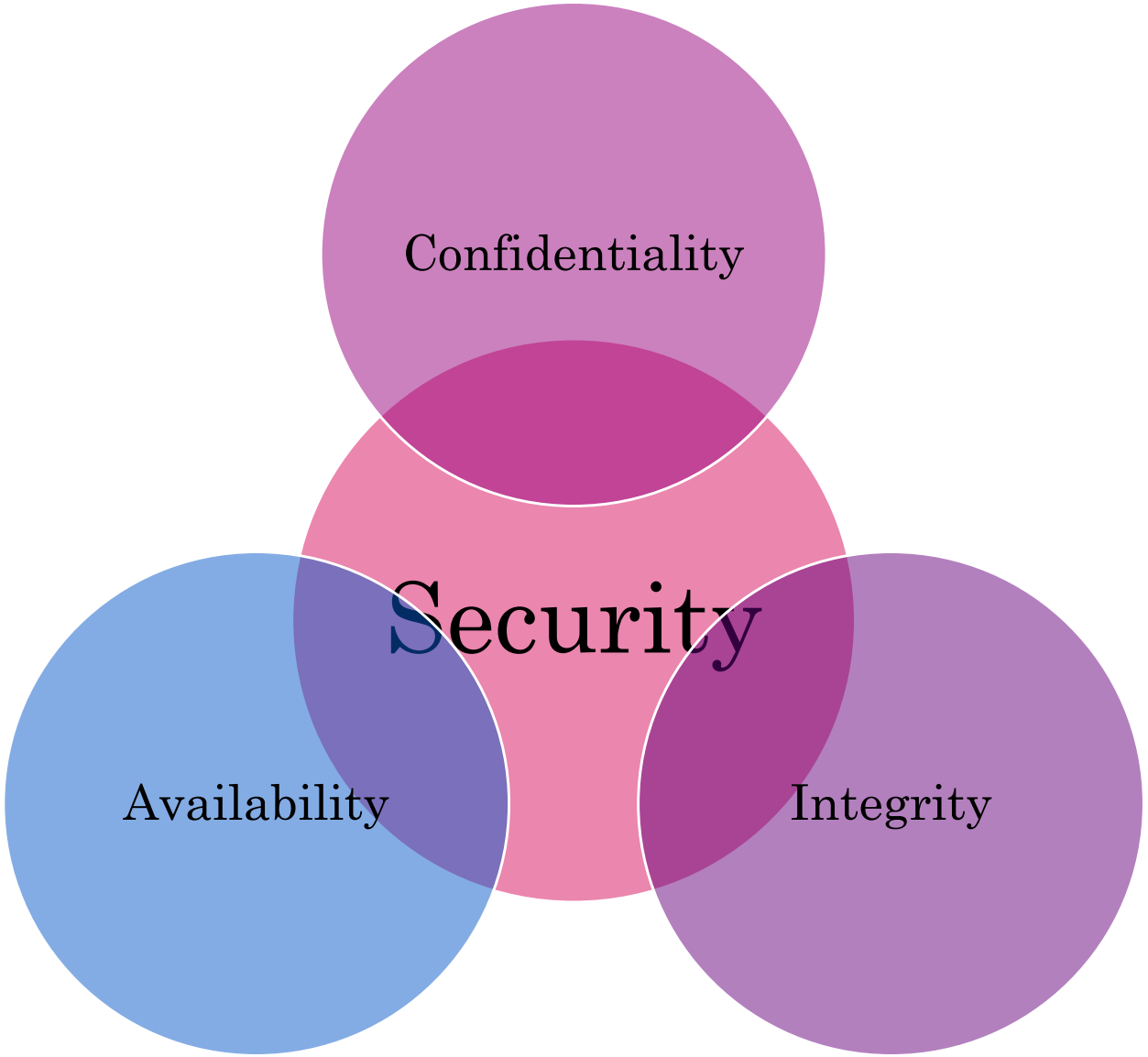
Network security

Chapter 07

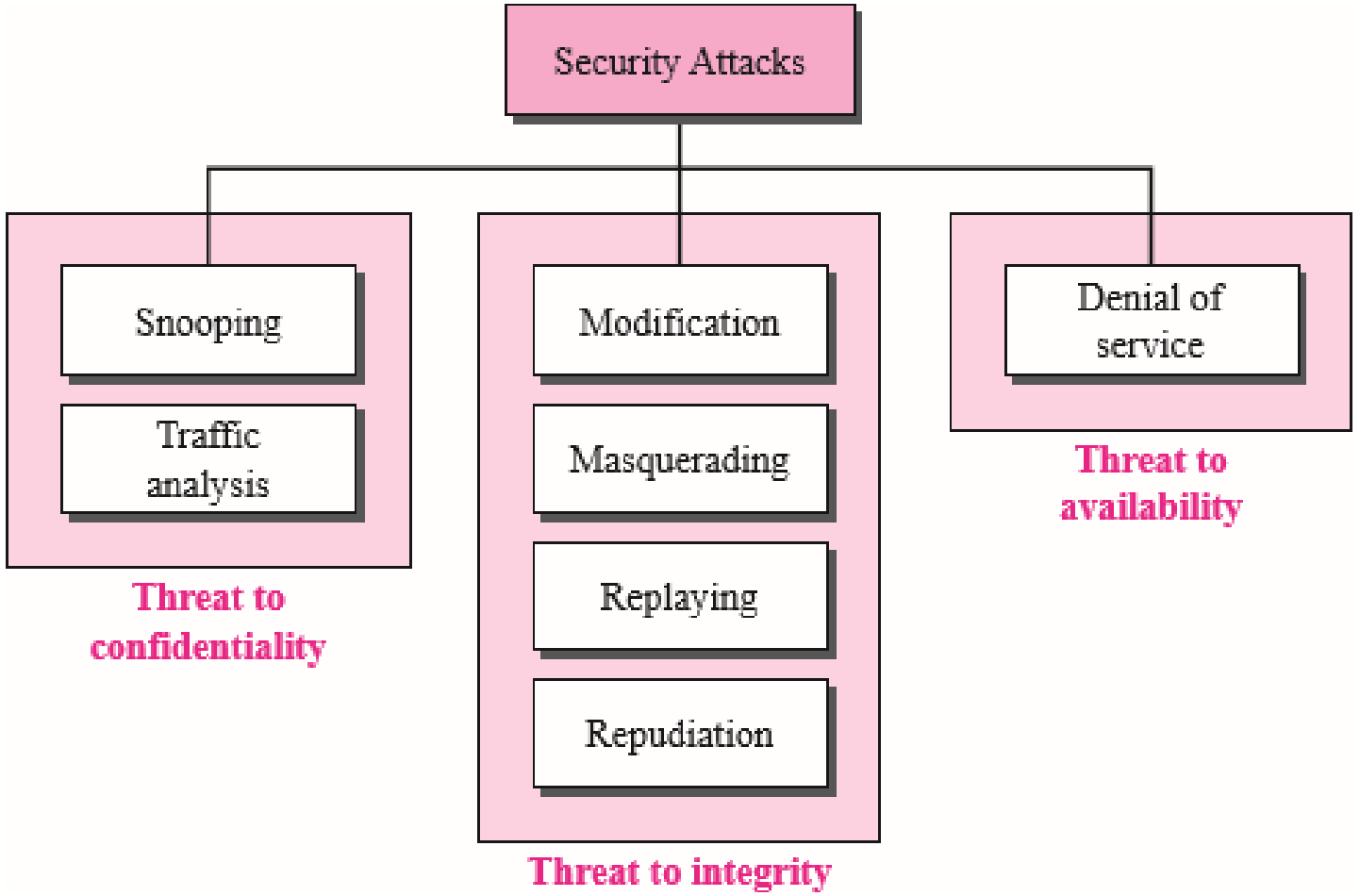
Contents

- Security Goals
- Cipher System
- Security Attacks
- Common System Attack
- Physical Protection
- Controlling Access
- Securing data
- Security protocols

Security Goals

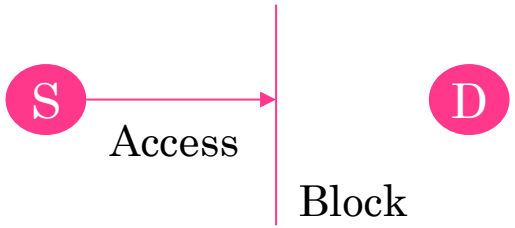


Security Attacks

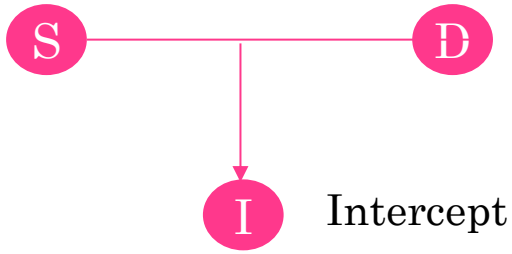


Security Attacks

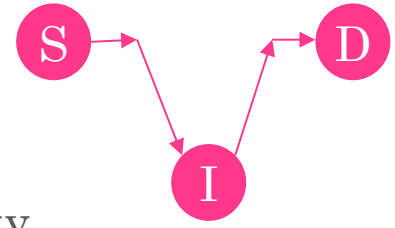
- **Attack**: Any action that compromises the security of information.
- Four **types of attack**:
  1. **Interruption**:
     Attack on Availability



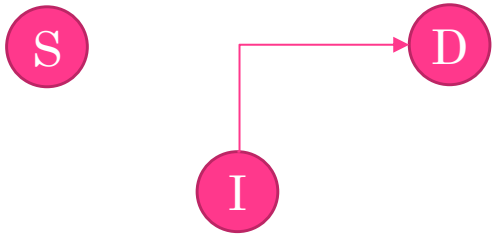
  2. Interception: Attack on Confidentiality



  3. Modification: Attack on Integrity



  4. Fabrication: Attack on Authenticity



Passive & Active Attacks

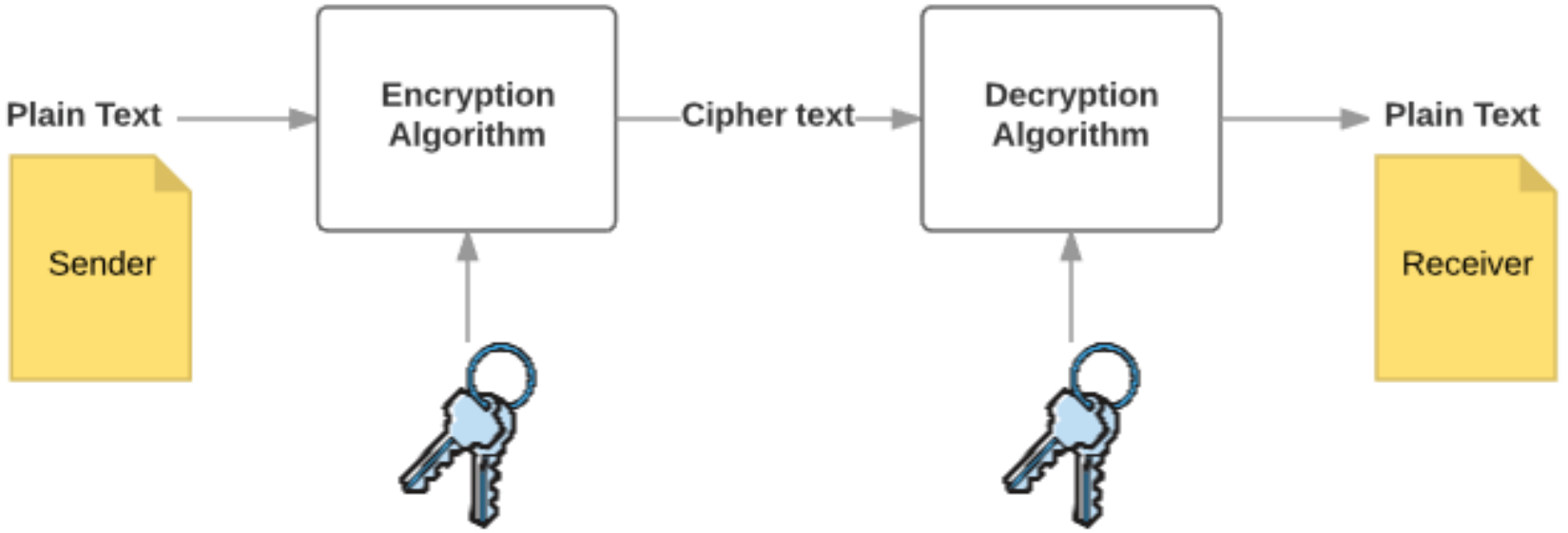
Passive

- Obtain information that is being transmitted (eavesdropping)
- Two types:
  - Release of message contents
  - Traffic analysis
- Very difficult to detect

Active

- Modify or create a false stream.
- Four categories:
  - Masquerade
  - Replay
  - Modification
  - Denial of services

Cipher System



- Symmetric Key Encryption: same keys are used for encrypting and decrypting (secret key cryptosystem). Primarily used for **privacy** and **confidentiality**
- Asymmetric Key Encryption: where different keys are used for encrypting and decrypting the information. Primarily used for **authentication**, **non-repudiation.**

Symmetric Key Cryptography

Features:

- Both parties must share a common key prior to exchange of information,
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome

Symmetric Key Cryptography

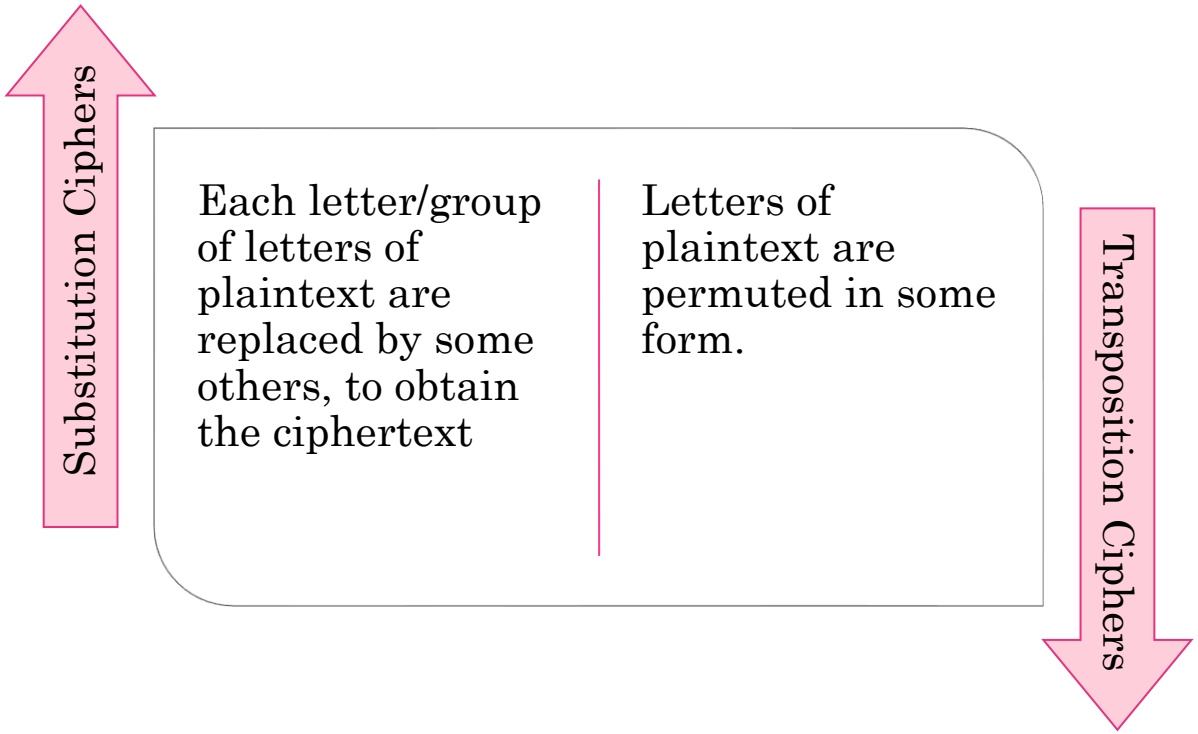
- In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) is smaller ➔ process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenges

- **Key establishment** – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other.

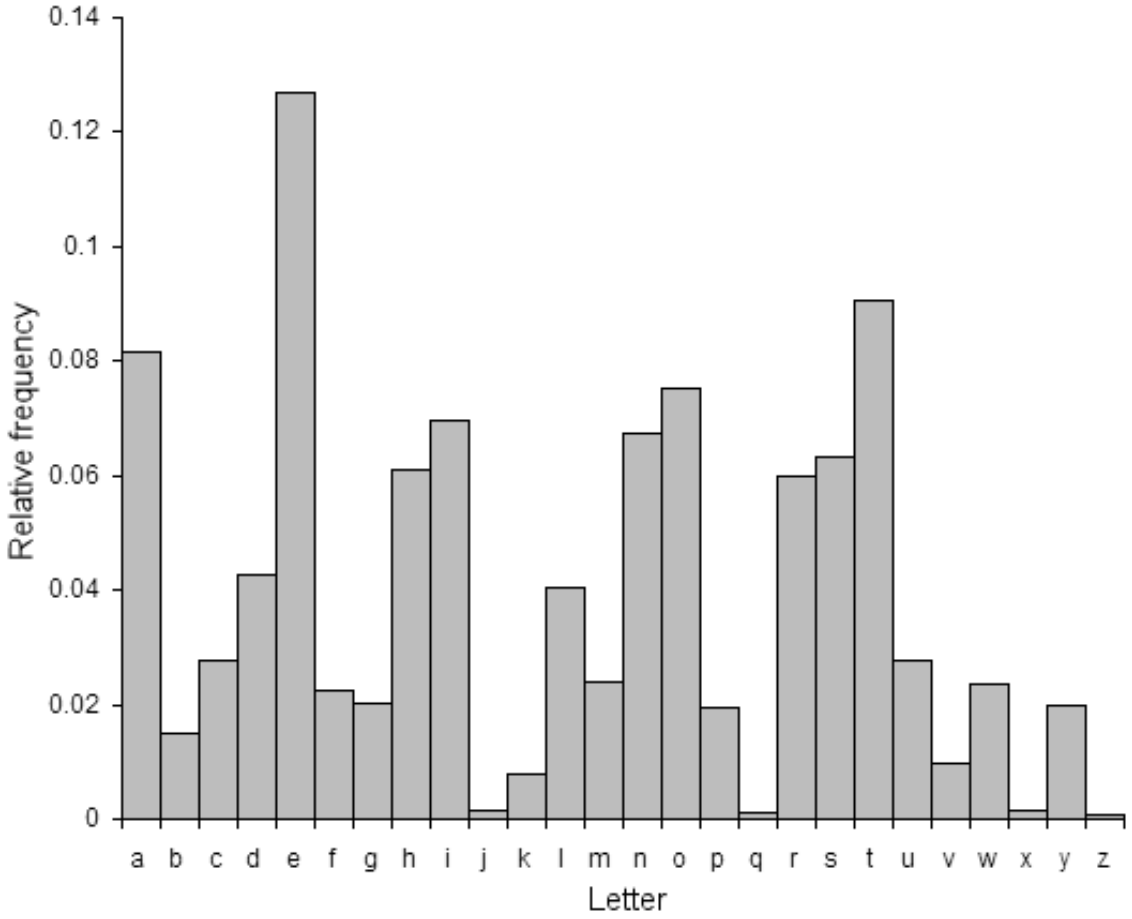
Traditional Ciphers

- **Based on symmetric key encryption** scheme.
- The only security service these systems provide is confidentiality.



Substitution Cipher

- All cryptographic algorithms involve substituting one thing for another.
- Caesar cipher: Taking each letter in the plaintext message and substituting the letter that is k letters later.
- For $k = 3$, the text “bob, i love you. alice” becomes “ere, l oryh brx. dolfh” in ciphertext.
- There are only 25 possible key values to break the code if one know that the Caesar cipher was being used.



A :	8.55	K :	0.81	U :	2.68
B :	1.60	L :	4.21	V :	1.06
C :	3.16	M :	2.53	W :	1.83
D :	3.87	N :	7.17	X :	0.19
E :	12.10	O :	7.47	Y :	1.72
F :	2.18	P :	2.07	Z :	0.11
G :	2.09	Q :	0.10		
H :	4.96	R :	6.33		
I :	7.33	S :	6.73		
J :	0.22	T :	8.94		

THE :	6.42	ON :	0.78	ARE :	0.47
OF :	2.76	WITH :	0.75	THIS :	0.42
AND :	2.75	HE :	0.75	I :	0.41
TO :	2.67	IT :	0.74	BUT :	0.40
A :	2.43	AS :	0.71	HAVE :	0.39
IN :	2.31	AT :	0.58	AN :	0.37
IS :	1.12	HIS :	0.55	HAS :	0.35
FOR :	1.01	BY :	0.51	NOT :	0.34
THAT :	0.92	BE :	0.48	THEY :	0.33
WAS :	0.88	FROM :	0.47	OR :	0.30

English letters frequency

Try to break this cipher

Ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf

Plaintext: ?

Substitution Cipher

- **Monoalphabetic**

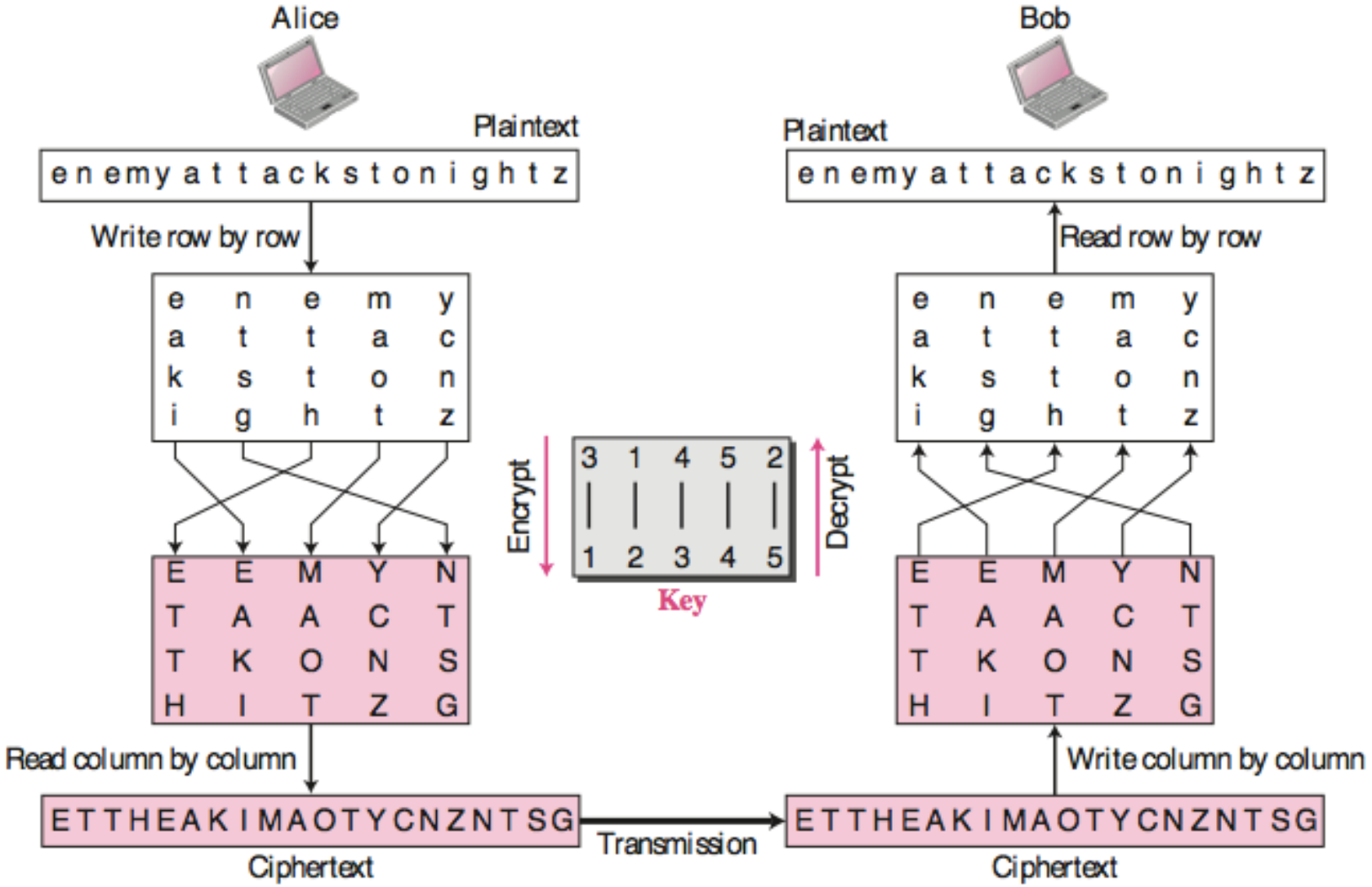
Plaintext letter:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext letter:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

- **Polyalphabetic**

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
$C_1(k = 5)$:	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
$C_2(k = 19)$:	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

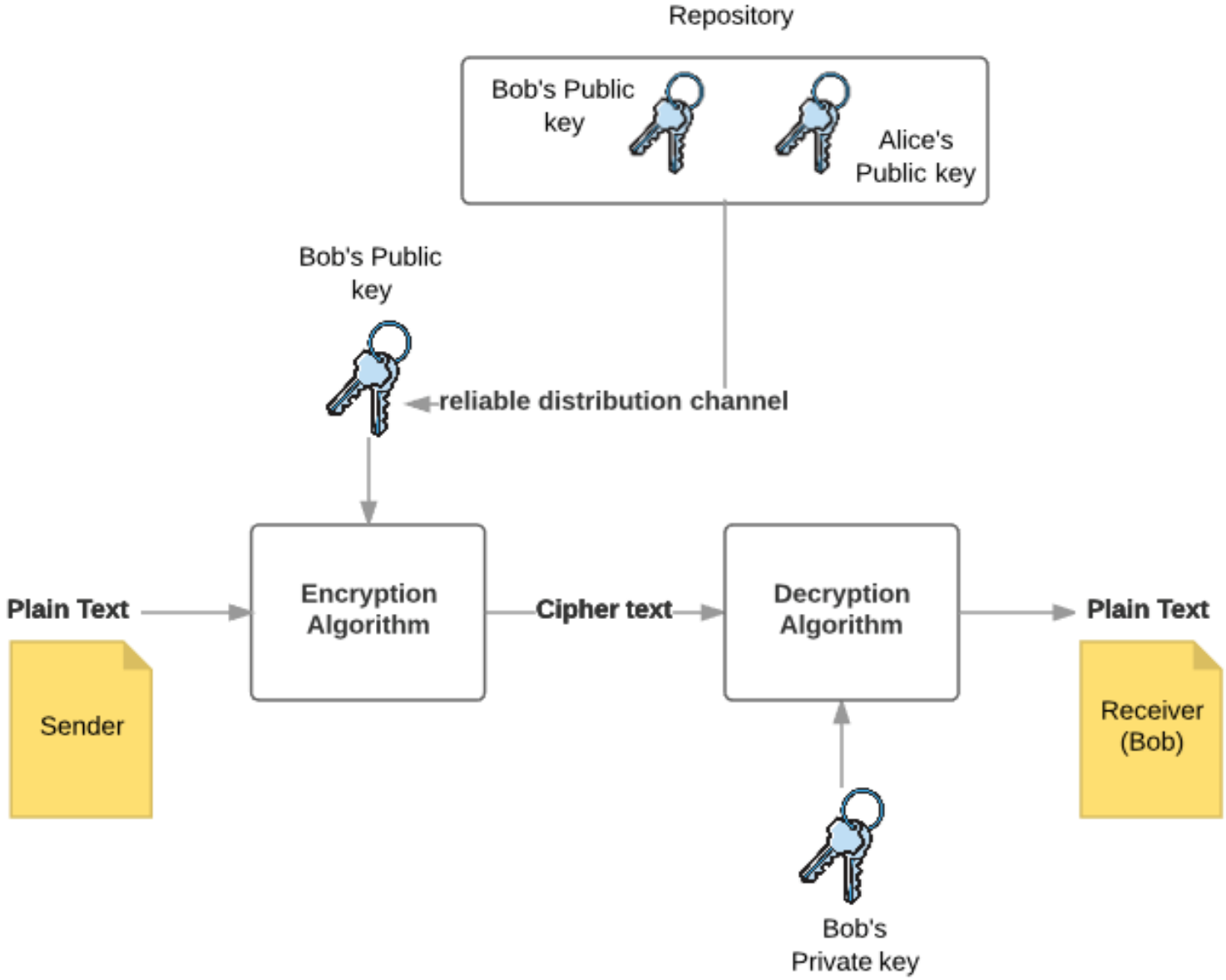
- These two Caesar ciphers, C1 and C2, can be used in the repeating pattern C1, C2, C2, C1, C2.

Transposition cipher



Asymmetric Key Encryption

- Invented in the 20th century to overcome the necessity of pre-shared secret key between communicating parties.



Asymmetric Key Encryption

- Every user needs to have a pair of dissimilar but mathematically related keys, **private key** and **public key**.
- One key is used for encryption, the other is for decryption.
- It requires to put the public key in public repository and the private key as a well-guarded secret → **Public Key Encryption**.

Asymmetric Key Encryption

- Though public and private keys are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- When *Alice* needs to send data to *Bob,* he obtains the public key of *Bob* from repository, encrypts the data, and transmits.
- *Bob* uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large →the process of encryption-decryption is slower than symmetric key encryption.

Challenges

- Public-key cryptosystems have one significant challenge – the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.
- This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party.

Common System Attack

1. Back door
2. Brute force
3. Buffer Overflow
4. Dos Attack (smurfing, Ping flood, SYN flood, TearDrop)
5. DDoS
6. Man-in-the-middle
7. Session Hijacking
8. Spoofing
9. Social Engineering
10. System bugs
11. Malicious software (Viruses, Trojan horses, worms, Other malwares, rootkits, keyloggers)

Physical Protection

- Causes of physical damage include fire, floods, earthquakes, power surges, and vandalism.
- Rooms containing computer equipment should always be **locked**, only allowed **authorized person**.
- **Cabling**, and the devices that cables plug into, **should not be left exposed**

Physical Protection

- To prevent electrical damage to computing equipment, high-quality surge protectors should be used.
- **Surveillance** may also be considered a form of physical protection - The placement of video cameras in key locations
- **Intrusion Detection** monitors data flow and system requests into and out of the systems. This is a growing field of study in network security
- A **honeypot** is a trap that is set by network personnel in order to detect unauthorized use of a network resource.

Controlling Access

- Controlling access to a computer network involves deciding and then limiting who can use the system and when the system can be used.
- Controlling Access Measures
  - Password & ID System
  - Access Rights
  - Auditing

Password & ID

- Typically, this password or ID is either a string of characters
  or
  a physical feature of a user, such as a fingerprint.
- Rules:
  - Change password often,
  - Use complex passwords
  - Do not share password with others

Password policy

Access rights

- Windows: NTFS Permissions, shared permission
- Linux: -rwxr-xr-x

Auditing

- Auditing a computer system is a good way to deter crime
- Be useful in apprehending a criminal after a crime has been committed
- Computer auditing usually involves having a software program that monitors every transaction within a system. As each transaction occurs, it is recorded into an electronic log along with the date, time, and "owner" of the transaction.
- Windows Event viewer
- Windows Security Auditing

Securing data

Properties of secure communication

1. **Confidentiality**: Only sender & receiver understand the contents of the transmitted message →Need to be **encrypted**.
2. **Integrity**: The content of communication is not altered (maliciously or accidentaly) in transit.
3. **End-Point authentication:** Both the sender and receiver should be able to confirm the identity of the other party.
4. **Operational security:** Firewall & IDS

Internet Security Protocols

1. Network Layer Protocols
2. Transport Layer Protocols
3. Application Layer Protocols

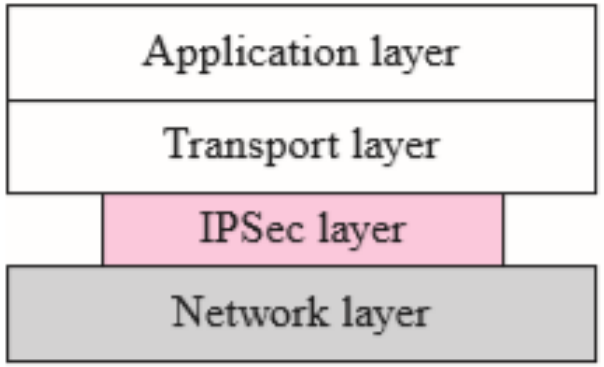
Network Layer Security

IP Security (IPSec)

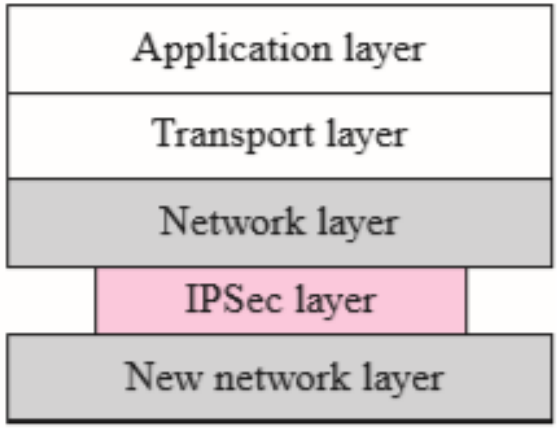
- IPSec is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level. IPSec helps create authenticated and confidential packets for the IP layer

IPSec Two Modes

- Transport mode: protects what is delivered from the transport layer to the network layer. It does not protect the IP header.

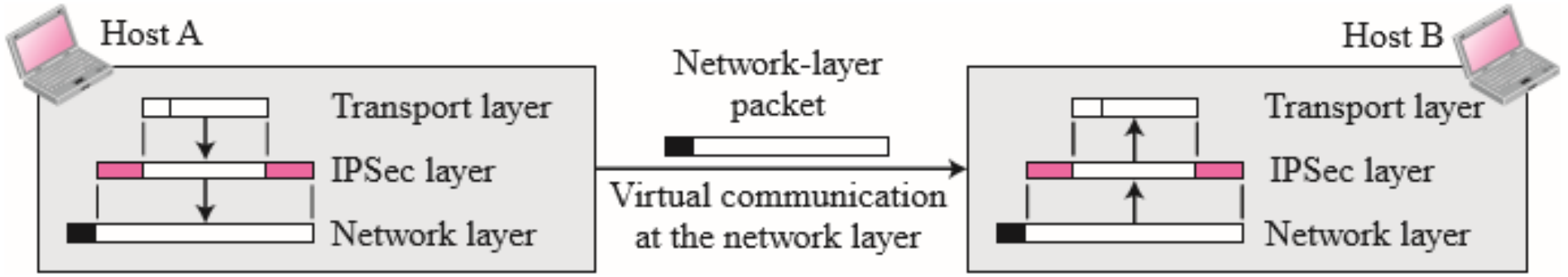


- Tunnel mode: protects the entire IP packet, including the header.



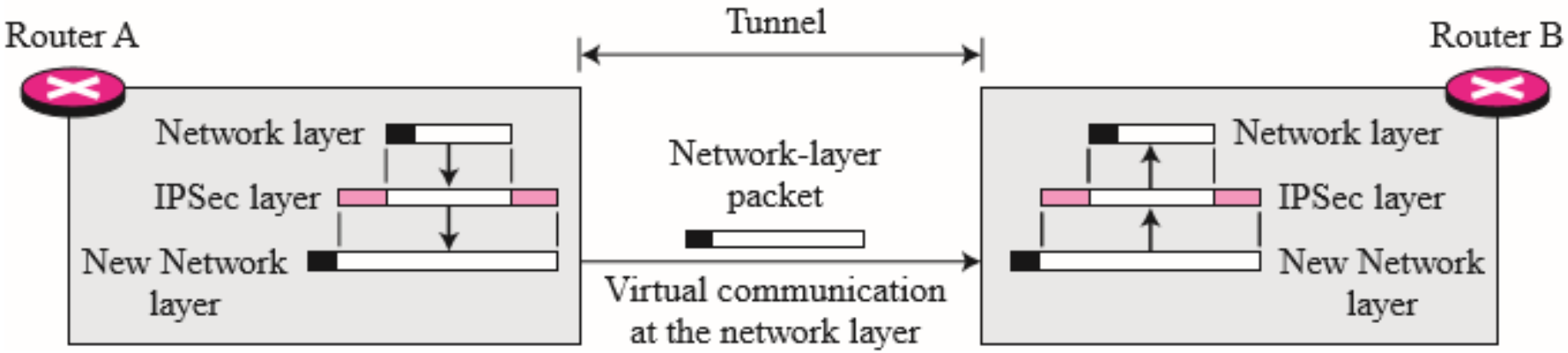
Transport mode

- Transport mode is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer. The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer.



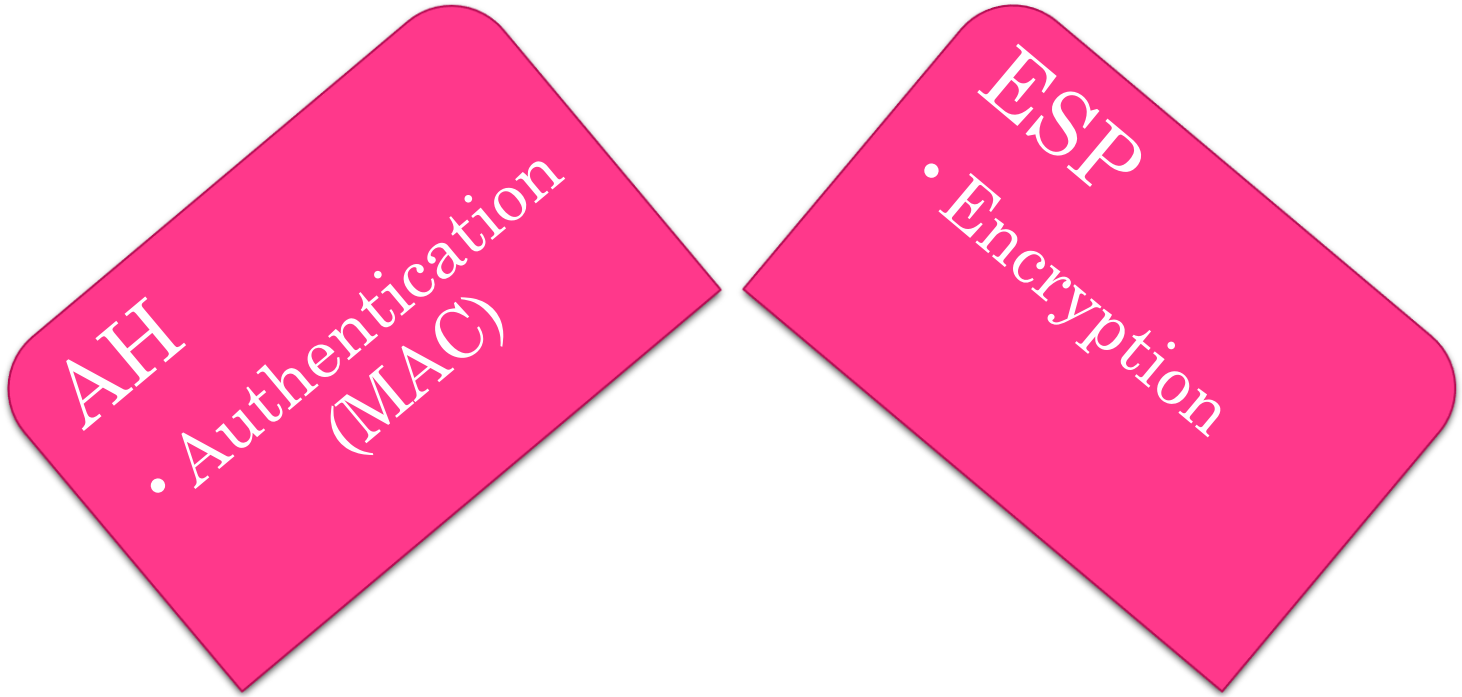
Tunnel mode

- Tunnel mode is normally used between two routers, between a host and a router, or between a router and a host. The entire original packet is protected from intrusion between the sender and the receiver, as if the whole packet goes through an imaginary tunnel



Two security protocols

IPSec defines two protocols:



Security Association

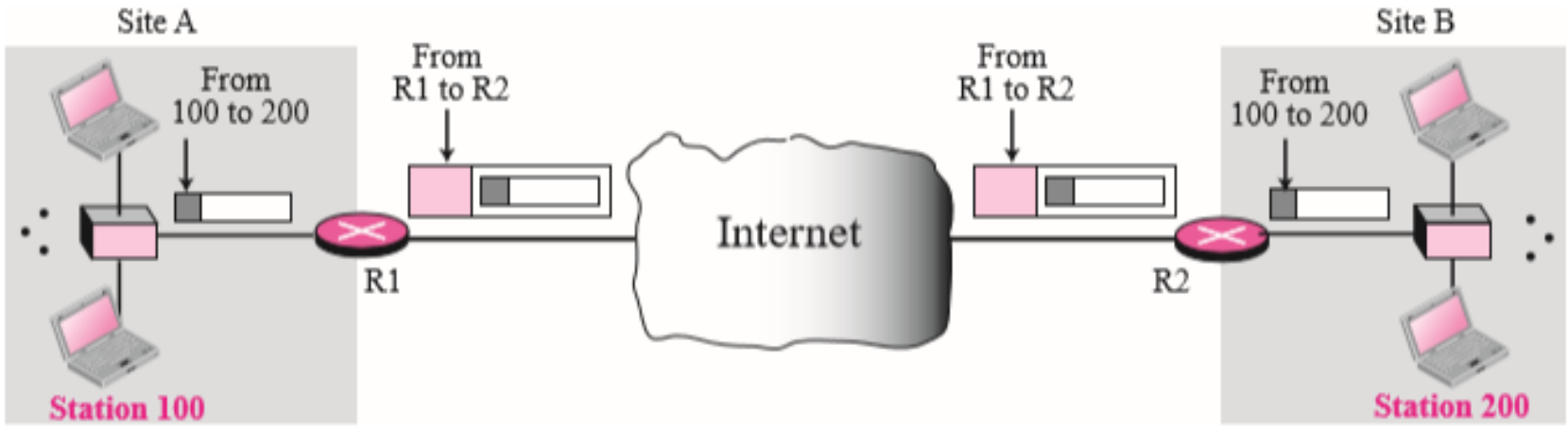
- Logical relationship between 2 hosts:
  - If confidentiality is concerned: the key used and the encryption /decryption algorithm
  - If Confidentiality, Authentication, Integrity is concerned:
    protocols used such as IPSec AH or IPSec ESP
- SA is the one-way relationship between a sender and a receiver, defined by IPSec parameters: One SA for inbound traffic, and one for outbound.
- SADB – Security Association Database
- SPI – Security Policy Index:
  - A unique index for each entry in the SADB
  - Identifies the SA associated with a packet

Internet Key Exchange

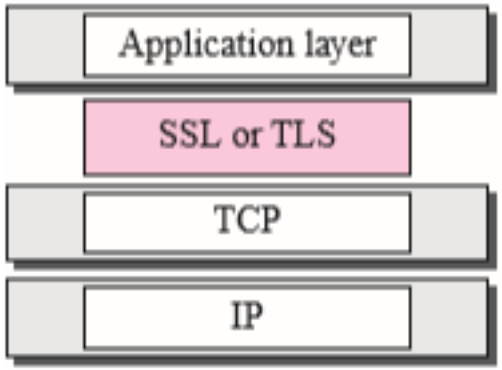
- A protocol designed to create both inbound and outbound Security Associations.
- When a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic. If there is no SA, IKE is called to establish one.
- **IKE creates SA for IPSec**
- **ISAKMP** is a protocol designed by the National Security Agency (NSA) that actually implements the exchanges defined in IKE

Virtual Private Network

- VPN Technology uses protocol ESP of IPSec in tunnel mode



Transport Layer Security



SSL Key principle and Techniques

Authentication: SSL/TLS authenticates the server using digital certificates. The client verifies the server's identity by:

- Checking the certificate's validity (expiry date, revocation status).
- Verifying the certificate's chain of trust (ensuring it's issued by a trusted CA).
- Checking the certificate's domain name against the domain name of the website. This prevents "man-in-the-middle" attacks where a malicious actor impersonates the server.

Encryption: SSL/TLS uses strong encryption algorithms (AES)

SSL Key principle and Techniques

- **Integrity:** The MAC (Message Authentication Code) Any modification to the data will result in an incorrect MAC, and the receiver will detect the tampering.
- **Confidentiality (using the Shared Secret):** Encryption of the data using a shared secret key, derived during the handshake.
- **Key Exchange Mechanisms :** The keys for each session are unique and based on temporary parameters exchanged during the handshake. This is a critical security enhancement.
- **Strong Cryptographic Algorithms:** robust cryptographic algorithms (e.g., AES-256 for encryption, SHA-256 for hashing)

Weakness and Attacks

- **Certificate Issues:** Problems with certificates (e.g., expired certificates, compromised private keys) can compromise the security of the connection.
- **Downgrade Attacks:** An attacker can try to force the client and server to use an older, weaker version of SSL/TLS or a less secure cipher suite.
- **Man-in-the-Middle Attacks:** While certificate validation aims to prevent these, attackers can still try to intercept the connection and impersonate the server.

Application Layer Security

E-mail Security

- Sending an e-mail is a one-time activity. The nature of this activity is different from IPSec or SSL, where the two parties create a session between themselves and exchange data in both directions.
- In e-mail, there is no session. Alice sends a message to Bob; sometime later, Bob reads the message and may or may not send a reply.
- The security here is unidirectional because what Alice sends to Bob is totally independent from what Bob sends to Alice

Cryptographic Algorithms

- The protocol defines a set of algorithms for each operation that the user used in his/her system.
- Alice includes the name (or identifiers) of the algorithms she has used in the e-mail. For example, Alice can choose DES for encryption/ decryption and MD5 for hashing. When Alice sends a message to Bob, she includes the corresponding identifiers for DES and MD5 in her message. Bob receives the message and extracts the identifiers first. He then knows which algorithm to use for decryption and which one for hashing

Cryptographic Secrets

- In e-mail security, the encryption/decryption is done using a symmetric-key algorithm, but the secret key to decrypt the message is encrypted with the public key of the receiver and is sent with the message
- **PGP (Pretty Good Privacy)** is the security protocol provided email with privacy, integrity and authentication.