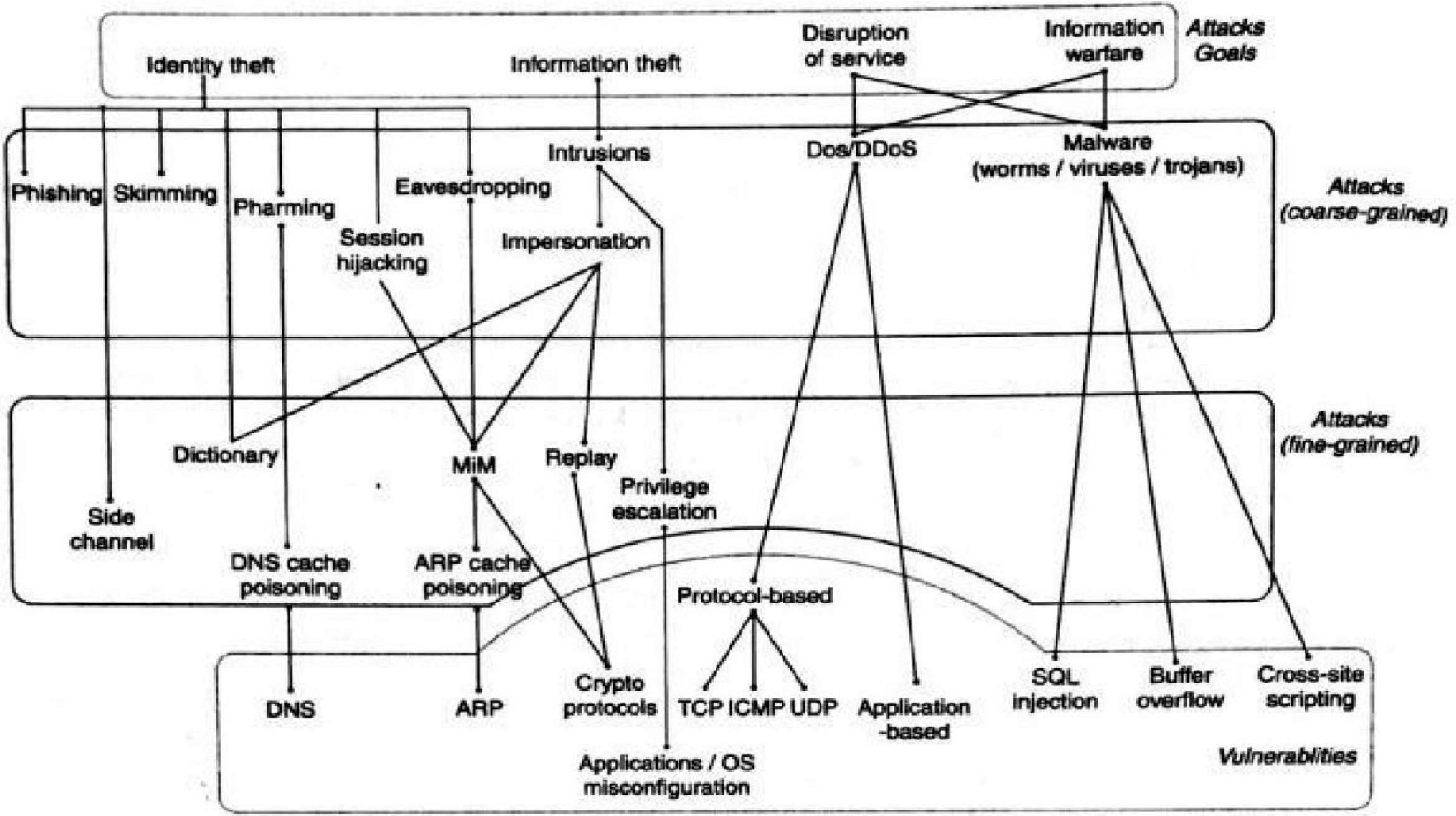
MAIN MOTIVES OF LAUNCHING CYBER-ATTACKS ARE:

1. THEFT OF SENSITIVE INFORMATION.
2. DISRUPTION OF SERVICE.
3. ILLEGAL ACCESS TO OR USE OF RESOURCES.

Common Attacks

Some of the common attacks are :

1. Phishing
2. Pharming
3. Dictionary attacks
4. Denial of Service (dos)
5. Trojan
6. Spyware


Identity theft
Information theft
Disruption of service
Information warfare
Attacks Goals
Phishing
Skimming
Pharming
Session hijacking
Eavesdropping
Intrusions
Impersonation
Dos/DDoS
Malware (worms / viruses / trojans)
Attacks (coarse-grained)
Dictionary
MiM
Replay
Privilege escalation
Side channel
DNS cache poisoning
ARP cache poisoning
Protocol-based
Attacks (fine-grained)
DNS
ARP
Crypto protocols
TCP ICMP UDP
Application -based
SQL injection
Buffer overflow
Cross-site scripting
Applications / OS misconfiguration
Vulnerablities

Vulnerabilities

1. Human Vulnerabilities
2. Protocol Vulnerabilities
3. Software Vulnerabilities
4. Configuration Vulnerabilities

DEFENCE STRATEGIES AND TECHNIQUES

- Access Control—Authentication and Authorization
- Data Protection
- Prevention and Detection
- Response, Recovery, and Forensics

- *Security policy* is the set of rules and practices that regulate how an organization manages and protects it computing and communication resources from unauthorized use or misuse.
- *A security mechanism* is a technique or device used to implement a security policy.
- A *vulnerability* is a weakness or flaw in the architecture, implementation, or operational procedures of a system that could be exploited to cause loss or failure.
- Exploitation of a vulnerability with malicious intent leads to a cyber attack.
- *Access control* is the process of preventing unauthorized access to a computing or communication resource.
- *Authorization* involves granting a specific entity or process the permission to access restricted data or perform a restricted operation.
- *Auditing* is the process of collecting and analyzing relevant information in order to ensure compliance with security policies laid out for an organization.

One or more of the following are implicit when we talk about a secure connection or session between two parties:

- *Entity authentication* is the process of verifying that the entity being communicated with is indeed the entity it claims to be.
- *Message authentication* is the process of verifying the source or origin of the received message.
- *Confidentiality* is the protection of data from disclosure to an unauthorized party or process.
- *Integrity* is the assurance that data has not been modified, tampered with, or made inconsistent in any way.
- *Non-repudiation* offers a guarantee against repudiation or denial by a party of the fact that it created or sent a particular message.

Basics of Cryptography

- Cryptography is the science of disguising messages so that only the intended recipient can decipher the received message.

- The original message or document to be transferred is called **plaintext**

- The plaintext which is encrypted is called **cipher text**.

- The process of converting the original plaintext to cipher text is called **encryption**

- The process of recovering the original plaintext from the cipher text is called **decryption.**

Elementary substitution ciphers

i. Mono alphabetic Ciphers - Caesar cipher

- The most basic cipher is a substitution cipher.
- The simplest substitution cipher is one that replaces each alphabet in a text by the alphabet k positions away (in the modulo 26 sense).
  - For k = 3, the substitutions are D for A, E for B, A for X, B for Y, etc.

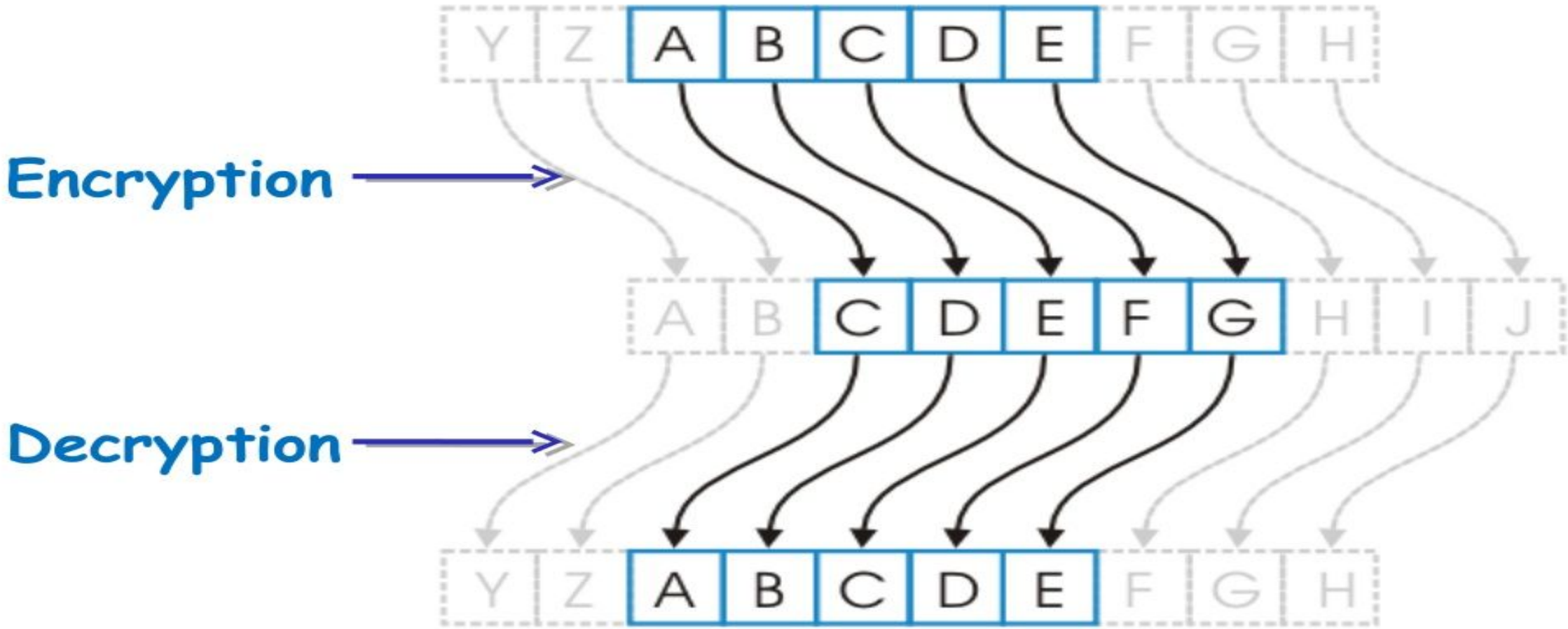
Plaintext: WHAT IS THE POPULATION OF MARS

Cipher text: ZKDW LV WKH SRSXODWLRQ RI PDUV

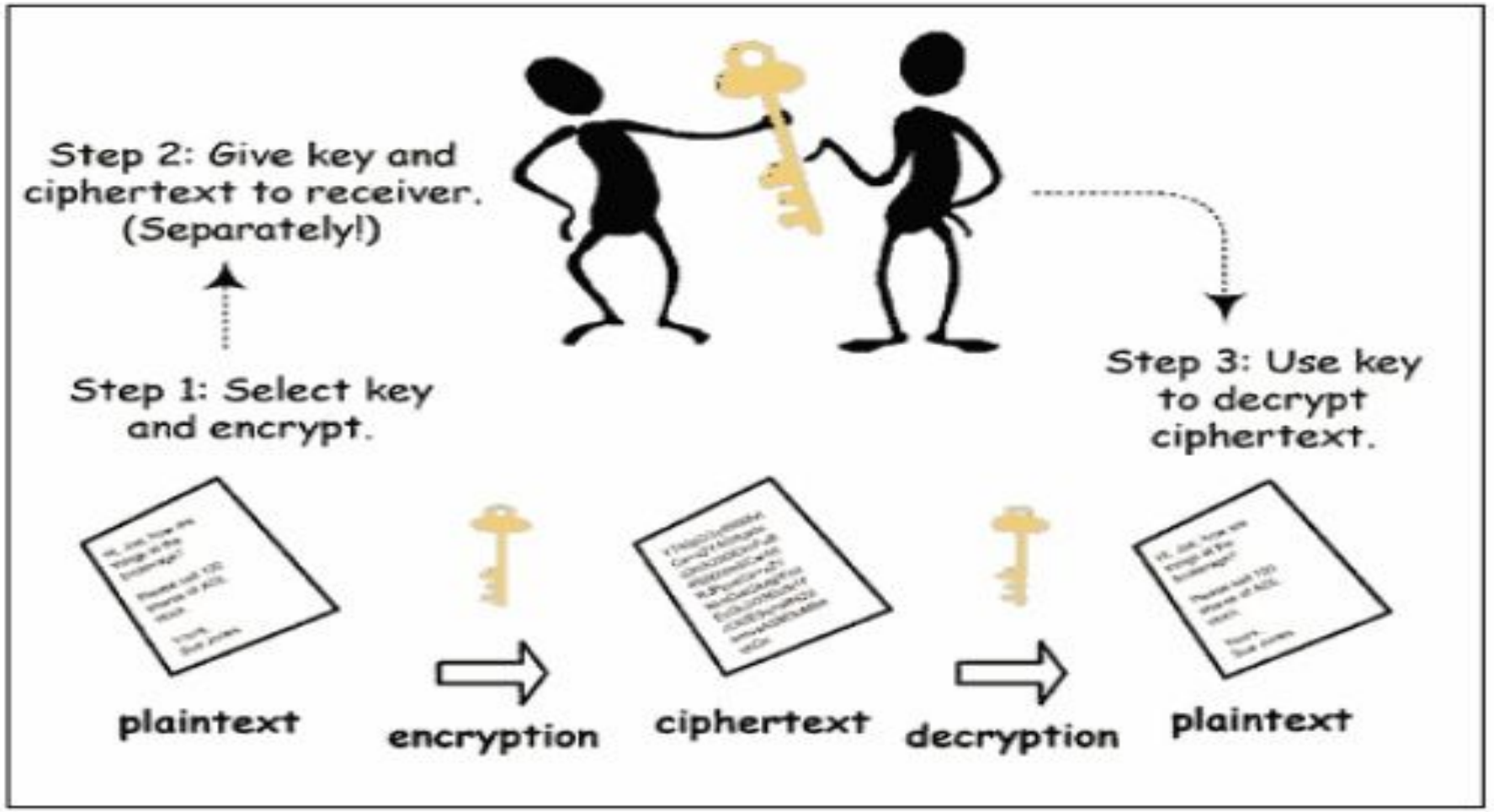
- The "Caesar Box," or "Caesar Cipher," is one of the earliest known ciphers.

- Developed around 100 BC, it was used by Julius Caesar to send secret messages to his generals in the field. In the event that one of his messages got intercepted, his opponent could not read them. This obviously gave him a great strategic advantage.

Caesar Cipher: Mathematical Base



Caesar Cipher: Example



Caesar Cipher

Caesar Cipher earliest known substitution cipher "by Julius Caesar" first attested use in military affairs replaces each letter by 3rd letter.

example:

meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

¨can define transformation as:

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

replaces each letter by 3rd letter →

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

Exercise 1:

Encrypt and decrypt the following plain text using caesar cipher, for k=5

Plain Text: Am studying Information and Network Security

Polyalphabetic Cipher

In a polyalphabetic cipher, the cipher text corresponding to a particular character in the plaintext is not fixed. It may depend on, for example, its position in the block.

1. Vigenere Cipher
2. Hill Cipher

1. Vigenere Cipher

Vigenere Cipher is a method of encrypting alphabetic text.

It uses a simple form of polyalphabetic substitution.

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .

The encryption of the original text is done using the *Vigenère square or Vigenère table*.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Example:

The plaintext is "JAVAPOINT", and the key is "BEST".

The first letter of the plaintext is combined with the first letter of the key. The column of plain text "J" and row of key "B" intersects the alphabet of "K" in the vigenere table, so the first letter of ciphertext is "K".

Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "A" and row of key "E" intersects the alphabet of "E" in the vigenere table, so the second letter of ciphertext is "E".

This process continues continuously until the plaintext is finished.

Ciphertext = KENTTGBOX

Encryption

- The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G.
- Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C.
- The rest of the plaintext is enciphered in a similar fashion.

Plaintext

Key

	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

Decryption

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

Exercise 2:

Encrypt and decrypt using Vigenere cipher

Plain Text:

ATTACKATDAWN

Key:

LEMON

The Hill Cipher

- The Hill cipher is another polyalphabetic cipher proposed by Lester Hill.
- As in the Vigenere cipher, the plaintext is broken into blocks of size m. However, the key in the Hill cipher is an in m x m matrix of integers between 0 and 25.
- Unlike the Caesar and Vigenere ciphers, each character in the ciphertext is a function of all the characters in that block.
- Let p1,, p2, . . . pm,,, be the numeric representation of the characters in the plaintext and let c1,c2,c3,...cm represent the corresponding characters in the ciphertext.
- To compute the cipher text, we map each alphabet to an integer.

Encryption:

$$C = Kp \bmod 26$$

Here,

C and p are row vectors corresponding to the plaintext and cipher text, respectively,

and K is the m x m in matrix comprising the key.

At the receiver end, the plaintext can be recovered from the ciphertext by using

$$p = K\ -1\ C \bmod 26$$

Ex 1: Consider a Hill Cipher using a block size of 2(m=2).

Where P = HELP

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

Ex 2: Consider a Hill Cipher using a block size of 2(m=2).

Where P = HELP

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

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.
4	A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream.	A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of the plain text character in the plain text stream.
5	It includes additive, multiplicative, affine and monoalphabetic substitution cipher.	It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.
6	It is a simple substitution cipher.	It is multiple substitutions cipher.
7	Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.	Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different cryptoalphabets.
8	Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.

One—time Pad

- To perform the one time pad cipher encryption operation, the pad values are added to numeric values that represent the plaintext that needs to be encrypted.
- Each character of the plaintext is turned into a number and a pad value for that position is added to it.
- The resulting sum for that character is then converted back to a ciphertext letter for transmission.

Plaintext:	S	A	C	K	G	A	U	L	S	P	A	R	E	N	O	O	N	E
Plaintext value:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05
One-time pad text:	F	P	Q	R	N	S	B	I	E	H	T	Z	L	A	C	D	G	J
One time pad value:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10
Sum of plaintext and pad:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15
After modulo Subtraction:				03								18						
Ciphertext:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

ELEMENTARY TRANSPOSITION CIPHERS

- A transposition cipher shuffles, rearranges, or permutes the bits in a block of plaintext.
- Unlike a substitution cipher, the number of 0's and 1's in a block does not change after the shuffling.
- For simplicity, we work with characters (letters) rather than bits.
- Imagine a block of plaintext arranged in a matrix row by row as below.

Plaintext: **Begin Operation at Noon (any case)**

$$\begin{bmatrix} b & e & g & i \\ n & o & p & e \\ r & a & t & i \\ o & n & a & t \\ n & & & \end{bmatrix}$$

Rearrange the rows as follows :

Row 1 to row 3

Row 2 to row 5

Row 3 to row 2,

Row 4 to row 1

Row 5 to row 4.

The resulting matrix is:

$$\begin{bmatrix} o & n & a & t \\ r & a & t & i \\ b & e & g & i \\ n & o & o & n \\ n & o & p & e \end{bmatrix}$$

Now rearrange the columns as follows

Column 1 to column 4,

Column 2 to column 3,

Column 3 to column 1,

Column 4 to column 2.

The resulting matrix is

$$\begin{bmatrix} a & t & & o \\ t & i & a & \\ g & i & e & b \\ o & n & o & n \\ p & e & o & n \end{bmatrix}$$

The cipher text thus generated is

A T N O T I A R G I E B O N O N P E O N

- To decrypt the message, the recipient would have to cast the cipher text in a 5 x 4 matrix, reverse the column shuffles, and then reverse the row shuffles.

Block Ciphers and Stream Ciphers

- Block Ciphers With block ciphers, the plaintext is split into fixed size chunks called blocks, and each block is encrypted separately.
- Typically all blocks in the plaintext are encrypted using the same key.
- Block ciphers include DES, AES, RSA, and ECC.
- Block sizes used in secret key cryptography are usually smaller — 64 bits in DES and 128 bits in AES.
- The block size in RSA is much larger — 768 or more bits, while the block size in ECC is about 200 bits.
- If two blocks of plaintext within a message are identical, their corresponding ciphertexts are identical. This statement, however, is only partially true.

Stream cipher

- Stream ciphers typically operate on bits.
- The one-time pad is an example of a stream cipher.
- Practical stream ciphers typically generate a pseudo-random keystream which is a function of a fixed length key and a per-message bit string.
- The key is known to both the sender and the receiver.
- The per-message string could be a message sequence number.
- Alternatively, it could be a random number generated by the sender and transmitted to the receiver along with the encrypted message.
- The ciphertext is itself obtained by performing an $\oplus$ operation between the plaintext and the keystream.
- An example of a stream cipher is RC4 used in the wireless LAN protocol, IEEE 802.11.
- Stream ciphers are usually faster than block ciphers and use less complicated circuits.
- However, RC4 and some other stream ciphers have been shown to be vulnerable to attack.

1. List differences between block cipher and stream cipher
2. List differences between mono alphabetic and poly alphabetic cipher

Secret key cryptography

Secret-key cryptography refers to cryptographic system that uses the same key to encrypt and decrypt data.

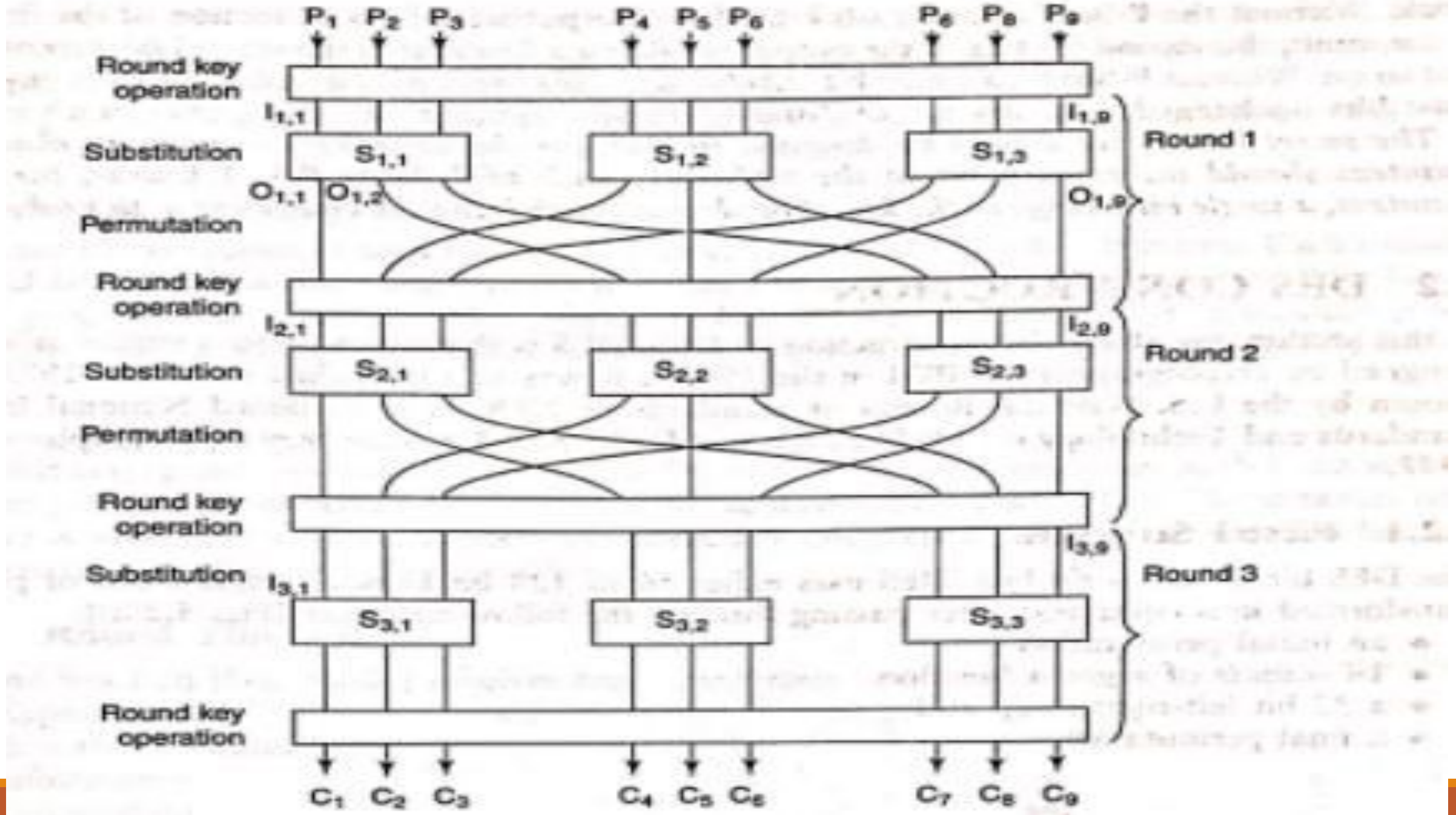
This means that all parties involved have to know the key to be able to communicate securely – that is, decrypt encrypted messages to read them and encrypt messages they want to send.

Therefore the key, being shared among parties, but having to stay secret to 3rd parties – in order to keep communications private – is considered a shared secret.

PRODUCT CIPHERS

The execution of two or more simple ciphers in such a way that the final output or product is cryptographically stronger than any of the component cipher is known as product cipher.

A product cipher combine two or more transformation in a manner that the resulting cipher is more secure than individual component to make it resistant to cryptanalysis.


P1 P2 P3 P4 P5 P6 P7 P8 P9
Round key operation
I1,1 I1,9
Substitution
S1,1 S1,2 S1,3
Round 1
O1,1 O1,2 O1,9
Permutation
Round key operation
I2,1 I2,9
Substitution
S2,1 S2,2 S2,3
Round 2
Permutation
Round key operation
I3,9
Substitution
I3,1
S3,1 S3,2 S3,3
Round 3
Round key operation
C1 C2 C3 C4 C5 C6 C7 C8 C9

The three operations that take place in sequence as shown in Fig. 5.1(Three Round SPN network):

(1) An Operation Involving A Function Of The Encryption Key

(2) A Substitution

(3) A Permutation

These operations are repeated over many rounds or iterations.

Of the three operations, the first is the only one that involves the encryption key. It is usually an ⊕(ex or) of the input with the “round” key.

Each round key is a function of the bits in the encryption key.

the S-box is usually implemented as a table.

If the block size of the cipher is b, the size of the table that implements a b x b

S-box is b x 2b bits.

Thus, the table size increases exponentially with the number of inputs.

To save table space, a single S-box is broken into multiple S-boxes as shown in each round of Fig. 5.1.

If s is the number of S-boxes, the number of inputs to each S-box is b/s._____

Each S-box is now implemented using a table of size (b/s)2b/s bits.

Thus, the total size of all the S-boxes is b x 2b/s bits.

For a block size of 64, the use of eight S-boxes (each with 8 inputs) would bring down the storage requirements to about 16,000 bits.

Usage of s box injects non-linearity into the design of the cipher.

Non-linearity implies the absence of a linear relationship between any subset of bits in the plaintext, cipher text, and key.

Finally, the third step in each round or iteration is a permutation.

A P-Box re-orders the inputs that it receives. it diffuses or spreads contiguous bits of the input across the entire block.

Without the P-Box, the first b/s bits of the output would be a function of the first b/s bits of the input, the second b/s bits of the output would be a function of the second b/s bits of the input and so on.