Computer Security

Chapter 1: Introduction

Definitions

- **Security:** the quality of state if being secure (free from danger or to be protected from adversaries).
- **Threat:** bad things that might happen.
- **Vulnerability:** weakness in your defenses (point whe re a system is suspectible to attack).
- **Attacks:** ways in which the threat may be actualized.
- **Countermeasures:** are techniques for protecting computer or network system from cyber threats.
- **Computer security:** provisions and policies adopted to protect information and property aganist intruders and malicious software while allowing the information and property to remain accessible and productive to it’s intended users.
- **Network security:** provisions and policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network accessible resources.

Types of vulnerabilities

- Physical vulnerabilities
- Natural vulnerabilities
- Hardware and software vulnerabilities
- Media vulnerabilities
- Communication vulnerabilities
- Human vulnerabilities

Types of threats

- Natural
- Unintentional
- Intentional (80% by fully authorized users)

Consequences of risks

- Failure/End of service.
- Reduction of Qos, (Denial of Service(DoS))
- Internal problems in enterprise
- Trust decrease
- Technology leakage
- Human consquences

Countermeasures

- Authentication
- Encryption
- Auditing/inspect the quality of the system
- Administrative procedures
- Standards
- Physical security
- Laws
- Backups
- Removing or reducing vulnerability to prevent an attack and block a threat.

Properties of secured system

- **Confidentiality:** information can only be accessible for reading by authorized parties. It requires that the system should verify the identity of a user.
- **Integrity:** information should be modifies or altered only by authorized parties. Modification includes writing, changing, deletin, and creating the message that is supposed to be transmitted across the network.
- **Availability:** computer and network assets are only available to authorized parties or data are accessible when you need them.
- **Nonrepudiation:** provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. It's assurance that the sender of information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having process the information.

Supplements to CIA

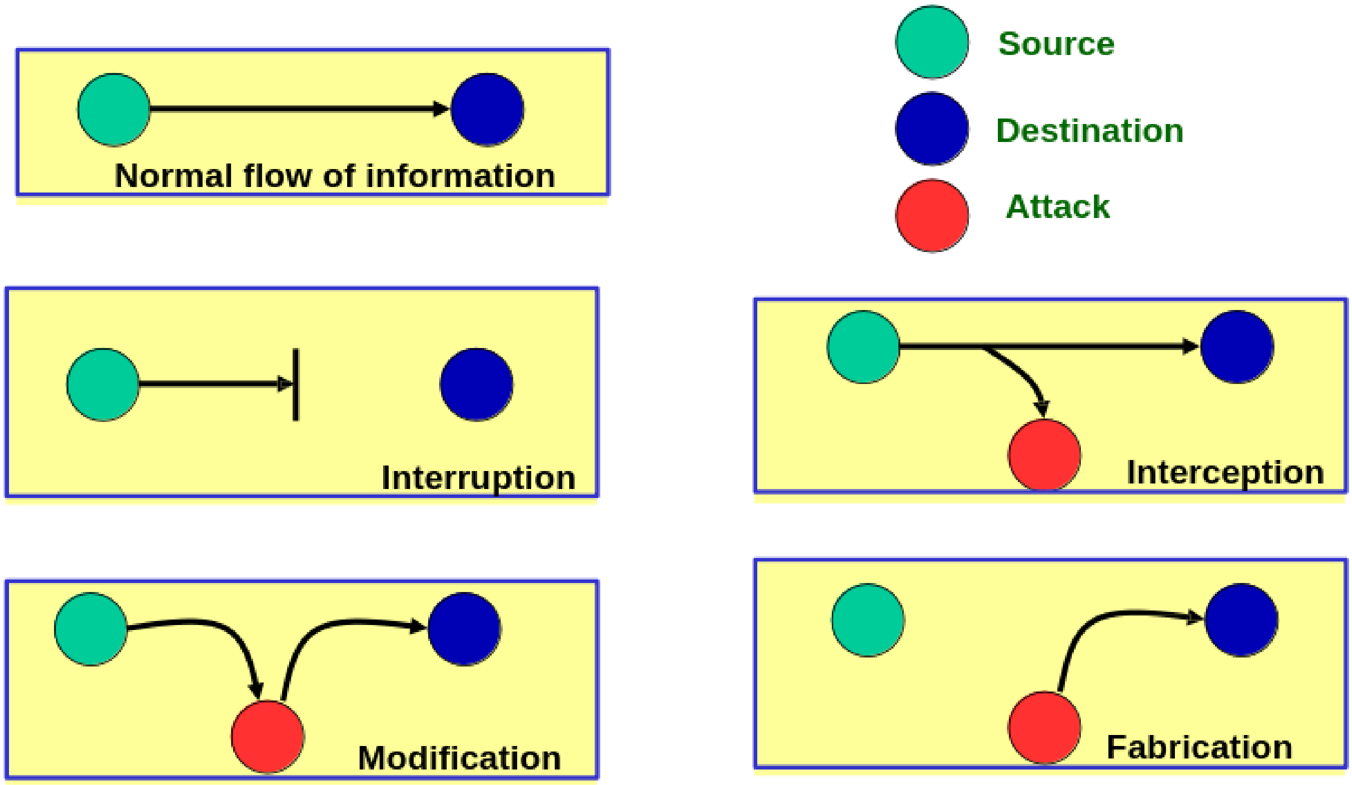
- **Authentication:** correctly identifying the communicating parties.
- **Authorization:** giving different access right for different types of users
- **Accountability:** keeps track of user activity while users are logged in to a network by tracking information such as how long they were logged in, the data they sent or received, their Internet

Protocol (IP) address, the Uniform Resource Identifier (URI) they used, and the different services they accessed.

Goals of security

- `Prevention` - preventing the system from being attacked.
- `Detection` - determinig that an attack is underway, or has occurred and report it.
- `Recovery` - resumption of correct operation. It has two forms:-
  - To stop an attack and to assess and repair any damage caused by that attack.
  - The system continues to function correctly while an attack is underway but the system may disable nonessential functionality.

Categories of attacks



- `Interruption` : An attack on availability
- `Interception` : An attack on confidentiality
- `Modification` : An attack on integrity
- `Fabrication` : An attack on authenticity

Passive attacks vs Active attacks

- **Passive attacks:**
  - Attempt to learn or make use of the information without changing the content of the message and disrupting the operation of the communication. Example: `Eavesdropping` and `Traffic` `analysis`
  - Very difficult to detect.
  - Prevention methods are more effective than detection methods.
- **Active attacks:**
  - Attempts to interrupt, modify, delete, or fabricate messages or information thereby disrupting normal operation of the network.

    - Example: `Jamming`, `Impersonating (Masquerade)`, `Modification`, `Denial of Service (DoS)`, and `Message replay`
    - Very difficult to prevent.
    - Detection methods are more effective than prevention methods.

Internal vs External attacks

- **External attacks:** are carried out by hosts that don't belong to the network domain, sometimes they are called outsider.
- **Internal attacks:** occur when malicious node from the network gains unauthorized access and acts as a genuine node and disrupts the normal operation of nodes.

Network protocol & Security

- `Network protocols` are a set of rules and conventions that govern how data is transmitted and received over a network. These protocols define:
    - Format of data packets,
    - Error handling,
    - Addressing, and other aspects of network communication.

TCP/IP protocol

- It is the foundation of modern networking. It consists of several layers, each with its own set of protocols.
    i. **Application Layer:** This layer includes protocols like HTTP, FTP, SMTP, and DNS. It deals with application-level data and user interactions.
    ii. **Transport Layer:** is responsible for end-to-end communication. It includes TCP for reliable, connection-oriented communication and UDP for connectionless communication.
    iii. **Internet Layer:** is primarily governed by the IP. It is responsible for routing and addressing data packets to their destination across networks.
    iv. **Link Layer:** includes protocols for the physical and data link layers of network communication. Ethernet and Wi-Fi are examples of link layer technologies.

Attacks on different layer of TCP/IP model and their countermeasures

Layer	Attacks	Countermeasures
Application layer	E-mail bombing, Repudiation, data corruption, malicious code attack. Example: SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).	Input validation, output encoding, and parameterized queries.
Transport layer	Session hijacking, Altering checksum, Man in the Middle attack and SYN flooding.	Use Transport Layer Security (TLS) for encryption, employ firewalls and intrusion detection systems, and implement SYN/ACK cookies.
Network layer	IP spoofing, ICMP echo, Worm hole, black hole, gray hole, Byzantine, flooding, DDoS attacks, or routing attacks.	Implement packet filtering, use Access Control Liss (ACLs), and deploy intrusion detection and prevention systems (IDPS)
Data link layer	MAC address spoofing, ARP poisoning, or VLAN hopping Traffic analysis, disruption (E.g MAC IEEE 802.11 Wi-Fi)	Implement port security, use MAC address filtering, empoy ARP inspection, and configure VLAN ACLs (Access Control Lists)
Physical layer	Wiretapping or eavesdropping on physical communication channels. Example: Jamming, interception, eavesdropping.	Use secure physical cabling and encryption technologie, like VPNs or TLS/SSL for higher-layer data protection.
Cross-layer attack	DoS, impersonation, replay, MiM attack.	Cross-layer traffic analysis

Common security attacks and their countermeasures

Attacks	Countermeasures
Finding a way into a network	Firewalls
Exploting software bugs, buffer overflows	Intrusion Detection Systems (IDS)
Denial of Service (DoS)	Access filtering, IDS
TCP hijacking	IPSec
Packet sniffing	Encyrption (SSL, HTTPS)
Social problems	Education

Malicious code

- A software written intentionally cause unanticipated or undesirable effects.
- Basic forms:
  - **Virus:**
    - Self-replicating software that attaches itself to other software.
    - Replicates within computer system, potentially attaching itself to every other program.
    - Innocuous, Humorous, Data altering, Catastrophic
    - Consists two parts:
      - `Replicator` - esponsible for copying the virus to other executable Programs.
      - `Payload` - action of a virus (part of the virus that performs modification and corruption of data).
    - Anti-virus, proper firewall configuration and various scanners serve as pervention and detection techniques aganist virus.
  - **Worm:**
    - Computer program that can run independently, can propagate a complete working version of itself onto other host on a network, may consume computer resources destructively.
    - Stand-alone applications
    - Do not need a carrier program
    - Replicate by spawning copies of themselves.
    - More complex and harder to write than the virus programs.
    - Multitasking computers with open network standards are vulnerable.

    - **Trojan horse:**
        - A programs that appears to have a useful function, but also has a hidden and malicious purpose that evades security mechanism, sometimes by exploiting the legitimate authorization of the user who invokes the programs.
        - A worm which pretends to be a useful program or virus purposely attached to a useful program prior to distribution.
        - Untrained users are vulnerable.
        - User training is one of the best prevention methods.

Aunthentication Mechanisms

- `Authentication` is the process or action of verifying the identity of a user or process.
- `Authenticator` is an entity which is used to confirm the identity of a user.

Why do we need authentication?

- To prevent attacks
- To revoke access from attackers
- To identify user’s identity which required to allow access to confidential data.

How to authenticate a human to a machine?

- Something the user knows
    - Passwords
        - Best practices
            - Choose passwords based on passphrase
            - Use password cracking tool to test for weak pwds
            - Require periodic password changes
        - Possible attacks
            - `Denial of Service (DoS)`
            - `Dictionary attack` : attacker pre-computes h(x) for all x in a dictionary of common passwords.
            - Other issues:
                - Too many passwords to remember
                - Failure to change default passwords
                - Social engineering
                - Bugs, keystroke logging and spyware

        - Password cracking tools:
            - Password Crackers
            - Password Portal
            - L0phtCrack and LC4 (Windows)
            - John the Ripper (Unix)
- Something the user has
    - ATM and smart cards
    - Car key
    - 2-factor Authentication
- Something the user is
    - Biometrics
        - Desirable replacement for passwords.
        - Hard to forge
        - Hand Geometry:
            - Popular form of biometric
            - Suitable for authentication
            - Quick
            - Can’t be used on very young and very old users
            - Relatively high equal error rate
        - Iris pattern:
            - Little or no genetic influence
            - Different even for identical twins
            - Pattern is stable through lifetime
            - Attackers could use photo of eye but it can be detected using scanner with light to be sure it’s living iris.

Chapter 2: Cryptography

Basic terms

- **Cryptography**: the study of encryption.
- **Encryption**: process by which plain text is converted to cipher text.
$$C = E(P)$$
- **Decryption**: process of obtaining the plain text from the cipher text.
$$P = D(C)$$
- **Cryptography**: sche:w
- mes for encryption and decryption.
- **Encryption algorithm**: technique or rules selected for encryption.
- **Key**: is secret value used to encrypt and/or decrypt the text.
- **Cryptanalysis**: study of “breaking the code”.
- **Cryptology**: cryptography and cryptanalysis.
- **Unconditional security**: when ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much computer power or time is available.
- **Computational security**: when decryption takes too long or too many resources more than the allocated.

Characteristics of Cryptographic systems

- Operations used:
  - `Substitution` : replace (bit, letter, group of bits letters).
  - `Transposition` : rearrange the order.
  - `Product` : use multiple stages of both substitution and transposition.
- Number of keys used:
  - `Symmetric` : same key , secret-key, private-key.
  - `Asymmetric` : different key , public-key.
- Way in which the plain text is processed:
  - `Block cipher`
  - `Stream cipher`

Substitution Ciphers

- **Caesar Cipher**:
  - used by julius caesar.
  - substitutes each letter of the alphabet with the letter standing three places further down the alphabet.

    $$C = E(3, p) = (p + 3) mod(26)$$
  - Algorithim:

    $$c = E(k, p) = (p + k) mod(26)$$

    $$p = D(k, c) = (c – k) mod(26)$$

    where k is secret key between 1 and 25.
- **Monoalphabetic Cipher**:
  - rather than just shifting the alphabet monoalphabetic cipher could shuffle the letters arbitrarily. Each plaintext letter maps to a different random ciphertext letter with 26 letters long key.

    $$E(x) = (ax + b) mod(26)$$
  - $26! = 4 \times 10^{26}$ keys
- **Playfair Cipher**:
  - a polyalphabetic cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
  - the first digraph substitution cipher.
  - Steps:
    - First create 5×5 matrix and fill it using each character in the given key (no duplicate characters). Since the matrix can only contain 25 characters put i and j in the same cell.

Example: key = MONARCHY, plain text = INSTRUMENTS

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

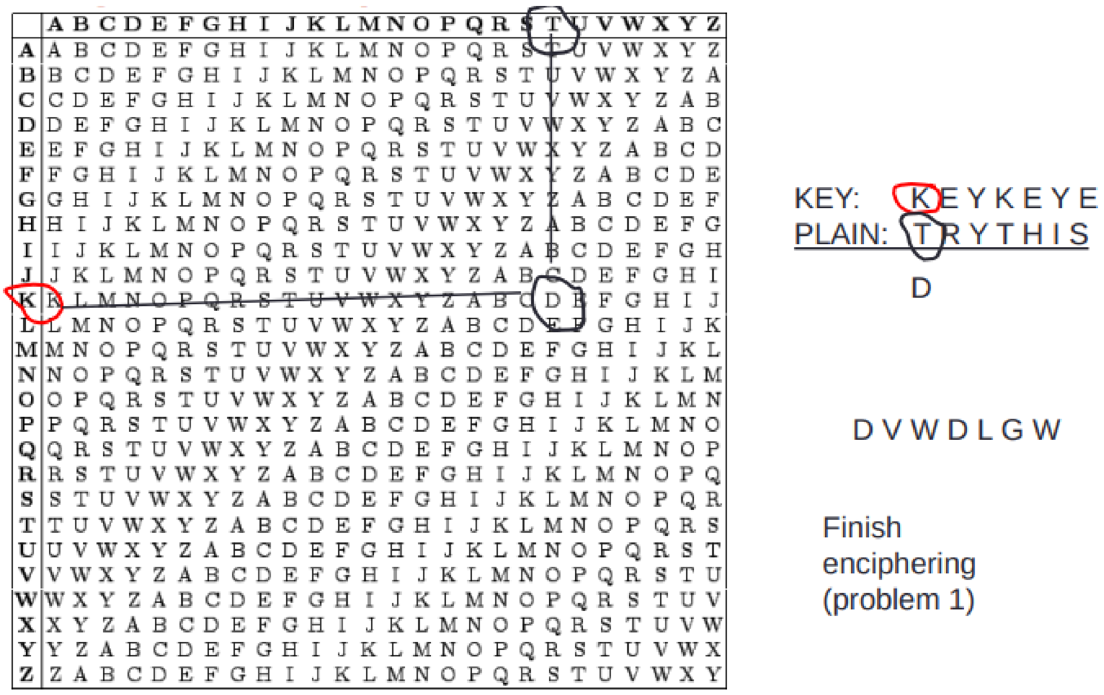
- Split the given plain text to pair of letters:
    - If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter.
      Example: plain text = art -> “ar” “tz” where “z” act as bogus letter
    - Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.
      Example: plain text = hello -> “he” “lx” “lo” where “x” act as bogus letter
- For each pair of letters obtained in the second step, apply playfair cipher:
    - If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).
    - If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
    - If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
    - Using the above example we can apply playfair cipher like this:

Pair	Case	Cipher text
“IN”	Neither	“GA”
“ST”	Same row	“TL”
“RU”	Neither	“MZ”
“ME”	Same column	“CL”
“NT”	Neither	“RQ”
“SZ”	Neither	“TX”

$$C = E(''INSTRUMENT'') = ''GATLMZCLRQTZ''$$

- Compared to monoalphabatic it’s secured but can be easily broken if both plain text and cipher text are known.

- **Polyalphabetic ciphers**:
  - uses multiple substitution alphabets.
  - make cryptanalysis harder with more alphabets to guess and flatter frequency distribution.
  - use a key to select which alphabet is used for each letter of the message:
    - use each alphabet in turn.
    - repeat from start after end of key is reached.
  - **Vigenère Cipher**:
    - simplest polyalphabetic substitution cipher.
    - multiple Caesar cipher.
    - Steps:
      - write the plaintext out.
      - write the keyword repeated above it.
      - use each key letter as a caesar cipher key.
      - encrypt the corresponding plaintext letter.



	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

KEY: KEYKEYE

PLAIN: TRYTHIS

D

DVWDLGW

Finish enciphering (problem 1)

- The strength of the Vigenère cipher is that it is not susceptible to frequency analysis due to the fact that the cipher rotates through different shifts, so the same plaintext letter will not always be encrypted to the same ciphertext letter.
- A Vigenère cipher is difficult to crack using brute-force because each letter in a message could be encoded as any of the 26 letters. Because the encoding of the message depends on the keyword used, a given message could be encoded in 26^k ways, where k is the length of the keyword.

- The primary weakness of the Vigenère cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the length of the key, then the ciphertext can be treated as interwoven Caesar ciphers, which, individually, can be easily broken. Repetitions in the ciphertext indicate repetitions in the plaintext, and the space between such repetitions hint at the length of the keyword.

Transposition Ciphers

- Transposition ciphers differ form substitution cipher technique in addition to replace on alphabet with another they perform some permutation over the plain text alphabet.
- Used by modern encryption algorithms such as DES and 3DES.
- Steps:
    - write your plaintext message along the rows of a matrix of some size.
    - generate ciphertext by reading along the columns. The order in which we read the columns is determined by the encryption key.
- **Spartians Cipher (Spartan scytale)**:
    - create $key \times n$ matrix where $n = floor(length/key)$ then fill it with each letter in the plain text.

      Exmaple: plain text = “Start the war today” key = 4, n = $16/4$ = 4

S	t	a	r
t	t	h	e
w	a	r	t
o	d	a	y

    - combine each letter in the every column to get the cipher text.
      $C = E("Start\ the\ war\ today") = "stwottadahrarety"$
- **Rail Fence Cipher**:
    - Write the plaintext downwards on successive “rails” of an imaginary fence. When you get to the bottom start moving up.

      Exmaple: plain text = “Start the war today” rails = 3

S				**t**				**w**		
	t		r		t		e		a	
		a				h				r

- Write the message line by line.
  $C = E(\text{"}Start\,the\,war\,today\text{"}) = \text{"}stwtrteaahr\text{"}$

- **Columnar Transposition**:
  - Write the message in rows of a fixed length, and then read out again column by column. The columns are chosen in some scrambled order. Both the length of the rows and the permutation of the columns are usually defined by a keyword.
  - Any spare spaces are filled with nulls or left blank or placed by a character().
    Exmaple: plain text = “Start the war today” key = “HACK”, order of letter in the key = “4123”

H	A	C	K
3	1	2	4
S	t	a	r
_	t	h	e
_	w	a	r
_	t	o	d
a	y	_	_

$$C = E(\text{"}Start\,the\,war\,today\text{"}) = \text{"}Sattwtyahaoredrd\text{"}$$

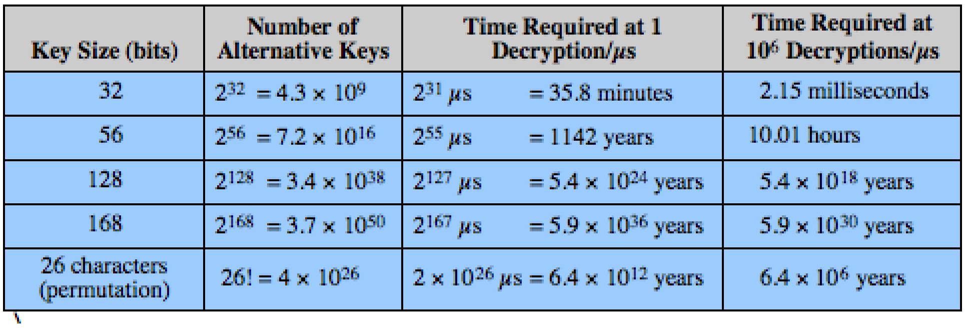
- **Route Cipher**:
  - The plaintext is first written out in a grid of given dimensions, then we read it off in a pattern given in the key.
    Example: The key say: read message from top right corner down and to the left.

S	t	a	r
t	t	h	e
w	a	r	t
o	d	a	y

$$C = E(”Start\,the\,war\,today”) = ”retyahrattadStwo”$$

Crptanalytic Attacks

- Types of Attacks:
  - An attacker has only the ciphertext and his goal is to find the corresponding plaintext.
  - An attacker has a ciphertext and the corresponding plaintext and his goal is to find the key.
- `Cryptanalytic attack` exploits the characteristics of the algorithm.
- **Brute Force Attack (BFA)**:
  - the attacker tries to determine the key by attempting all possible keys.
  - time required to break the system by getting the secret key depends on the size of the key.



Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

  - Ciphertext Only Attacks (COA):
    - In this method, the attacker has access to a set of ciphertext(s) but not the plain text.
    - COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack.
    - Modern cryptosystems are guarded against ciphertext-only attacks
  - Known Plaintext Attack (KPA):
    - In this method, the attacker knows the plaintext for some parts of the ciphertext.
    - Know/suspect plaintext & ciphertext -> Find key or algorithm
    - The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method.

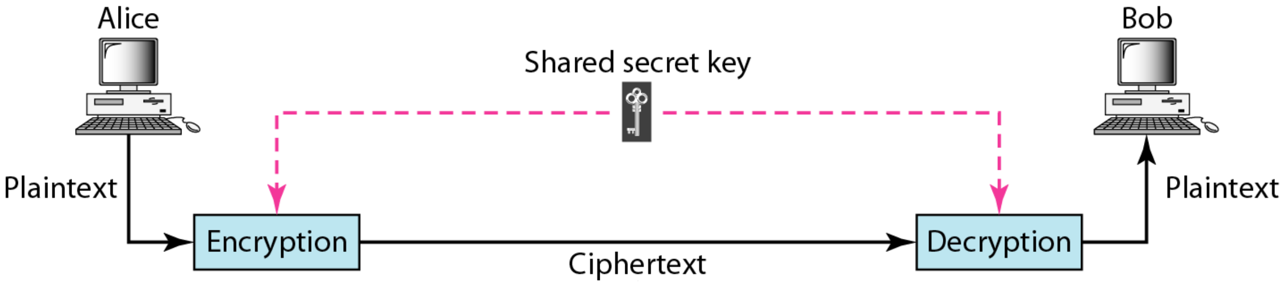
  - Chosen Plaintext Attack (CPA):
    - In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key.
    - select plaintext and obtain ciphertext -> select ciphertext and obtain plaintext -> select plaintext or ciphertext to en/decrypt.

Language Redundancy and Cryptanalysis

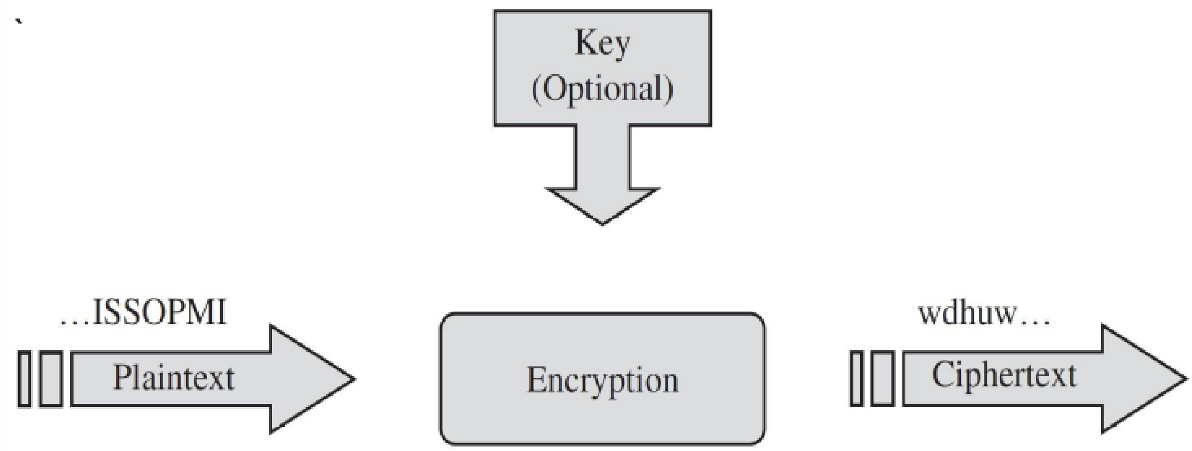
- Letters are not equally commonly used in English, `E` is by far the most common letter followed by `T` , `R` , `N` , `I` , `O` , `A` , `S` . Other letters like `Z` , `J` , `K` , `Q` , `X` are fairly rare.

Categories of cryptography

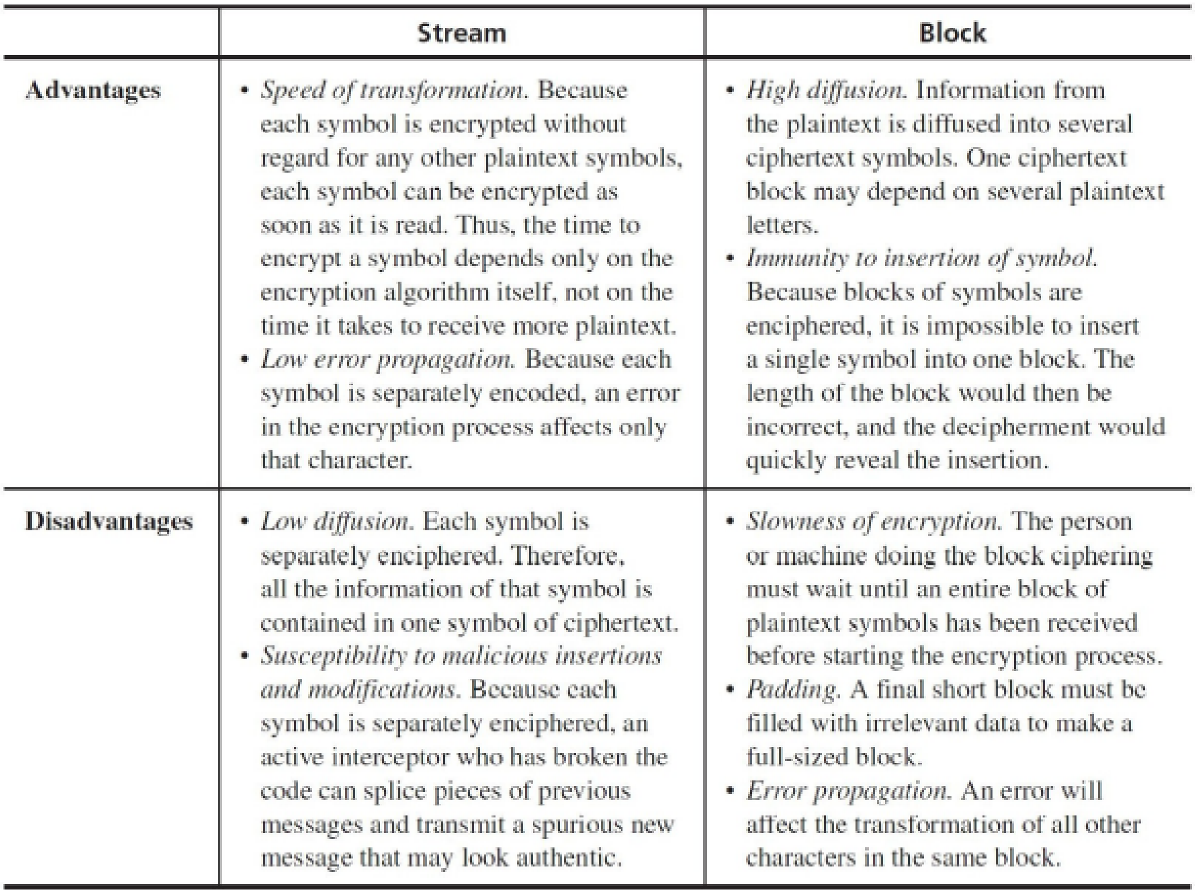
- **Symmetric**:
  - same key (secret key) used between the sender and the receiver.



  - Stream cipher:
    - encrypt data one bit or one byte at a time.
    - used if data is a constant stream of information.
    - combines plaintext digits with a pseudo-random cipher digit stream (keystream) to obtain the ciphertext.



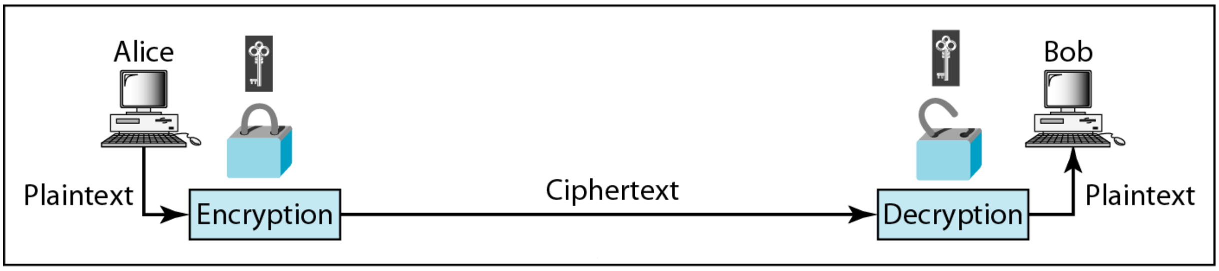
- Block cipher:
    - operates on fixed length group of bits, called blocks, with an unvarying transformation.
    - takes n block of plain text as input and output a corresponding n block of cipher text. Same thing applies for decryption.
    - the exact transformation is controlled using a second input which is the secret key.



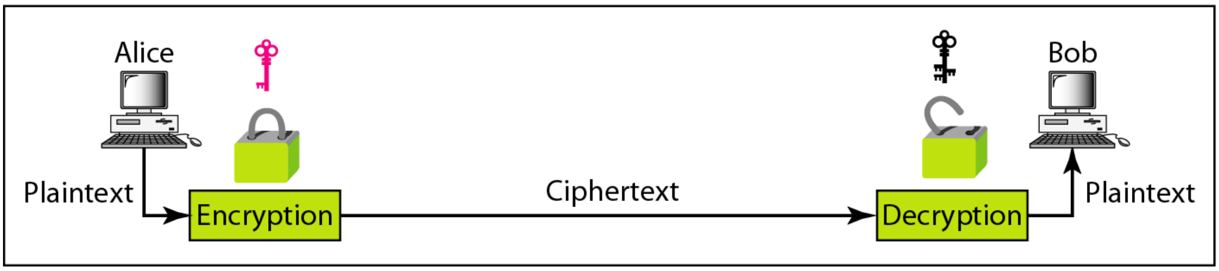
	Stream	Block
Advantages	• *Speed of transformation.* Because each symbol is encrypted without regard for any other plaintext symbols, each symbol can be encrypted as soon as it is read. Thus, the time to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext. • *Low error propagation.* Because each symbol is separately encoded, an error in the encryption process affects only that character.	• *High diffusion.* Information from the plaintext is diffused into several ciphertext symbols. One ciphertext block may depend on several plaintext letters. • *Immunity to insertion of symbol.* Because blocks of symbols are enciphered, it is impossible to insert a single symbol into one block. The length of the block would then be incorrect, and the decipherment would quickly reveal the insertion.
Disadvantages	• *Low diffusion.* Each symbol is separately enciphered. Therefore, all the information of that symbol is contained in one symbol of ciphertext. • *Susceptibility to malicious insertions and modifications.* Because each symbol is separately enciphered, an active interceptor who has broken the code can splice pieces of previous messages and transmit a spurious new message that may look authentic.	• *Slowness of encryption.* The person or machine doing the block ciphering must wait until an entire block of plaintext symbols has been received before starting the encryption process. • *Padding.* A final short block must be filled with irrelevant data to make a full-sized block. • *Error propagation.* An error will affect the transformation of all other characters in the same block.

- Shanon Substitution-Permutation ciphers:
    - contains two basic operations substitution (S-box) and permutation (P-box).
    - `Diffusion` : dissipates statistical structure of plaintext over bulk of ciphertext.
    - `Confusion` : makes relationship between ciphertext and key as complex as possible.
    - Characteristics of “GOOD” ciphers:
        - The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
        - The set of keys and the enciphering algorithm should be free from complexity.
        - The implementation of the process should be as simple as possible.
        - Errors in ciphering should not propagate and cause corruption of further information in the message.
        - The size of the enciphered text should be no larger than the text of the original message.

  - **Asymmetric**:
    - uses two different keys private key (kept by the receiver) and public key (kept by the sender).



a. Symmetric-key cryptography



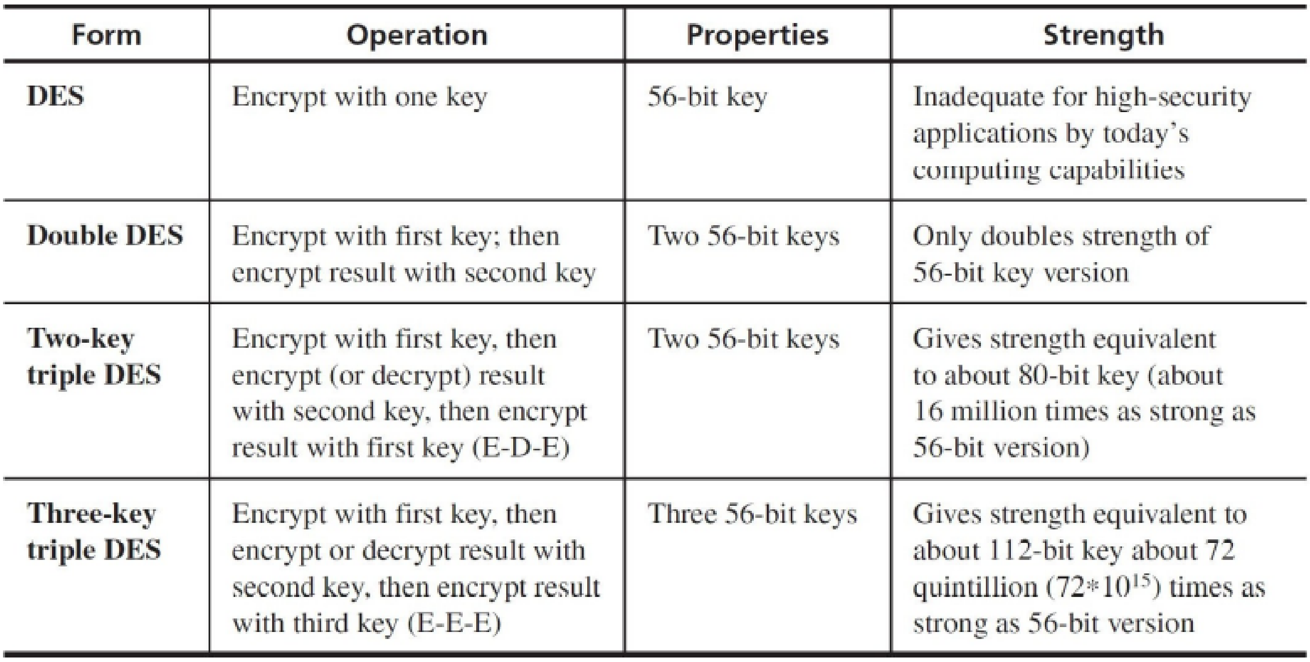
b. Asymmetric-key cryptography

DES (Data Encryption Standard)

- DES encrypts 64-bit blocks by using a 56-bit key.
- Steps:
  - 56 bit of key produced by removing the `8`, `16`, `24`, `32`, `40`, `48`, `56` and `64` th bit of the original secret key.
  - 64-bit plain text block is handed over to an initial Permutation (IP) function.
  - The initial permutation is performed on plain text.
  - Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
  - Now each LPT and RPT go through 16 rounds of the encryption process. 48 bit key generated from the 56 bit key in every round created by method called `key transformation`.
  - In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block

- The result of this process produces 64-bit ciphertext. ![DES-steps](media/DES-steps.png "steps in DES")

- Basic forms:



Form	Operation	Properties	Strength
DES	Encrypt with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
Double DES	Encrypt with first key; then encrypt result with second key	Two 56-bit keys	Only doubles strength of 56-bit key version
Two-key triple DES	Encrypt with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit keys	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
Three-key triple DES	Encrypt with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit keys	Gives strength equivalent to about 112-bit key about 72 quintillion ($72*10^{15}$) times as strong as 56-bit version

- Modes of operation:
  - `Electronic Codebook (ECB)` : Each 64-bit block is encrypted and decrypted independently.
  - `Cipher Block Chaining (CBC)` . Each 64-bit block depends on the previous one and uses an Initialization Vector (IV).
  - `Cipher Feedback (CFB)` . The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit.
  - `Output Feedback (OFB)` . Much like CFB, except that the encryption algorithm input is the output from the preceding DES.
  - `Counter (CTR)` . Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each subsequent block.
- weakness:
  - key size is small.
  - slower compared to AES and other algorithms.
  - vulnerable for exhaustive key search attack.

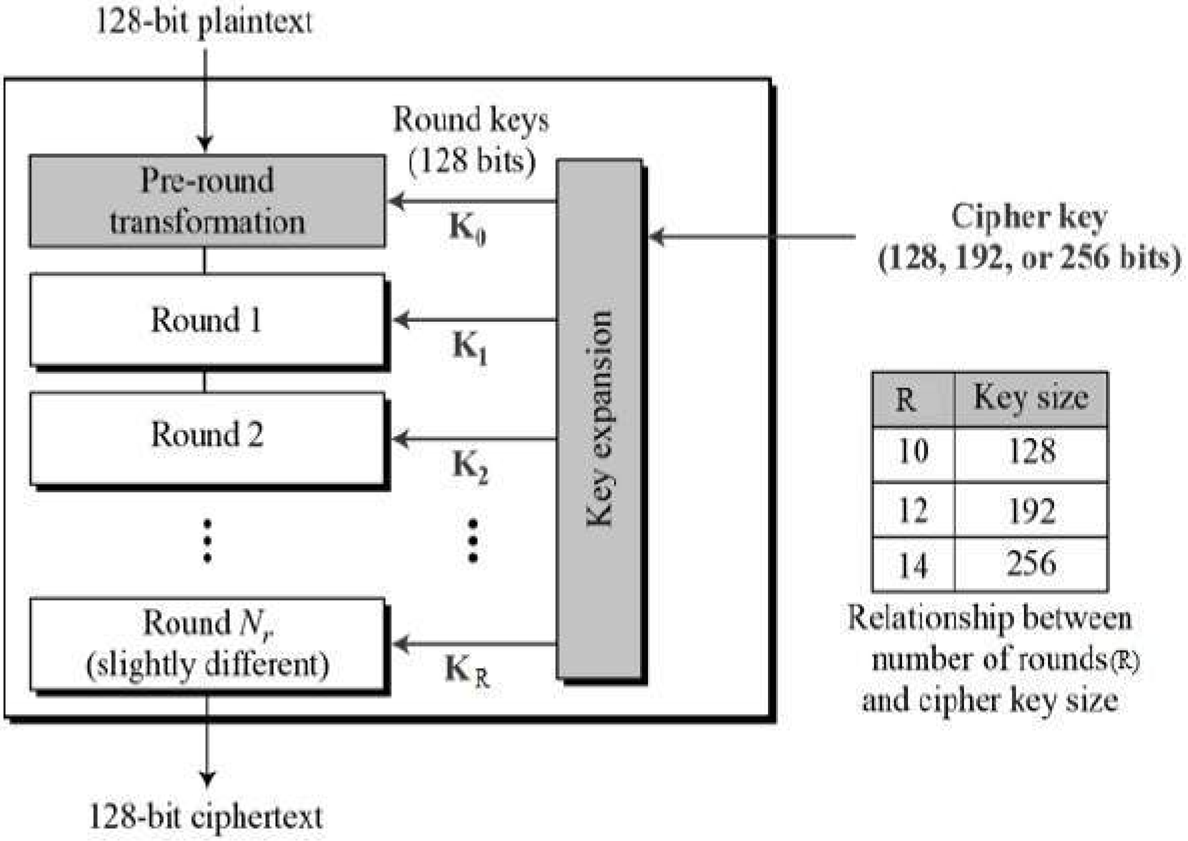
AES (Advanced Encryption Standard)

- most popular and widely adopted symmetric encryption algorithim.
- introduced to replace DES.

- features:
  - symmetric key and symmetric block cipher.
  - relies on substitution-permutation network principle.
  - 128-bit data, 128/192/256-bit keys.
  - stronger and faster than Triple-DES.
  - provide full specification and design details.
  - software implementable in C and Java.
  - performs all its computations on bytes rather than bits.
  - variable number of rounds unlike DES.
- steps:
  - generates 16 byte from the 128 bit input using 4×4 matrix.

    ```
    [ b0 | b4 | b8  | b12 |
    | b1 | b5 | b9  | b13 |
    | b2 | b6 | b10 | b14 |
    | b3 | b7 | b11 | b15 ]
    ```

  - total number of rounds and subkeys generated from the original symmetric key.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

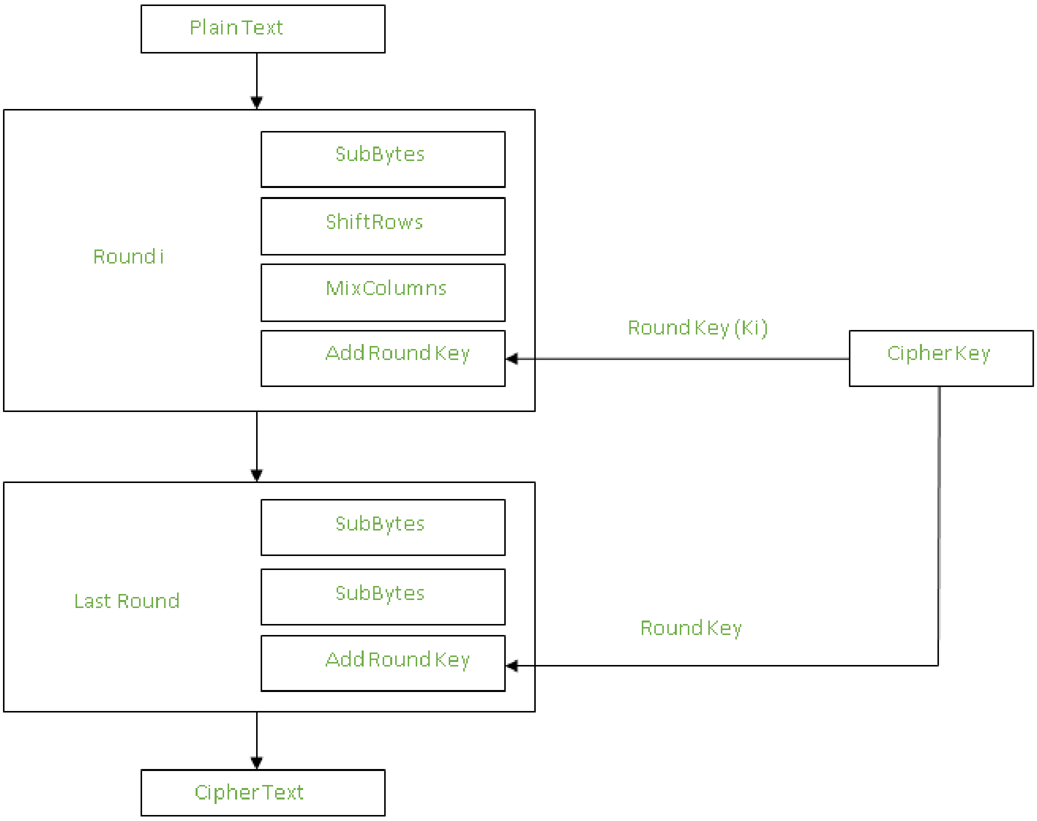
- each round comprises of 4 steps:
    - `SubBytes` : performs substitution on each byte with another byte different from the original and the complement.
    - `ShiftRows` : shifts a particular number of times.
        - The first row is not shifted.
        - The second row is shifted once to the left.
        - The third row is shifted twice to the left.
        - The fourth row is shifted thrice to the left.

```
[ b0  | b1  | b2  | b3  ]         [ b0  | b1  | b2  | b3  ]
| b4  | b5  | b6  | b7  |    ->   | b5  | b6  | b7  | b4  |
| b8  | b9  | b10 | b11 |         | b10 | b11 | b8  | b9  |
[ b12 | b13 | b14 | b15 ]         [ b15 | b12 | b13 | b14 ]
```

- `MixColumns` : each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

```
[ c0 ]      [ 2  3  1  1 ]  [ b0 ]
| c1 |   =  | 1  2  3  1 |  | b1 |
| c2 |      | 1  1  2  3 |  | b2 |
[ c3 ]      [ 3  1  1  2 ]  [ b3 ]
```

- `Add Round Key` : resultant output of the previous stage is XOR-ed with the corresponding round key.



DES vs AES

	DES	AES
Developed	1977	2000
Key length	56 bits	128, 192 or 256 bits
Cipher Type	Symmetric block	Symmetric block
Block size	64 bits	128 bits
Security	Inadequate	Secure

Issues with symmetric key cryptography

- Large number of keys required if the number of communicating users increase.
- No support for digital signature.
- Security of exchange keys.

Public key cryptography

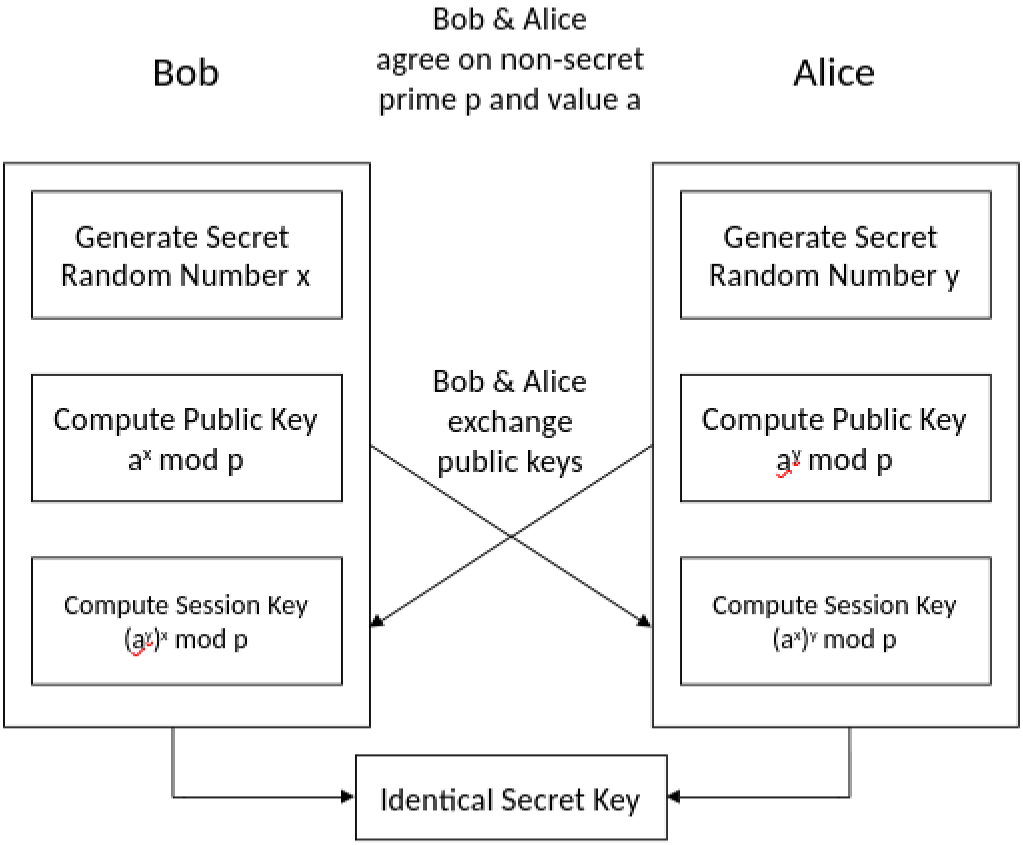
- also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and one of which is public.
- major parts:
  - `Plaintext` : message to be encrypted.
  - `Encryption algorithim` : performs substitutions and transformations to the plaintext.
  - `Public and Private keys` : a pair of keys, one for encryption and the other for decryption.
  - `Ciphertext` : this is the encrypted or scrambled message.
  - `Decryption algorithim` : generates the ciphertext and the matching key to produce the plaintext.

$$C = E(K\ pub, P)$$

$$P = D(K\ priv, C)$$

Diffie-Hellman Mathematical Analysis

- Provided ability for messages to be exchanged securely without having to have shared some secret information previously.
- Inception of public key cryptography which allowed keys to be exchanged in the open.
- Avoided Man in Middle attack.


Bob
Bob & Alice agree on non-secret prime p and value a
Alice
Generate Secret Random Number x
Generate Secret Random Number y
Compute Public Key a^x mod p
Bob & Alice exchange public keys
Compute Public Key a^y mod p
Compute Session Key $(a^y)^x$ mod p
Compute Session Key $(a^x)^y$ mod p
Identical Secret Key

Symmetric vs Asymmetric cryptography

Symmetric	Asymmetric
Same key used for both encryption and decryption	Different key for both encryption and decryption
Faster	Slower (upto 10,000 times)
Need secure channel to transfer the key	Secure channel not needed to transfer the key
Used when performance is required	Used to exchange key, encrypt communication, protect symmetric keys, authentication, signing

RSA algorithim

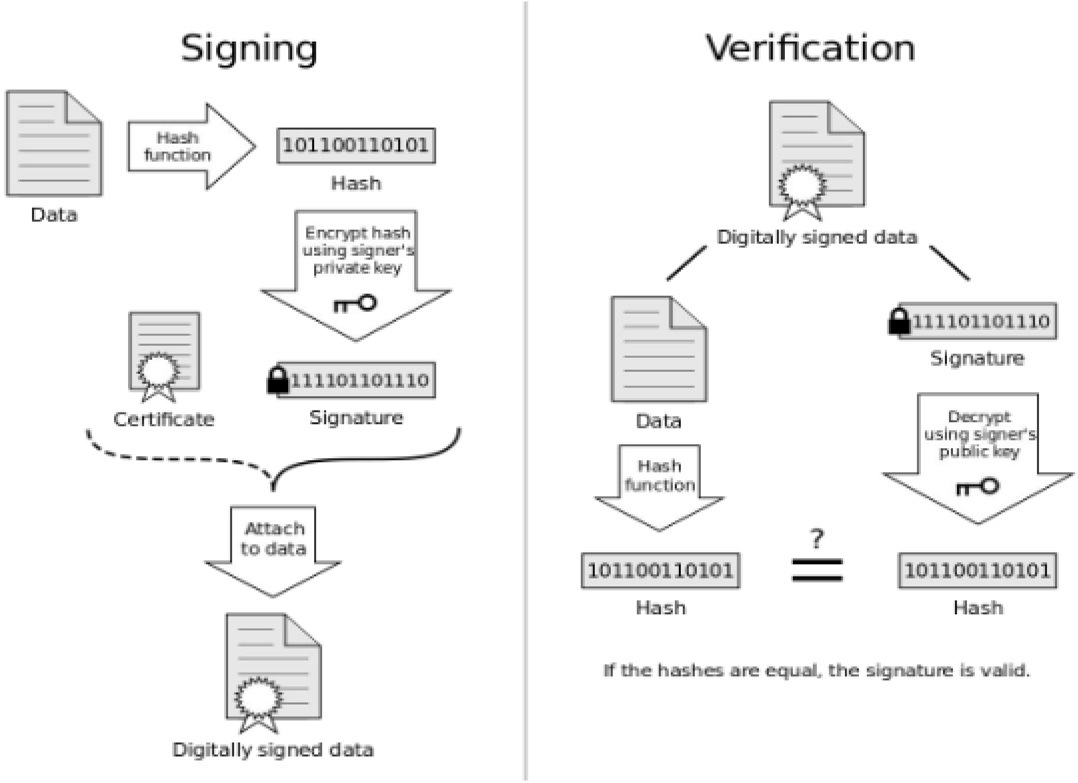
- The first practicable public-key cryptosystems and is widely used for secure data transmission.
- Both public and private key are interchangeable.
- Variable Key Size (512, 1024, or 2048 bits).
- Operates with arithmetic `mod n`, which makes factorization exteremely difficult.
- Steps:
  - choose two large prime numbers `p` and `q`.
    let $p = 61\, and\, q = 53$
  - compute $n = p \times q$ and $z = \phi(n) = (p-1)(q-1)$
    $n = 61 \times 53 = 3233$
    $z = (61-1)(53-1) = 60 \times 52 = 3120$
  - choose prime number `e` (often 3, 17 or 65537) which is less than `z` and has no common factor with `z`
    $let\ e = 17,\ where\, gcd(17, 3120) = 1\ and\ 3120 > 17$
  - choose prime number `d` where $(d \times e)\, mod \phi(n) = 1$
    $d = 2753$
  - public key `(n, e)` and private key `(n, d)`.
    $public\, key = (3233, 17)\ and\, private\, key = (3233, 2753)$
    $C = M^e\, mod(n)\ and\, M = C^d\, mod(n)$
- `El Gamal`: another asymmetric encryption type that’s used in protocols like PGP.

Encryption protocols

- **Pretty Good Privacy (PGP)**:
  - used to encrypt e-mail using session key encryption.
  - combines RSA, Triple DES, and other algorithms.
- **Secure/Multipurpose Internet Mail Extension (S/MIME)**:
  - Newer algorithm for securing e-mail.
  - Backed by Microsoft, RSA, AOL.
- **Secure Socket Layer(SSL) and Transport Layer Socket(TLS)**:
  - Used for securing TCP/IP Traffic.
  - Mainly designed for web use.
  - Can be used for any kind of internet traffic.

Digital Signature

- A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document.
- A valid digital signature gives a recipient reason to believe that the message was created by a trustable sender, such that the sender cannot deny having sent the message and that the message was not altered in integrity.
- Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.
- Components:
  - a file
  - demonstartion that the file hasn’t been altered
  - indication of who applied the signature
  - validation that the signature is authentic, that it belongs the singer
  - connection of the signature to the file



Hash Functions

- also called message digests, use one-way encryption with no key.
- for any input value, you will always receive the same output value whenever the hash function is run.
- it is impossible to recover the the contents or length of the plaintext from hash.
- typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus.
- commonly employed by many operating systems to encrypt passwords.
- provide a measure of the integrity of a file.
- algorithims:
  - MD5:
    - Computes 128-bit hash value.
    - Widely used for file integrity checking.
  - SHA-1:
    - Computes 160-bit hash value.
    - NIST approved message digest algorithm.
  - HAVAL:
    - Computes between 128 and 256 bit hash in between 3 and 5 rounds.
  - RIPEMD:
    - Developed in Europe published in 1996.
    - Patent-free.

Chapter 3: Infrastrucutre Security

Definition

- Protection of hardware, software networks, data centers and other essential components that constitute an organization’s information technology infrastructure.
- Ensuring the confidentiality, integrity, and avaliability of information and resources.
- Practice of protecting critical systems and assets aganist physical and cyber threats.
- Process of protecting the data from unauthorized access disclosure, destruction or disruption.

Technology assets

- Computers and endpoints/devices
- Networking systems
- Cloud resources

Key components of infrastructure security

- Physical security
- Network security
- Server security
- Data security
- Endpoint security
- Cloud security
- Incident response and Disaster recovery
- Security Policies and Training

Goals of Infrastructure Security

- Protect an organization’s Information Technology(IT) from a variety of threats and risks. (Primary goal)
- Boost security measures and your overall posture.
- Protect data from being stolen or otherwise compromised, minimizing financial risk incurred with steep fines.
- Ensure compliance with evolving data privacy rules that mandate consumer information be kept safe from attack.
- Minimize the risk of damage due to user carelessness.

- **Overarching objectives:**
  - Confidentiality of Information
  - Integrity of Systems and Data
  - Availability of Resources
  - Resilience Aganist Cyber Threats
  - Compliance with Regulations and Standards
  - Mitigation of Risks
  - Efficient Incident Response
  - Protection Aganist Unauthorized Access
  - Continous Monitoring and Improvement
  - User Awareness and Training

Levels of Infrastrucutre Security

- Physical level
- Network level
- Application level
- Data level

Host Security

- A host is any computer including workstations, network servers, laptops, wirelessly networked devices.
- **Activities:**
  - Protecting the physical devices.
  - Securing an operating system software.
  - Using software based software application.
  - Monitoring logs
- **Elements:**
  - Securing devices
    - Physical access security (hardware lock, deadbolt locks)
    - Hardware security
    - Mobile device security (Remote wipe/sanitation, GPS tracking and Voice encryption)
  - Network monitoring and diagnosis tools
    - Network Monitoring: a process in which all network components (Router, switch, firewall, servers and VM) are monitored.
    - Tools:
      - SNMP(simple network management protocol)
        - Widely used
        - Used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

    - Implemented on the application layer.
    - Components:
        - SNMP Manager: centeralized system that is used to monitor network.
        - SNMP Agent: specialized software run by Managed devices which collect data and store information about the device’s status and configuartion.
        - Management Information bases: consists of information on resources that are to be managed.
- Nagios core
    - Open-source monitoring software that enables organizations to monitor the availability and performance of their entire IT infrastructure.
    - Tracks performance events through the alerts system, which send out notifications by email and SMS.
    - It contains performance dashboard, alert system, avaliability reports, capacity planning, community-created plugins and APIs.
- Zabbix
    - Open-source network monitoring that combines network, server, cloud, application, service monitoring into one unified solution.
    - It uses SNMP and IPMP to monitor your network.
    - The Autodiscover feature automatically locates network devices and add them to be monitored.
    - It has a notification system in which alerts are sent by email, SMS, messenger, jabber, or custom scripts to update you on evolving network security events.
- Icinga
    - Open-source network monitoring tool that monitors the performance of your network, cloud-service, and data center.
    - Web based (supports both GUI and DSL).
    - It contains web based GUI, DSL configuration avaliable, Dashboard and Icinga modules/extensions.
- Datadog
- Paessler PRTG
- Atera
- ManageEngine opManager

Security of different media

- Media:
  - Print media
  - Broadcast media
  - Internet media
  - Out-of-home (outdoor) media
- Main memory (RAM) and Backing (secondary) storage device
- **Storage medium:** the device that actually holds the data.
- **Storage devices:** the device that save data onto the storage medium, or read data from it.

Intrusion Detection mechanism

- **Intrusion:** any set of action that attempt to compromise the confidentiality, integrity, or avaliability of a computer resource.
- **Intrusion detection:** detection of break-ins and break-in attempts via automated software systems. process of identifying and responding to malicious activities targeted at resources.
- **Intrusion detection system:** a system designed to test/analyze network system traffic/events against a given set of parameters and alert/capture data when these thresholds are met.
- Functions:
  - Detecting attacks as soon as possible
  - Take reactive measures than preventive mesaure when an attack is detected
  - It plays a role of information rather than a police officer
- Major components:
  - Central processing devices(control panel)
    - Alarm/notification devices
  - Audit data preprocessor
  - Detection engine
  - Decision engine
  - Detection models
  - Decision table

Detection methods in IDS

Signature based IDs	Anomaly base IDs
Signature: DB of known attack patterns	Profile: model of normal behaviors
IDS reports situation that match signatures	IDS reports situation that deviate from profile
Good”low false alarm rate, instantaneous detection	Good cat detect some new attacks
Bad: cannot detect new attacks	Bad: high false alarm rates, high complexity

Chapter 4: Managing communication and network security

Remote Access Technologies

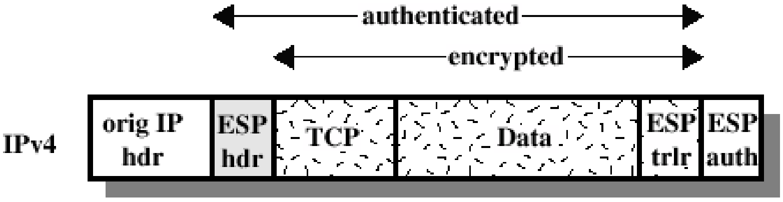
- Various methods and technologies that enable users to connect to computer sysystems or networks from a location other than the physical site.
- Uses:
  - Flexibility and Work-Life Balance
  - Increased Productivity
  - Global Collaboration
  - Cost Saving
  - Technology Advancements
  - Security and Compliance
  - Business Continuity
  - Employee Satisfaction and Retention
  - Challenges and Solutions
- Common technologies:
  - Virtual Private Network (VPN): establishes a secure and encrypted connection over the internet.
  - Remote Desktop Services (RDS): allows users to connect a desktop environment or specific application on a remote server.
  - Cloud-Based solutions
  - Secure Shell (SSH): cryptographic network protocol that provides a secure way to access and manage network devices remotely.
  - Mobile Device Management (MDM): allow organizations to manage and secure mobile devices remotely.
  - Web based remote access
  - Remote file access (File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP))
  - Remote Access Software

Network Security

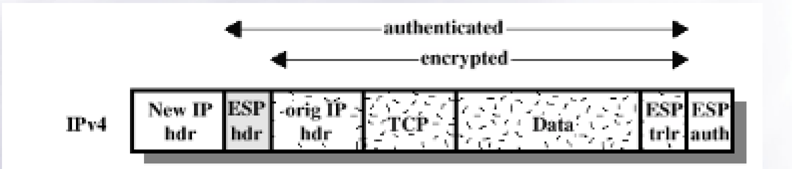
- Major concerns:
  - Confidentiality: only sender and intended receiver should “understand” message contents.
  - Authentication: sender and receiver want to confirm identity of each other.

    - Message integrity: sender and receiver want to ensure message not altered (in transit, or afterwards) without detection.
    - Access and avaliability: services must be accessible and avaliable to users.
- Types of attacks in network security:
    - Active:
        - Threatening the integrity and avaliability of data being transmitted.
        - Quite possible in TCP/IP
        - Examples:
            - Denial of Services (DoS):
                - `E-mail bombing` : flooding someone
                - `Smurf attack` : sending a “ping” multicast or broadcast with a spoofed IP of a victim.
            - Spoofing attack:
                - `IP spoofing` : putting wrong IP address in the source of an IP packet.
                - `DNS spoofing` : changing DNS info so that it directs to a wrong maching.
                - `URL spoofing (web phishing)`
                - `E-mail address spoofing`
                - `Session hijacking`
    - Passive:
        - Listening to a network and make a use of the information without altering iy.
        - Passive wiretapping and traffic analysis
        - Utilities such as EtherDetect and tcpdump used
- Protocols and Vulnerabilities:
    - IP Security (IPSec):
        - A set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.
        - Applications:
            - Secure branch office connectivity over the Internet
            - Secure remote access over the Internet
            - Establsihing extranet and intranet connectivity with partners
            - Enhancing electronic commerce security
        - Benefits:
            - Transparent to applications (below transport layer)
            - Provide security for individual users
        - It ensures:
            - A redirect message comes from the router to which the initial packet was sent
            - A routing update is not forged
            - A router or neighbor advertisement comes from an authorized router

        - Services:
            - `Network-layer secrecy` : data encryption in IP datagram
            - `Network-layer authentication` : destination host can authenticate source IP address.
            - `Two principal protocols` : Authentication Header (AH) protocol and Encapsulation Security Payload (ESP) protocol.
            - `Network-layer logical channel` : Security Association (SA)
    - Security Associations:
        - A one way relationship between a sender and a receiver that provides security services (authentication and confidentiality).
        - Modes:
            - `Transport mode` : protection of upper layer protocols (TCP, UDP).



            - `Tunnel mode` : protection of the entire IP packet.



    - IP-level authentication is provided by inserting an Authentication Header (AH) into the packets.

    - IP-level confidentiality is provided by inserting an Encapsulating Security Payload (ESP) header into the packets. An ESP header can also do the job of the AH header by providing authentication in addition to confidentiality.

    - Before ESP can be used, it is necessary for the two ends of a communication link to exchange the secret key that will be used for encryption. Similarly, AH needs an authentication key.

    - IPSec is a specification for the IP-level security features that are built into the IPv6 internet protocol. These security features can also be used with the IPv4 internet protocol.

    - IPSec is transparent to applications (functions below transport layer)

TCP SYNC attack

- A TCP SYN Flood attack seeks to exploit the TCP three-way handshake mechanism, which is foundational for establishing connections in TCP/IP networks. The handshake involves three steps:

  - A client sends a SYN (synchronize) message to a server, indicating a desire to establish a connection.
  - The server acknowledges this request by sending a SYN-ACK message back to the client.
  - The client responds with an ACK (acknowledgment), and the connection is officially established.
- In a TCP SYN Flood attack, the malicious entity sends a barrage of SYN requests to a target server but intentionally avoids sending the final ACK. This leaves the server waiting for a response that never comes, consuming resources for each of these half-open connections.

- **Impacts**:

  - Service Disruption: Legitimate users find it difficult or impossible to access the affected service.
  - Resource Strain: The server's resources, including memory and processing power, are consumed by the flood of bogus requests.
  - Potential System Failures: In extreme cases, the server might crash or malfunction due to the overwhelming number of half-open connections.
- **Mitigation techniques:**

  - Firewall and proxies server
  - SYN Cookies
  - Reducing SYN-RECEIVED Timer
  - Filtering
  - Increasing backlog
  - SYN cache

SSL/TLS protocols

- Widely deployed "real world" security protocol
- Provides transport layer security to any TCP-based application using SSL services.
- Provides security services like client and server authentication, data encryption.
- SSL is used extensively by web browsers to provide secure connections for transferring sensitive data. SSL-protected HTTP transfer uses port 443 (instead of port 80), and is identified with a special URL method - https.
- SSL, like most modern security protocols, is based on cryptography.
- When an SSL session is established, the server begins by announcing a public key to the client, no encryption is in use initially. Both parties (and any eavesdropper) can read this key. The client then transmits information to the server in a way that no one else could decode using the server's public key. Session key is then negotiated on and established between the server and the client to encrypt the rest of the session.

DNS spoofing

- Modifying or poisoning server so that it gives false information by mapping server IP to own (attacker's) IP address.

E-mail Security

- SMTP Limitations:
  - Executable files or other binary files.
  - “National language” characters.
  - Messages over a certain size.
  - ASCII to EBCDIC translation problems.
  - Lines longer than a certain length.
- **Pretty Good Privacy (PGP):**
  - Provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
  - Services:
    - Digital Signature
    - Message Encryption
    - Compression
    - E-mail Compatibility
    - Segmentation
  - How PGP works:
    - User A wants to send User B a private email.
    - User B generates a public and private key.
    - User B keeps the private key and sends back the public key.
    - User A encrypts their message using the public key.
    - User A sends the private encrypted message.
    - User B decrypts the message with the private key.
- **S/MIME:**
  - `MIME` is a techniques used to describes transfer of a multimedia including audio, video and pictures.
  - Functions:
    - Enveloped Data: encrypted content and encrypted session keys for recipients.
    - Signed Data: message digest encrypted with private key of “signer”.
    - Clear-Signed Data: signed but not encryoted.
    - Signed and Enveloped Data: various orderings for encrypting and signing.

PGP	S/MIME
designed for processing the plain texts	designed to process email as well as many multimedia files
cheap	expensive
good for persnal use	good for industry use
less efficient	more efficient
depends on user key exchange	it relies on a hierarchically valid certificate for key exchange

PGP	S/MIME
contains 4096 public keys	only 1024 public keys
standard for strong encryption	the standard for strong encryption but it has some drawbacks
doesn’t provide authentication	provides authentication

Web threats and countermeasures

Threats	Countermeasures
Integrity (data modification)	Cryptographic checksums
Confidentiality (Eavesdropping, access to information about the client and network configuration)	Encryption
Denial of Service (DDoS, killing user thread and machine flooding)	Detection and action
Authentication (Impresonation and Data forgery)	Cryptographic techniques

Web Security

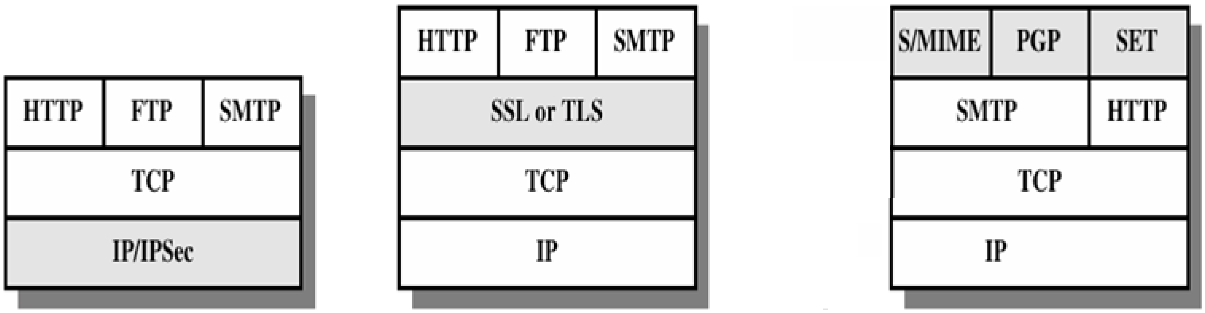
- **Secure Electronic Transactions (SET):**
  - An open ecnryption and security specification.
  - Set of security protocols and formats.
  - Protect credit card transaction on the Internet (Not a payment system).
  - Enables users to employ existing credit card payment infrastructure.
  - Key features:
    - Confidentiality of information
    - Integrity of data
    - Cardholder account authentication
    - Merchant authentication
  - SET participants:
    - Cardholder: authorized holder of payment card.
    - Merchant: Has goods to sell to the cardholder.
    - Issuer: financial institution (such as bank).
    - Acquirer: verifies that a card account is active and the proposed purchase doesn’t exceed the credit limit connected with the merchant.

        - Payment gateway: operated by the aquirer or a designated third party that process merchant payment messages.
        - Certification Authority: trusted entity to issue the X.509V3 public key certificate for card holders, Merchants and payment gateways (the success of SET depends on CA).
    - Sequence of events for transactions:

        i. The customer opens an account.
        ii. The customer receives a certificate.
        iii. Merchants have their own certificates.
        iv. The customer places an order.
        v. The merchant is verified.
        vi. The order and payment are sent.
        vii. The merchant request payment authorization.
        viii. The merchant confirm the order.
        ix. The merchant provides the goods or service.
        x. The merchant requests payments
- Dual Signature: linking two messages that are intended for two different recipients.

Security features in TCP/IP protocol stack

- **Network Level:**
    - Transparent to applications
    - Provide general purpose solution
    - Provides filtering capability
    - Example: IPSec
- **Transport Level:**
    - Alternatively, can be embedded into applications
    - Exmaples: SSL and TLS
- **Application level:**
    - Embedded within specific application
    - Examples: SET, HTTP, S/MIME, PGP and SMTP.



(a) Network Level (b) Transport Level (c) Application Level

Security enhanced application protocols

- FTPS, HTTPS, SMTPS and DNSSEC

Directory security concern

- **Directory**: a location for storing files on a computer.
- **Directory security**: involves controlling access to directories or folders on a computer system. It can also be expressed as ensuring that only authorized users or processes can view, modify or execute the contents of a directory.
- Common security mechanisms:
  - `File System permissions` : sepcify what actions can be performed by the owner, the group, and others.
  - Read, Write and Execute permissions
  - User groups
  - Access Control Lists (ACLs)
  - Ownership
  - Group memberships and inheritance
  - Security Contexts (Linux and SELinux)
  - Encryption and authentication
  - Logging and auditing

Chapter 5: Security Policies

Definition

- Set of guidelines, rules, and practices put in place by an organization to ensure the `confidentiality` , `integrity` , and `availability` of its information assets. These policies help define the framework for managing and safeguarding sensitive information, technology systems, and resources.

Components and Considerations for security policies

- Access Control Policies
- Data Classification and Handling
- Network Security Policies
- Endpoint Security Policies
- Incident Response and Reporting
- Physical Security Policies
- Password and Authentication Policies
- Security Awareness and Training
- Data Backup and Recovery
- Remote Access Policies

- Compliance Policies
- Vendor and Third-Party Security

Access Control Policies

- Fundamental aspect of information security, ensuring that only authorized individuals or systems have access to specific resources or data.
- A set of rules and guidelines that define how access to these resources is `granted`, `managed`, and `monitored` within an organization.
- Defines `who has access` `to what resources`.
- Specifies `user roles and permissions`.
- Enforce the `principle of least privilege (PoLP)`:
  - Users should be given the minimum level of access or permissions necessary to perform their job functions.
  - Reduces the potential impact of accidental or intentional misuse of privileges.

Access Control Types

- **Mandatory Access Control (MAC)**:
  - Based on security labels and predefined rules.
  - Commonly used in government and military environments.
- **Discretionary Access Control (DAC)**:
  - Owner determines access permissions.
  - Common in most business environments.
- **Role-Based Access Control (RBAC)**:
  - Access is based on job roles.
  - Simplifies administration and enhances security.

Access Control Models

- **Rule-Based Access Control (RBAC)**:
  - Type of access control model where access decisions are based on `a set of predefined rules`.
  - Permissions are associated with `roles`, and users are assigned to specific roles based on their job responsibilities.
  - This approach simplifies the management of access rights and enhances security by ensuring that individuals only have the permissions necessary for their roles.
- **Attribute-Based Access Control (ABAC)**:
  - An access control model that determines access permissions based on `attributes associated with the user`, `the resource being accessed`, and the `environment`.
  - Unlike traditional access control models that rely on predefined roles, ABAC allows for more dynamic and context-aware access control decisions.
  - In ABAC, access is granted or denied based on evaluating the attributes against a set of policies.

Key Concepts and Features of ABAC

- **Attributes**:
  - Characteristics associated with entities such as users, resources, and the environment.
  - User attributes include `role`, `department`, and `clearance level`.
  - Resource attributes include `sensitivity level`, `location`, and `type`.
- **Policies**:
  - Rules or conditions that define access control decisions based attribute values.
  - Involve combinations of attributes and specify when access should be granted or denied.
- **Subject, Action, Resource, and Environment (SARE)**:
  - ABAC typically revolves around the concept of `Subject (user)`, `Action (operation)`, `Resource (object)`, and `Environment (context)`.
  - Policies are defined based on the values of attributes associated with these elements.
- **Dynamic Access Control**:
  - ABAC allows for dynamic and context-aware access control decisions.
  - Access decisions can take into account various attributes and their values at the time of the access request.
- **Attributes and Relationships**:
  - Relationships between entities can be considered when making access decisions.
  - For example, a manager attribute may have a relationship with the employees reporting to that manager.
- **Scalability**:
  - ABAC is scalable and adaptable to changing organizational structures and requirements.
  - New attributes can be added without the need for significant restructuring.

Data Classification and Handling Security Policy

- A set of guidelines and procedures that define how an organization `classifies`, `labels`, `protects`, and `handles` different types of data based on its `sensitivity`, `criticality`, and `regulatory requirements`.
- Essential for safeguarding sensitive information, ensuring compliance with relevant regulations, and mitigating the risk of data breaches.
- Specify how different types of data should be `handled`, `stored`, and `transmitted`.

Network Security Policies

- Define rules for network access and usage.
- Specify the use of `firewalls`, `intrusion detection/prevention systems`, and other security measures.
- Establish guidelines for `secure network configurations`.

Endpoint Security Policies

- Specify security measures for `computers` , `mobile devices` , and other endpoints.
- Include guidelines for `antivirus software` , `encryption` , and `device management` .

Incident Response and Reporting

- Establish procedures for responding to security incidents.
- Define reporting mechanisms for reporting security breaches or suspicious activities.

Physical Security Policies

- Define measures to protect physical assets, such as servers and data centers.
- Specify access controls for physical spaces containing sensitive information.

Password and Authentication Policies

- Set guidelines for strong password creation and management.
- Define authentication methods, such as `multi-factor authentication (MFA)` .

Security Awareness and Training

- Outline programs for educating employees about security best practices.
- Emphasize the importance of recognizing and reporting security threats.

Vendor and Third-Party Security

- Establish criteria for selecting and evaluating third-party vendors based on security standards.
- Define expectations for security measures when working with external partners.

Compliance Policies

- Ensure that security policies align with relevant legal and regulatory requirements.
- Specify procedures for regular audits and compliance checks.

Remote Access Policies

- Define guidelines for secure remote access to organizational resources.
- Specify the use of `virtual private networks (VPNs)` and other `secure connectivity methods` .

Data Backup and Recovery

- Specify backup procedures to ensure data availability.
- Define recovery processes in case of data loss or system failures.