Chapter 8
Network Security

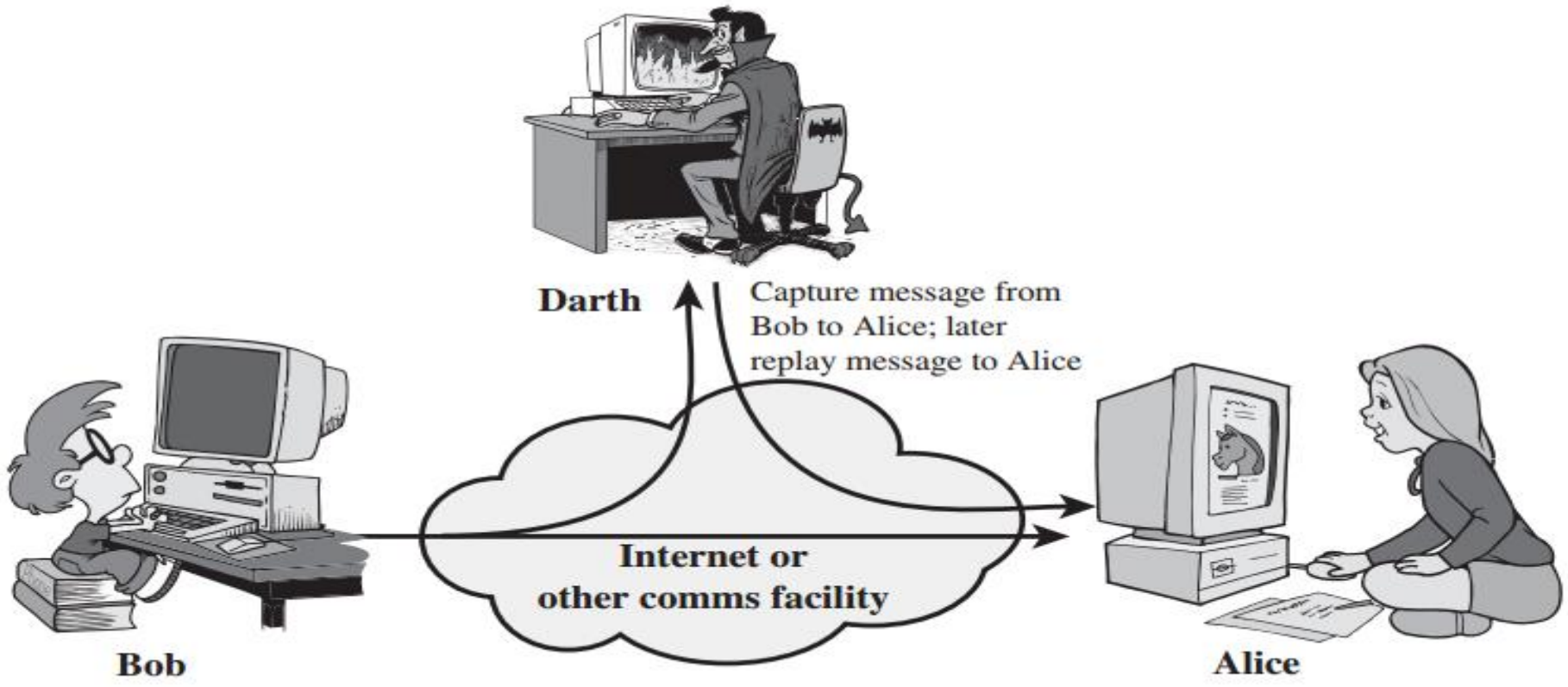
- ***Outline:***
  - 8.1 Properties of secure communication
  - 8.2 Principles of cryptography: Symmetric Key and Public Key
  - 8.3 RSA Algorithm,
  - 8.4 Digital Signatures
  - 8.5 Securing e-mail (PGP)
  - 8.6 Securing TCP connections (SSL)
  - 8.7 Network layer security (IPsec, VPN)
  - 8.8 Securing wireless LANs (WEP)
  - 8.9 Firewalls: Application Gateway and Packet Filtering, and IDS

Network Security

- Network Security is the protection of information and systems and hardware that use, store, and transmit that information.
- Network Security encompasses those steps that are **taken to ensure the confidentiality, integrity, and availability of data or resources.**
- ***Properties of secure Communication***
  - **Confidentiality:** Only sender, intended receiver should "understand" message contents. Sender encrypts message and receiver decrypts message.
  - **Authentication: S**ender, receiver want to confirm identity of each other.
  - **Message integrity**: Even if sender and receiver are able to authenticate each other, they must ensure that the data received is not altered either maliciously or by accident.
  - ***Non-repudiation:*** Sender cannot deny later that messages received were indeed sent.
  - ***Availability***: Services must be accessible and available to users upon demand.

Types of Security Attacks

- **Active attacks** involve some modification of the data stream or the creation of a false stream



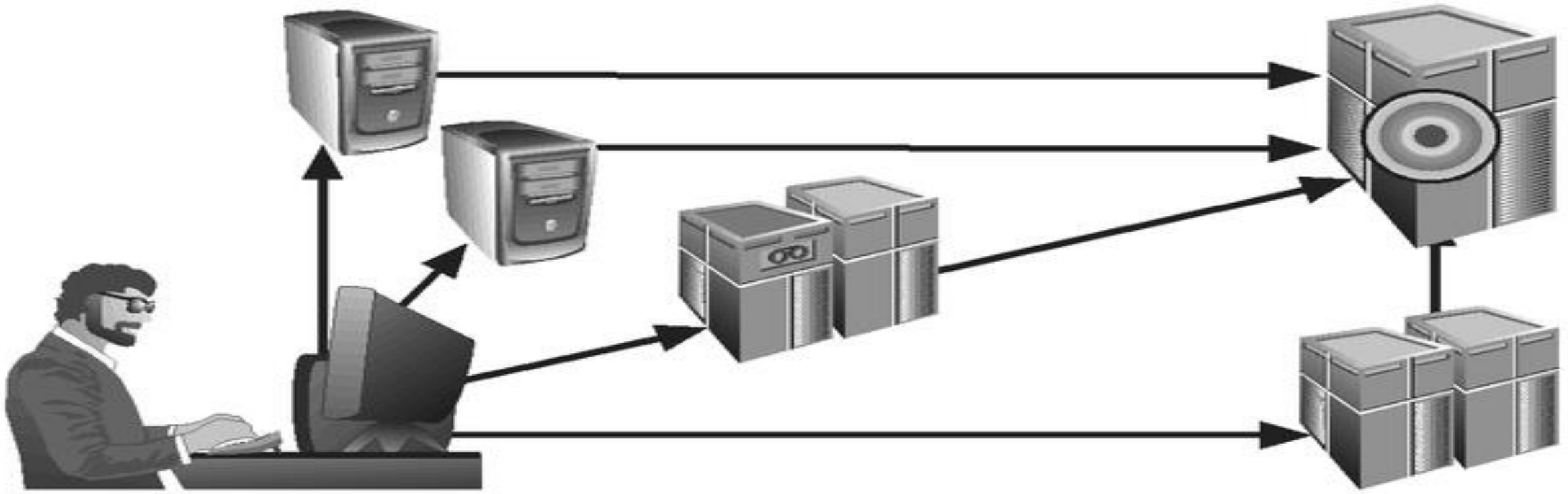
Active attacks

- **Masquerade**
  - Masquerade attack takes place when one entity pretends to be different entity.
- **Modification of messages**
  - It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. ***For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".***
- **Repudiation**
  - This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. ***For example, customer ask his Bank "To transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.***
- **Replay**
  - It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.
- **Denial of Service**
  - This attack may have a specific target. ***For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.***

Denial-of- Services Attacks

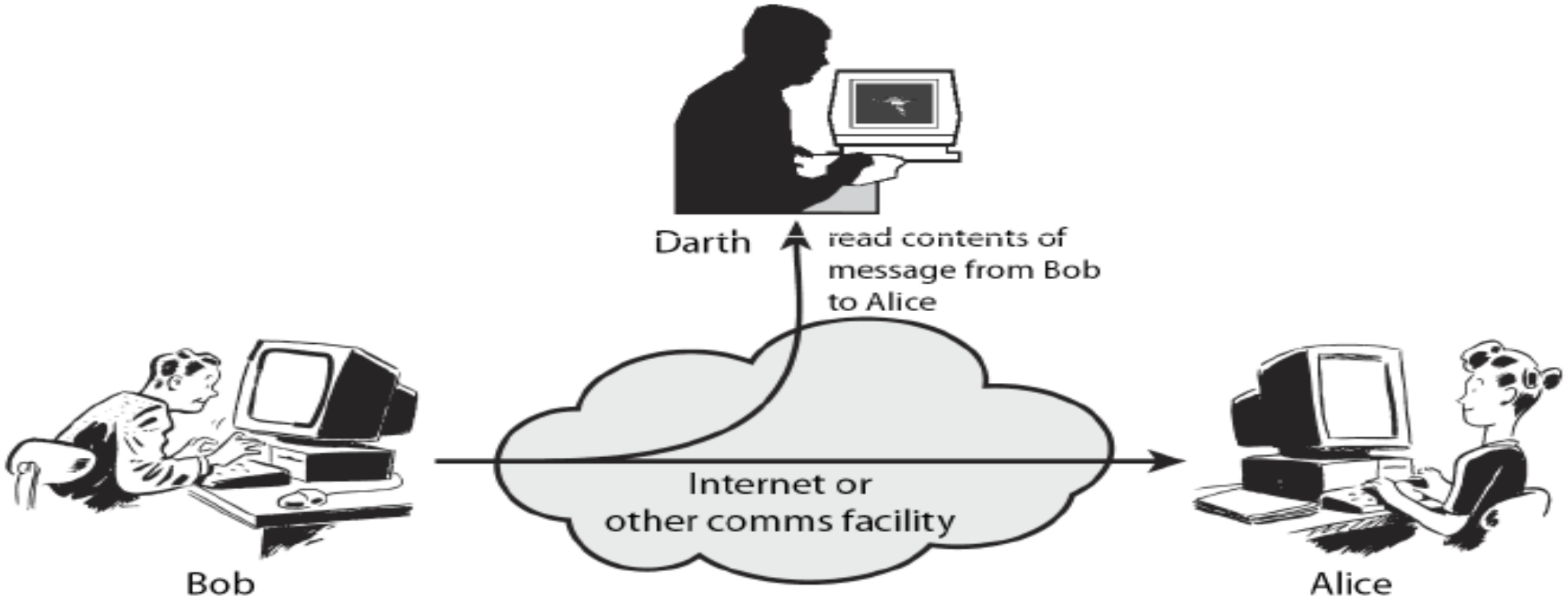
In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.



Types of Security Attacks

- A **passive attack** on a cryptosystem is one in which the cryptanalyst cannot interact with any of the parties involved, attempting to break the system solely based upon observed data (i.e. the ciphertext).

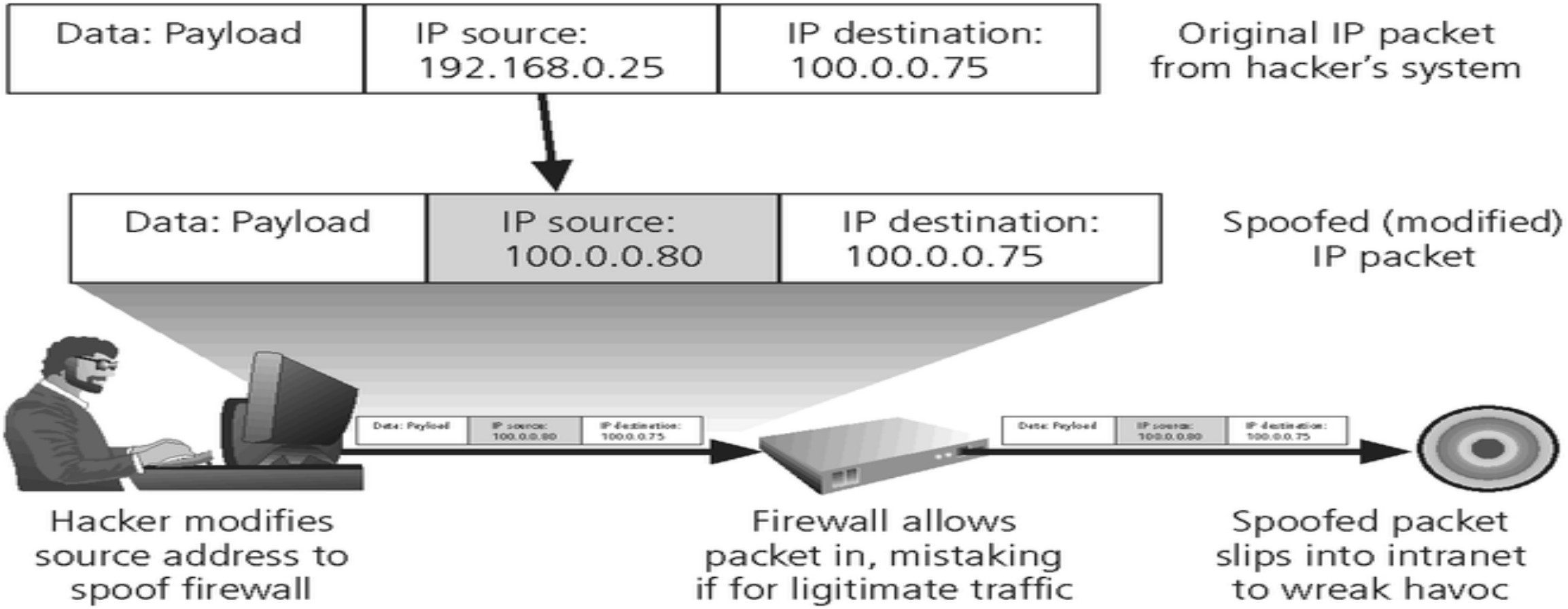


Passive attacks

- **The release of message content**
  - Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- **Traffic analysis**
  - Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
  - The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

IP Spoofing

- **IP spoofing:** a user can ***invent an IP packet containing any payload*** data he desires and make it appears as if it was sent from some other host.



Malicious Logic/Programs

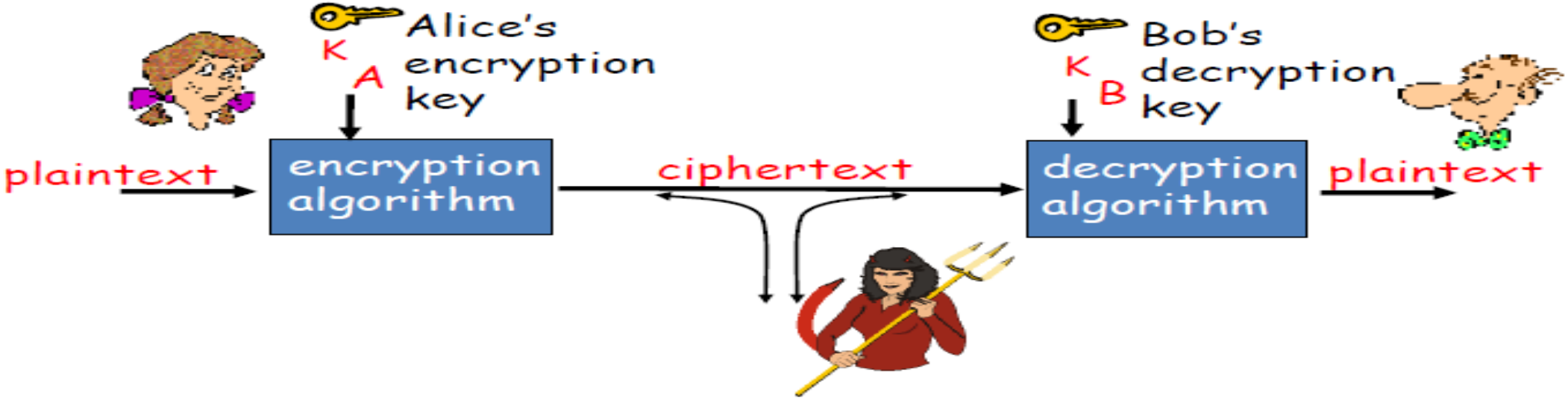
- **Viruses:** Rogue software program that attaches itself to other software programs or data files in order to be executed
- **Worms:** Independent computer programs that copy themselves from one computer to other computers over a network.
- **Trojan horses:** Software program that appears to be benign but then does something other than expected.
- **SQL injection attacks:** Hackers submit data to Web forms that exploits site's unprotected software and sends rogue SQL query to database.
- **Spyware:** Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising.
- **Key loggers:** Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks.

Cryptography

- **Cryptography** means "secret writing." The term to refer to the science and art of transforming messages to make them secure and immune to attacks.
- **Plaintext :** Original Message
- **Ciphertext :** Coded Message
- **Cipher :** encryption and decryption algorithms
- **Key :** Info Used in Cipher known only to Sender/ Receiver
- **Encipher (encrypt) :** Converting Plaintext to Ciphertext
- **Decipher (decrypt) :** Recovering Ciphertext from Plaintext
- **Cryptology :** Field of both Cryptography and Cryptanalysis
- **Cryptanalysis :** Code breaking or “Cracking the Code”
- An **encryption algorithm** transforms the **plaintext into ciphertext**; a **decryption algorithm** transforms the **ciphertext back into plaintext**. The **sender uses an encryption** algorithm, and the **receiver uses a decryption algorithm**.

Cryptography

- **Categories of cryptography**
  - In **symmetric key cryptography**, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.
  - In **asymmetric or public-key cryptography**, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.



Symmetry Key Cryptography: Caesar cipher

- In a **substitution cipher**, each letter or group of letters is replaced by another letter or group of letters to disguise it.
- One of the oldest known ciphers is the **Caesar cipher**, attributed to Julius Caesar.
- A slight **generalization of the Caesar cipher** allows the ciphertext alphabet to be **shifted by *k* letters**, **instead of always three**. In this case, ***k* becomes a key** to the general method of circularly shifted alphabets.
- The general system of symbol-for-symbol substitution is called a **monoalphabetic substitution cipher.**

```
plain:  abcdefghijklmnopqrstuvwxyz
cipher: bcdefghijklmnopqrstuvwxyza
```

Symmetry Key Cryptography: Polyalphabetic cipher

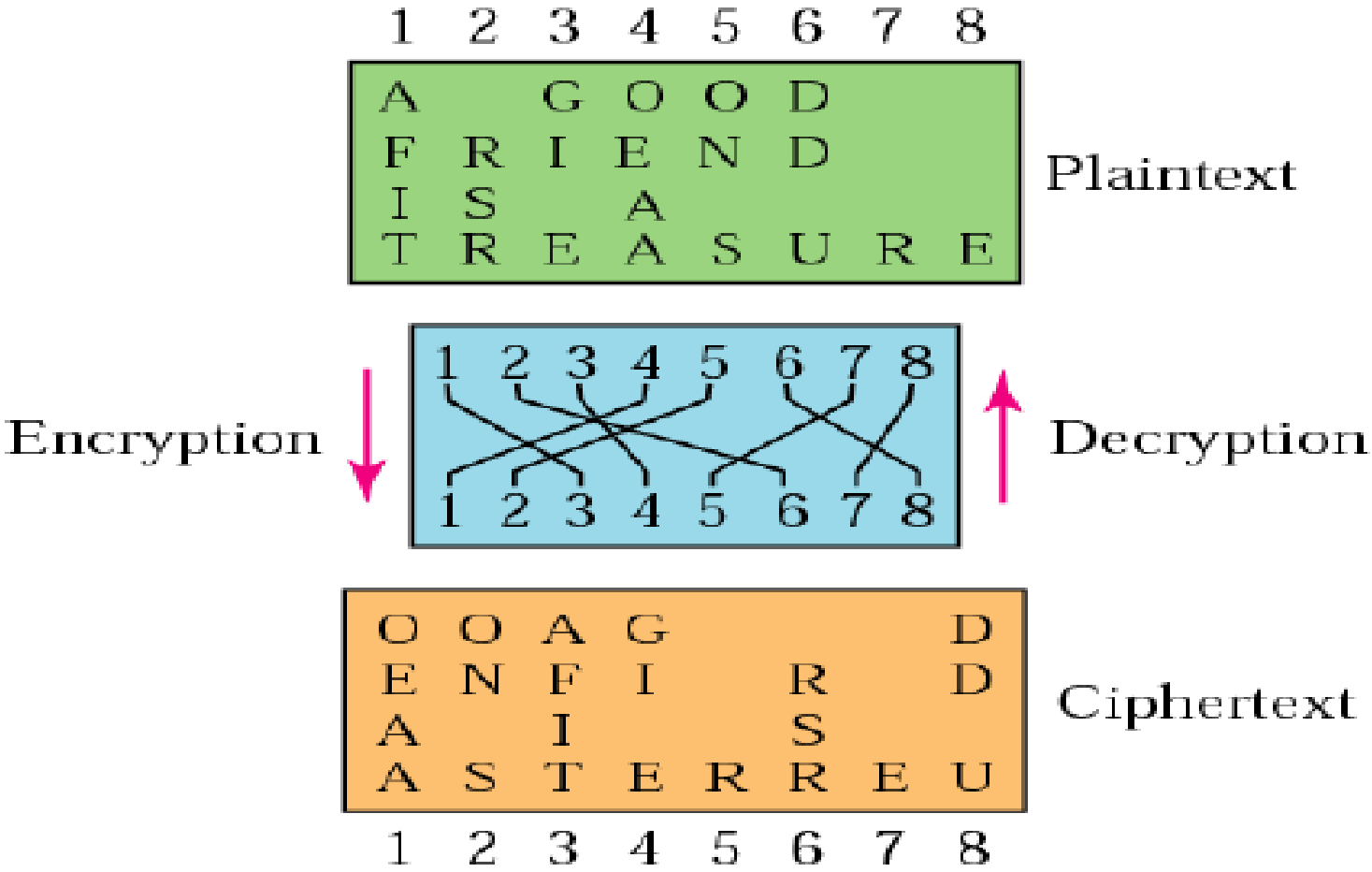
- In a **polyalphabetic cipher**, each occurrence of a character can have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is a **one-to-many relationship**.
- For example, character **A could** be changed to **D in the beginning** of the text, but it could be changed to **N at the middle**.

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

♦ A polyalphabetic cipher using two Caesar ciphers

Symmetry Key Cryptography: Transposition cipher

- **Transposition ciphers reorder** the letters but **do not disguise** them.



Symmetry Key Cryptography: DES

- **DES -** Data Encryption Standard.
- DES is the **block cipher** — an algorithm that takes a **fixed-length string** of plaintext bits and transforms it through a **series of complicated operations** into another **cipher text bit string of the same length**.
- In the case of DES, the **block size is 64 bits**.
- DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt.
- The key ostensibly **consists of 64 bits**; however, only **56 of these are actually used** by the algorithm. **Eight bits are used solely for checking parity**, and are thereafter discarded.
- Hence the effective **key length is 56 bits**, and it is always quoted as such. **Every 8th bit of the selected key is discarded**, that is, positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64 bit key leaving behind only the 56 bit key.

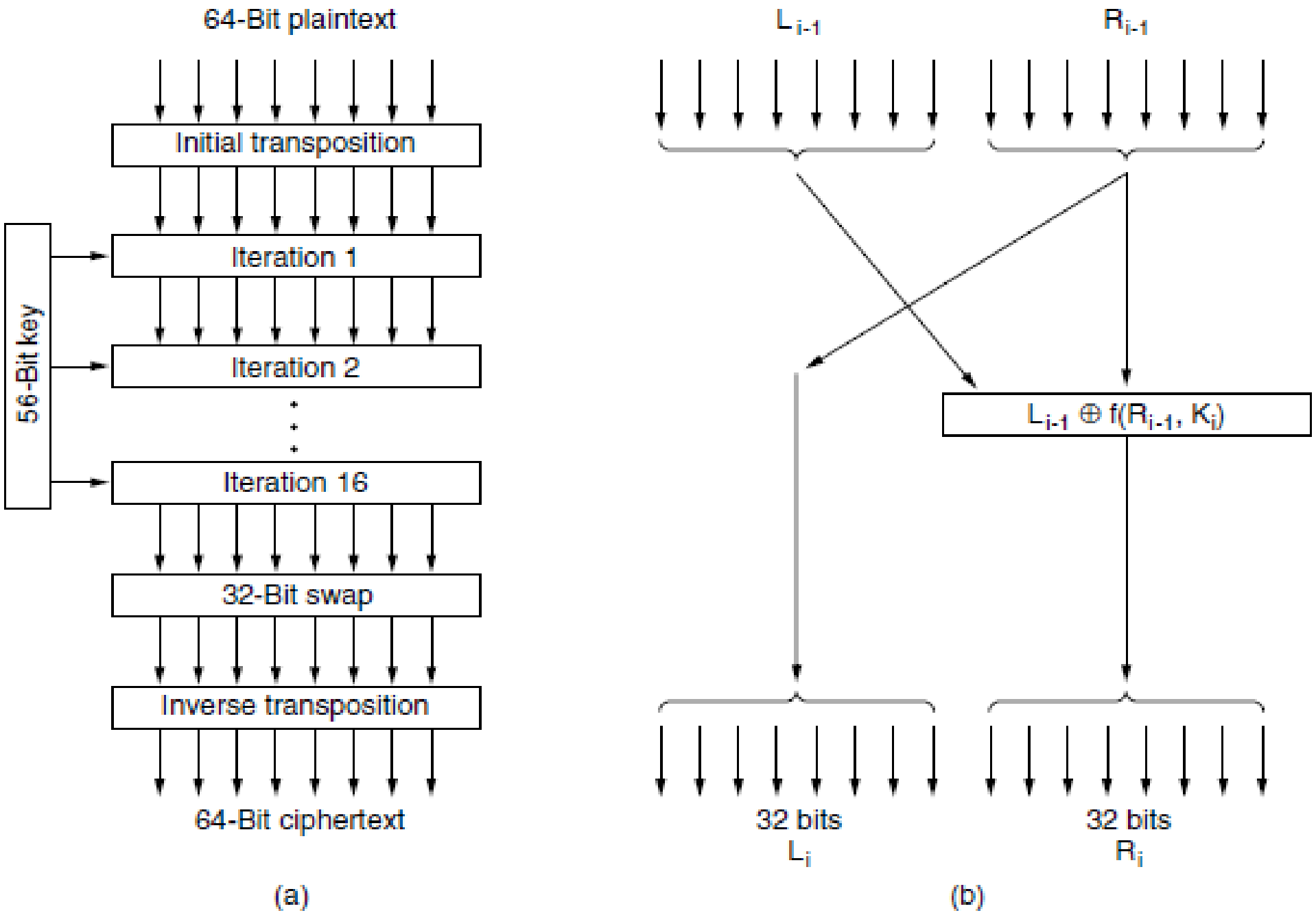
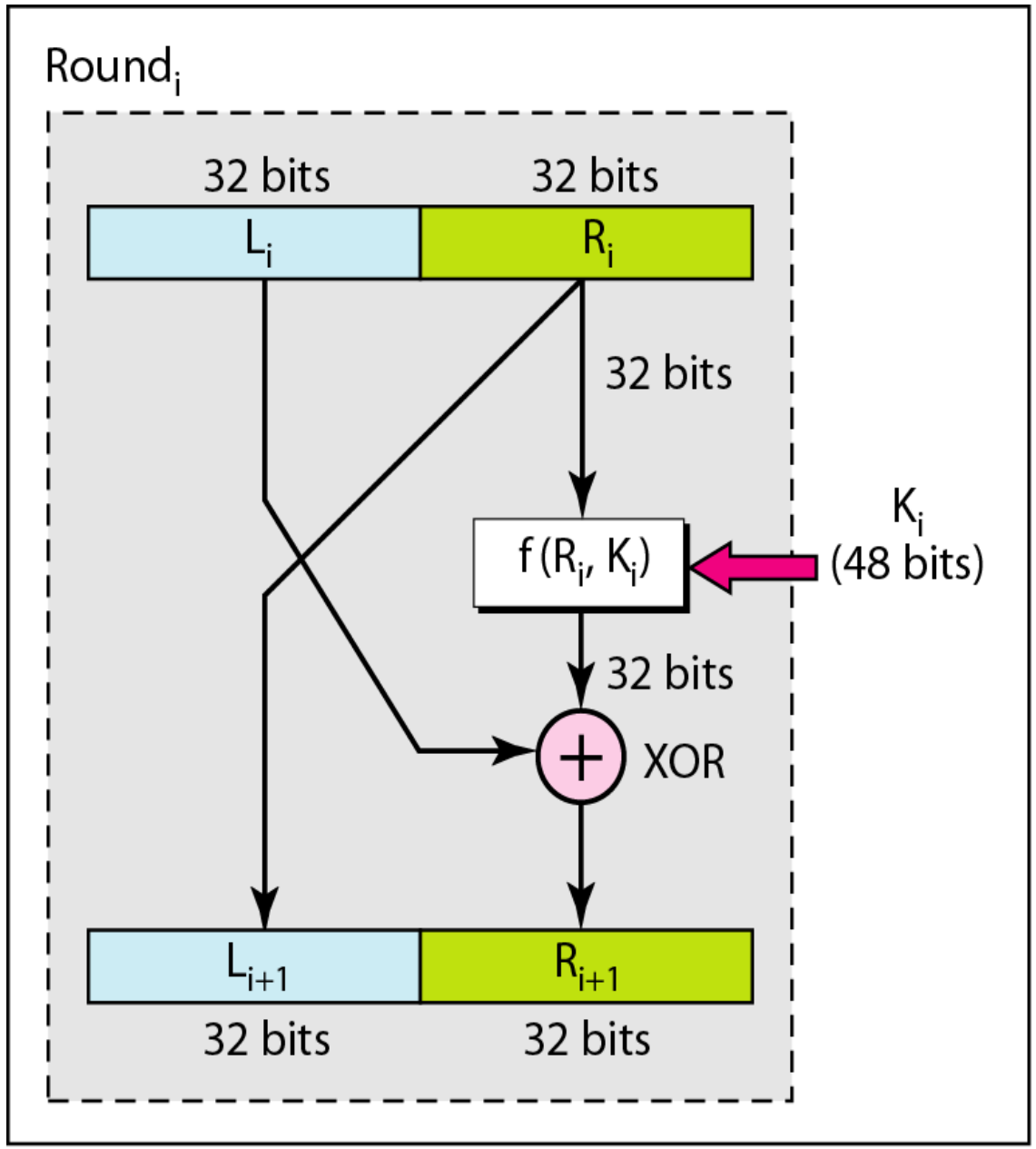
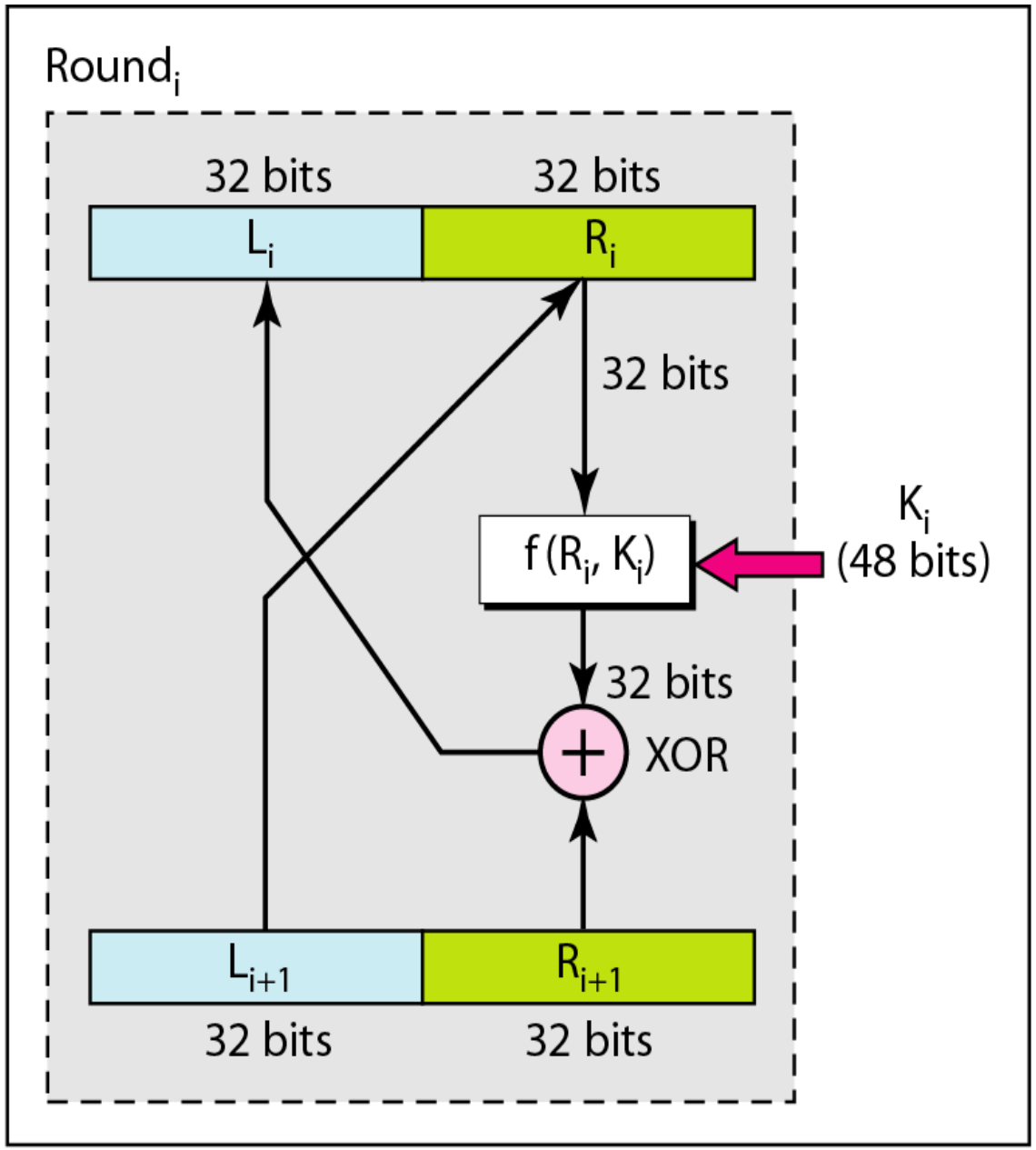


Figure : The Data Encryption Standard. (a) **General outline**. (b) **Detail of one iteration**. The circled + means exclusive OR.



a. Encryption round

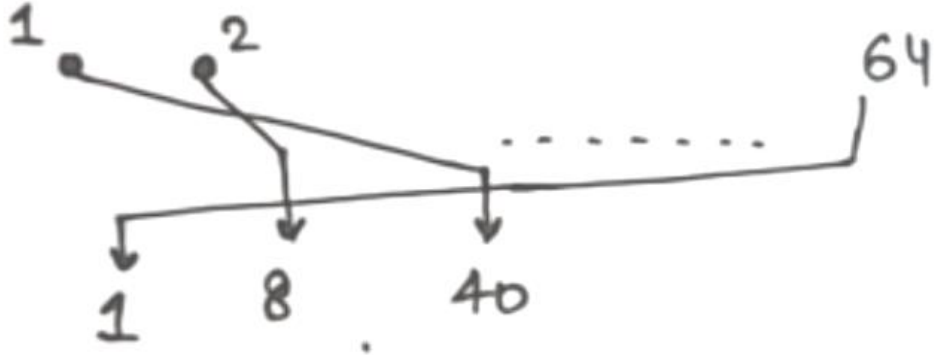


b. Decryption round

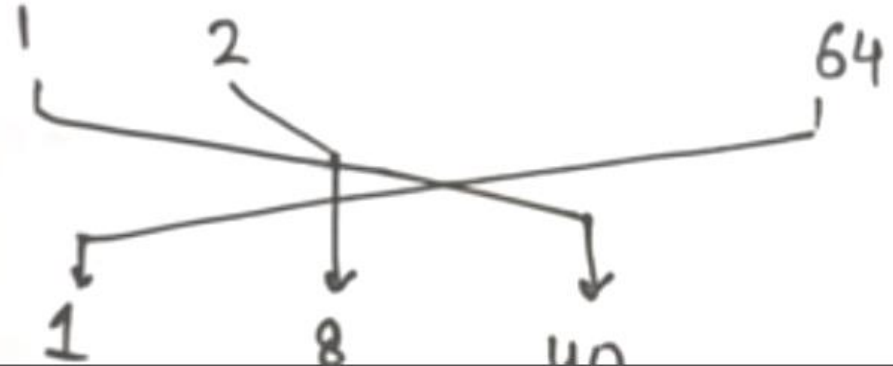
Initial Permutation (IP):

Occurs Only once before the first round.

Initial Permutation.



16 Rounds



Final Permutation (FP)

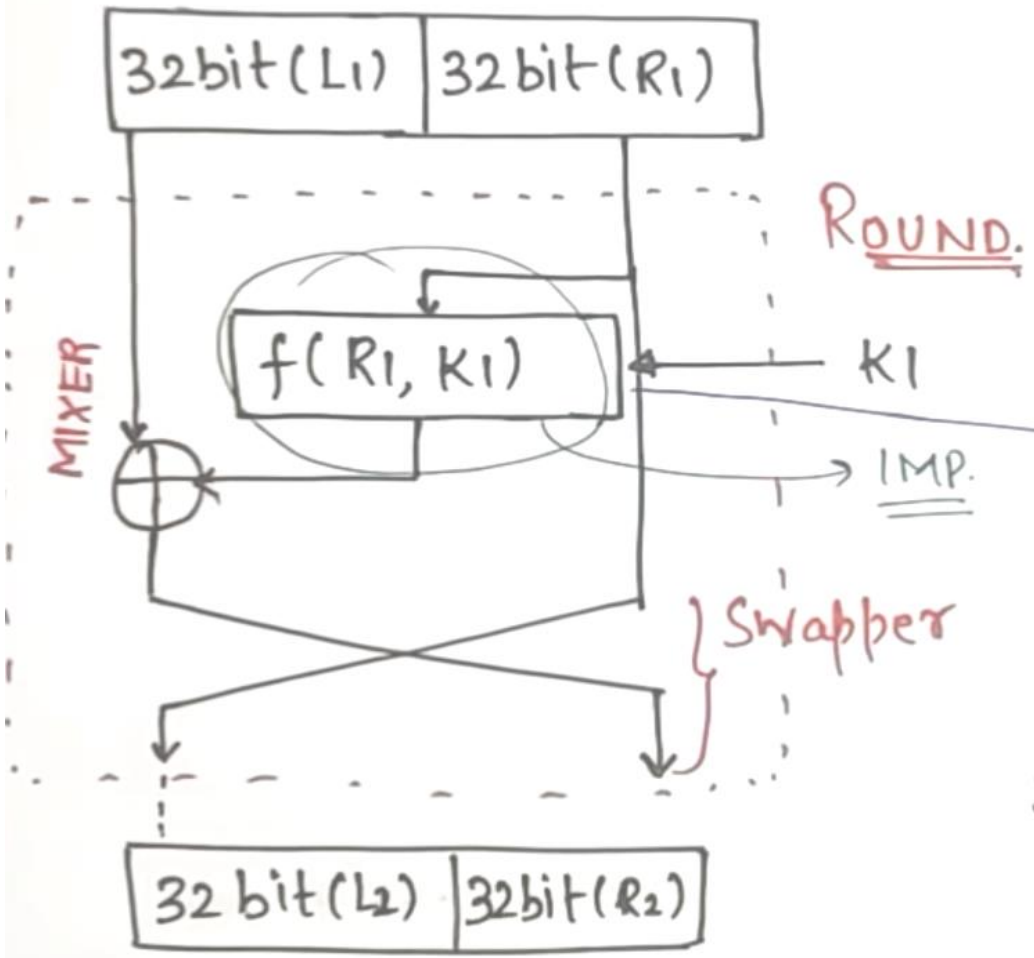
Both Initial and final permutation are straight P-Boxes that are inverses of each other. They have no cryptographic significance in DES.

Initial Permutation	Final Per.
58 50 42	40 08 48 ...
.....	.....
.....1.....	.....
.....	.....

Predefined table.

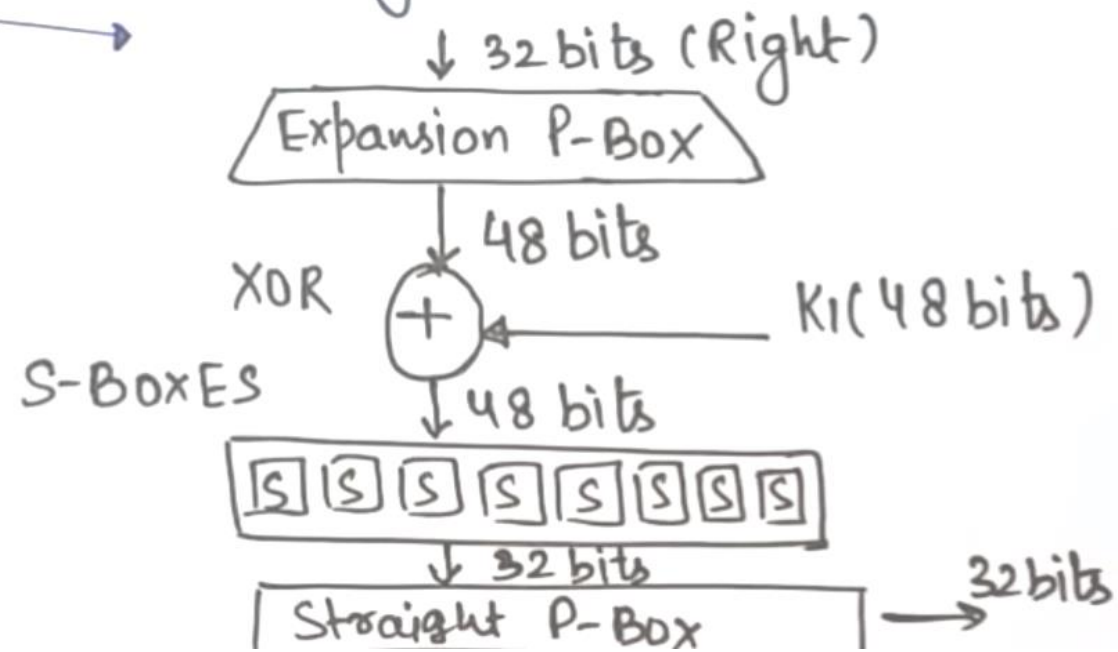
ROUNDS:

There are 16 rounds and each round is a Fiestel Cipher.

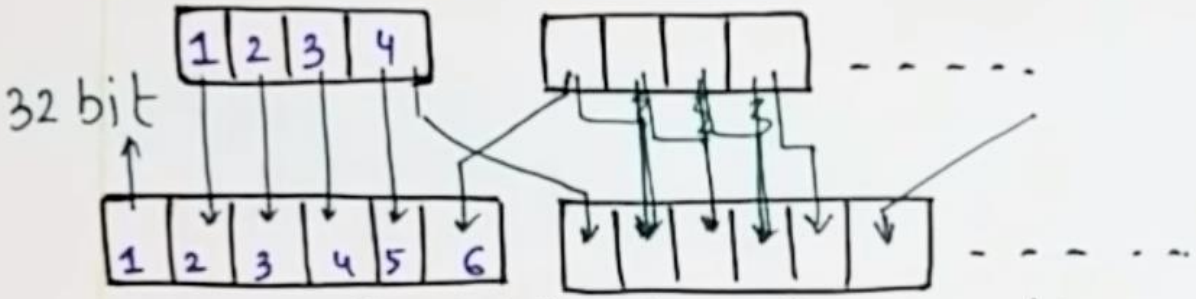


DES Function: Applies 48-bit key to the rightmost 32 bits to produce 32-bit o/p.

- Expansion P-Box
- Whitener
- Group of S-Boxes
- Straight P Box.



Expansion P-BOX: (32bit – 48bit)



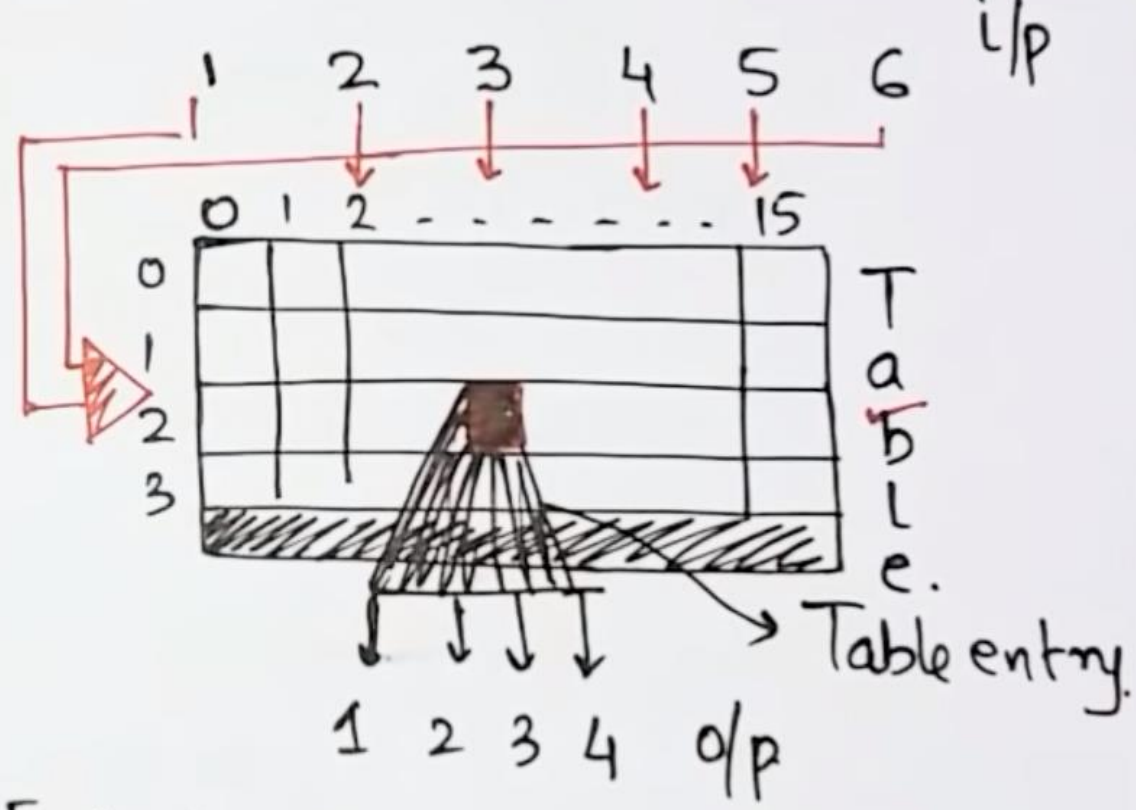
1 → 4th bit of Previous block.

1 → 2
2 → 3
3 → 4
4 → 5
6] → 1 bit of next block

Whitener:- XOR oper^{n} b/w 48 bit key and 48 bit o/p from expansion P-BOX.

S-BOXES: 8 are used.

6 bit i/p and 4 bit o/p.



Each S-Box has diff. table.

bit 1 and 6 → Row selected

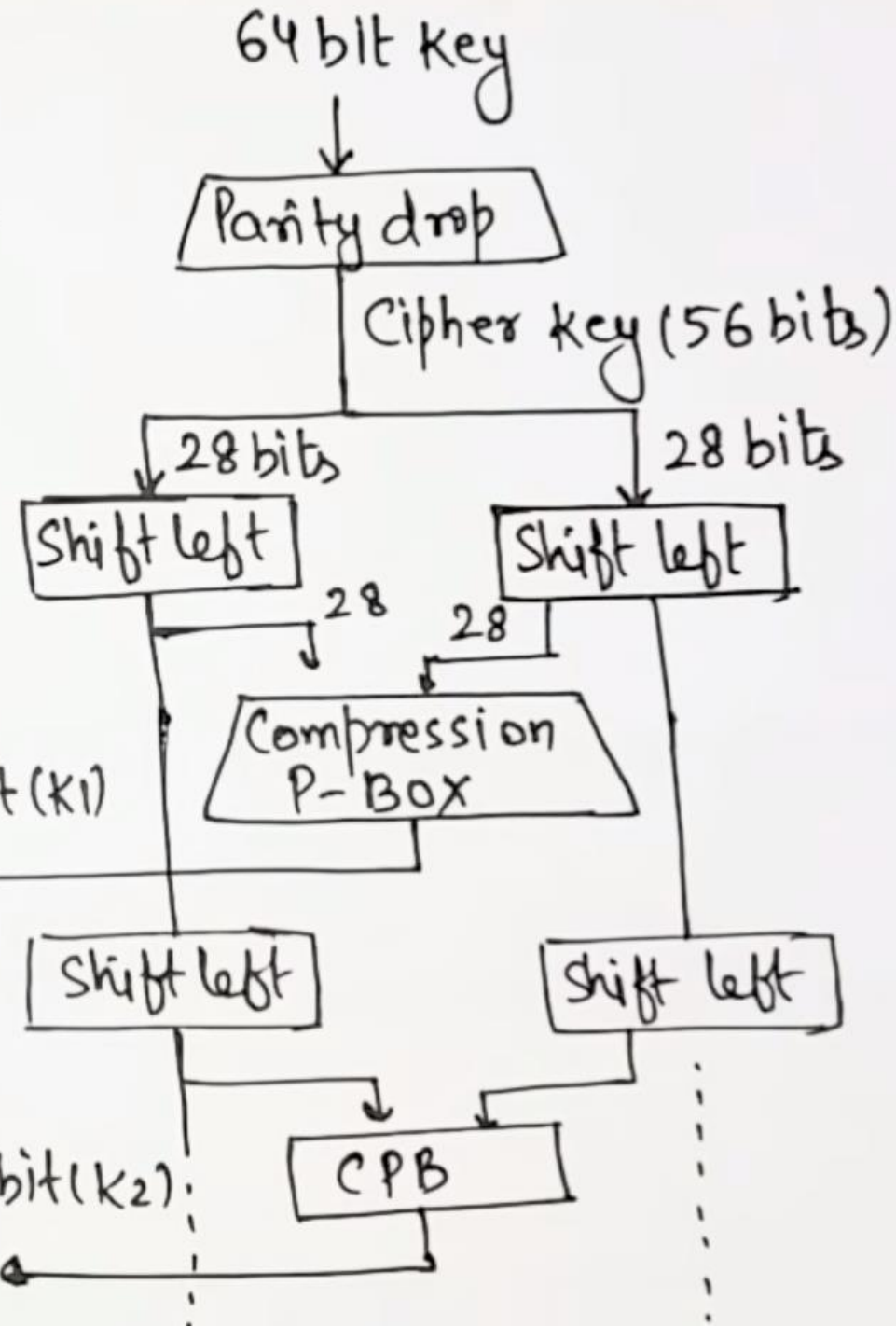
bit 2, 3, 4 and 5 → Column selected.

KEY GENERATION:

Round-Key Generator Creates sixteen 48-bit keys out of a 56-bit cipher key.

Actual Key is of **64 bit** from which 8 extra Parity bits are dropped.

↳ (8,16,24,32,40,48,56,64)



SHIFTING.

IMP.

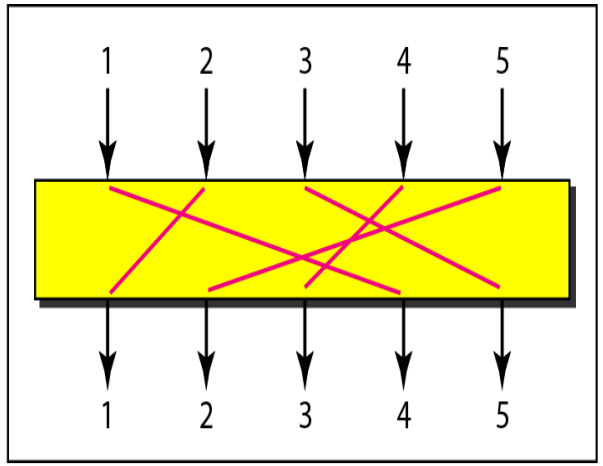
1, 2, 9, 16 → one bit

others → Two bits

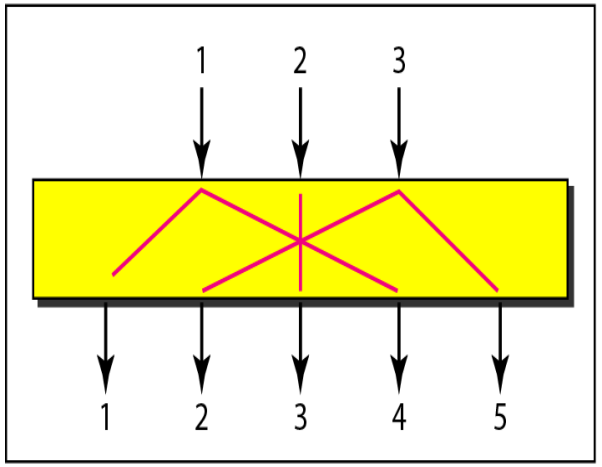
Symmetry Key Cryptography: DES

- The **function consists of four steps**, carried out in sequence.
  - First, a 48-bit number, *E*, is constructed by expanding the 32-bit R_{i-1} according to a fixed transposition and duplication rule.
  - Second, *E* and K_i are XORed together.
  - This output is then partitioned into ***eight groups of 6 bits each***, each of which is fed into **a different S-box**. Each of the 64 possible inputs to an S-box is mapped onto a 4- bit output.
  - Finally, these 8 × 4 bits are passed through **a P-box**.
- In **each of the 16 iterations, a different key is used**. Before the algorithm starts, a 56-bit transposition is applied to the key.
- Just before each iteration, the key is **partitioned into two 28-bit units**, each of which is **rotated left by a number of bits dependent on the iteration number *(1,2,9 and 16th 1-bit) and others 2-bit)***.
- **A different 48-bit subset of the 56 bits is extracted and permuted on each round.**

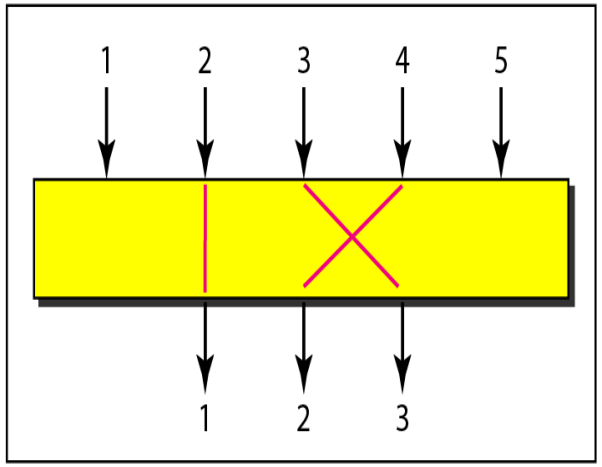
P-boxes: straight, expansion, and compression



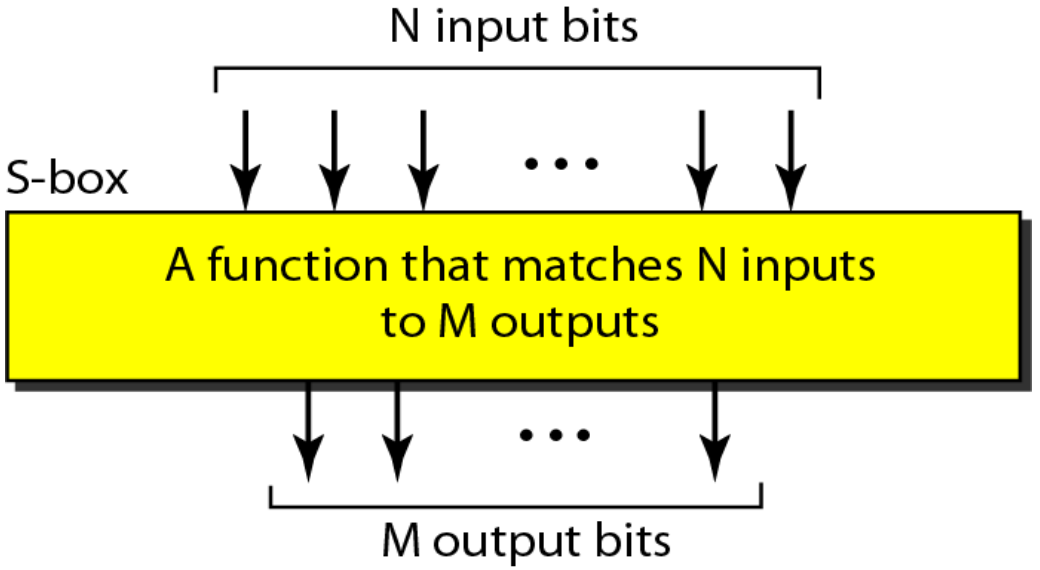
a. Straight



b. Expansion



c. Compression

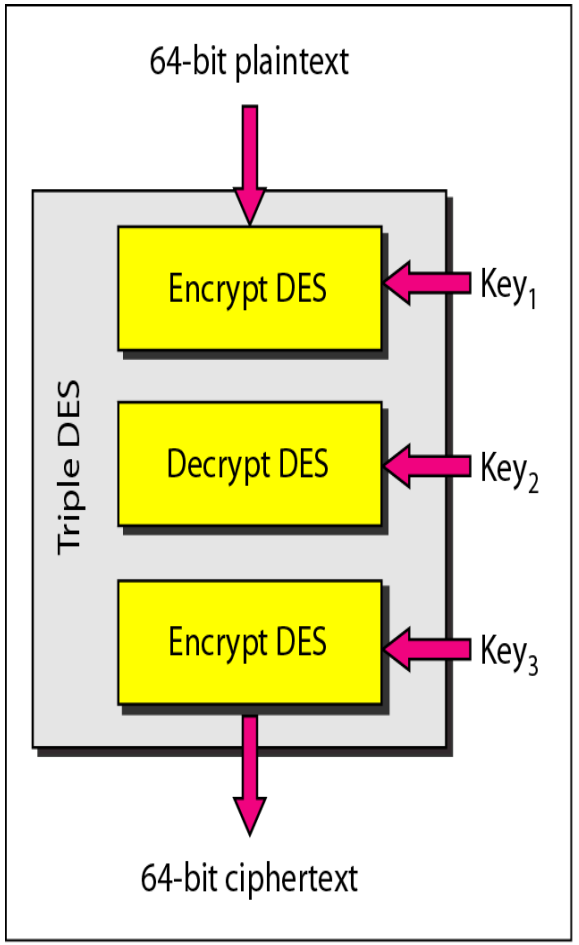


Symmetry Key Cryptography: DES

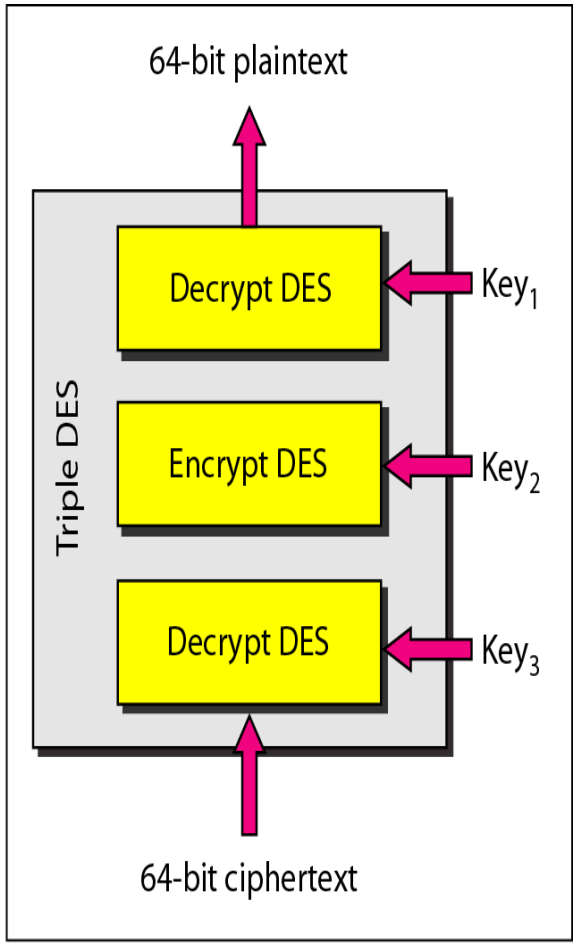
- In 1977, two Stanford cryptography researchers, **Diffie and Hellman** (1977), designed a machine to break DES and estimated that it could be built **for 20 million dollars.**
- Given a **small piece of plaintext** and matched ciphertext, this machine could find the key by exhaustive search of the **2^{56}-entry key** space in **under 1 day**.
- Nowadays, the game is up. Such a machine exists, is for sale, and costs less than $10,000 to make.

Triple DES

- Critics of DES contend that the key is too short.
- To lengthen the key, Triple DES or 3DES has been proposed and implemented.
- Ciphertext = **EK3(DK2(EK1(Plaintext)))**
- Plaintext = **DK1(EK2(DK3(Ciphertext)))**
- Has 112 bits of security, **NOT 3 x 56 = 168**
- For high security use 3DES and chain block coding

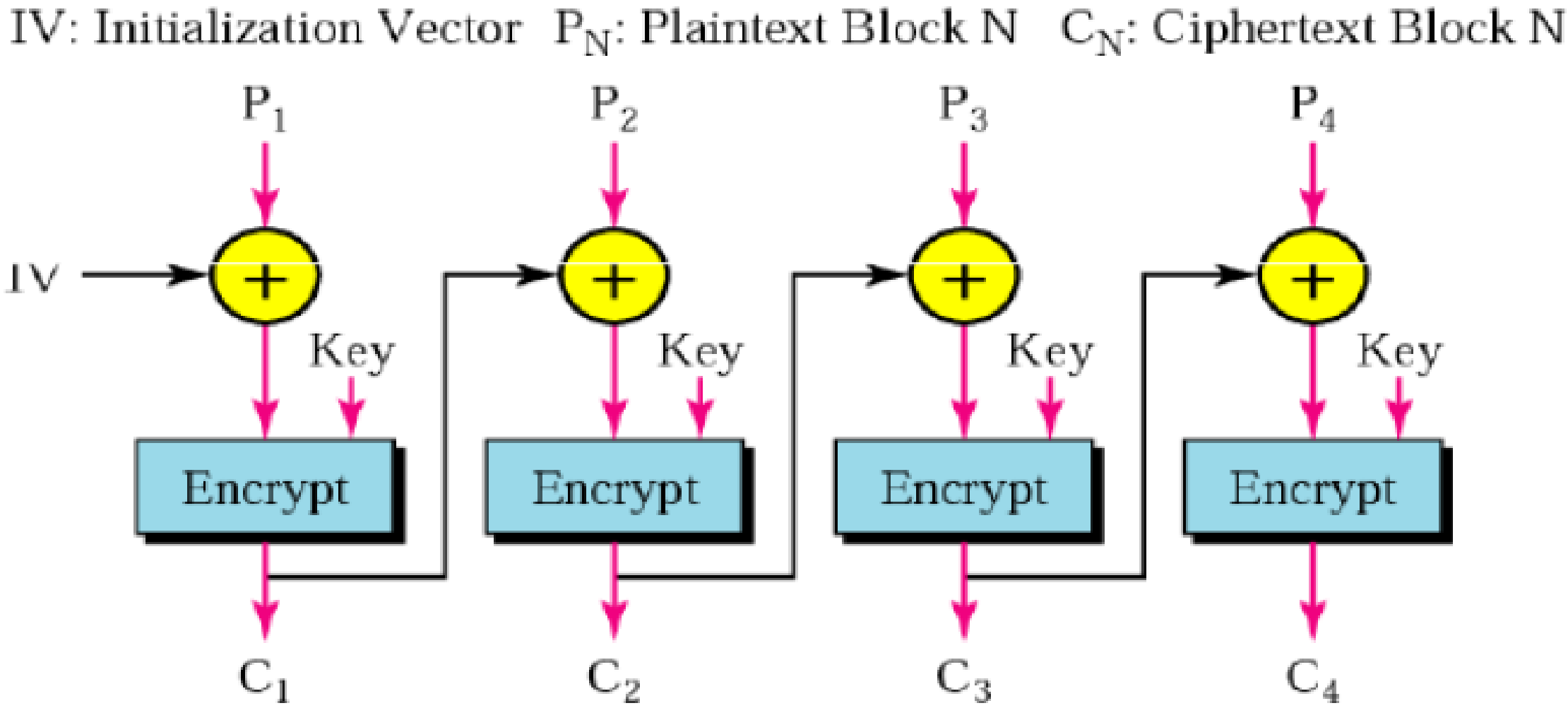


a. Encryption Triple DES



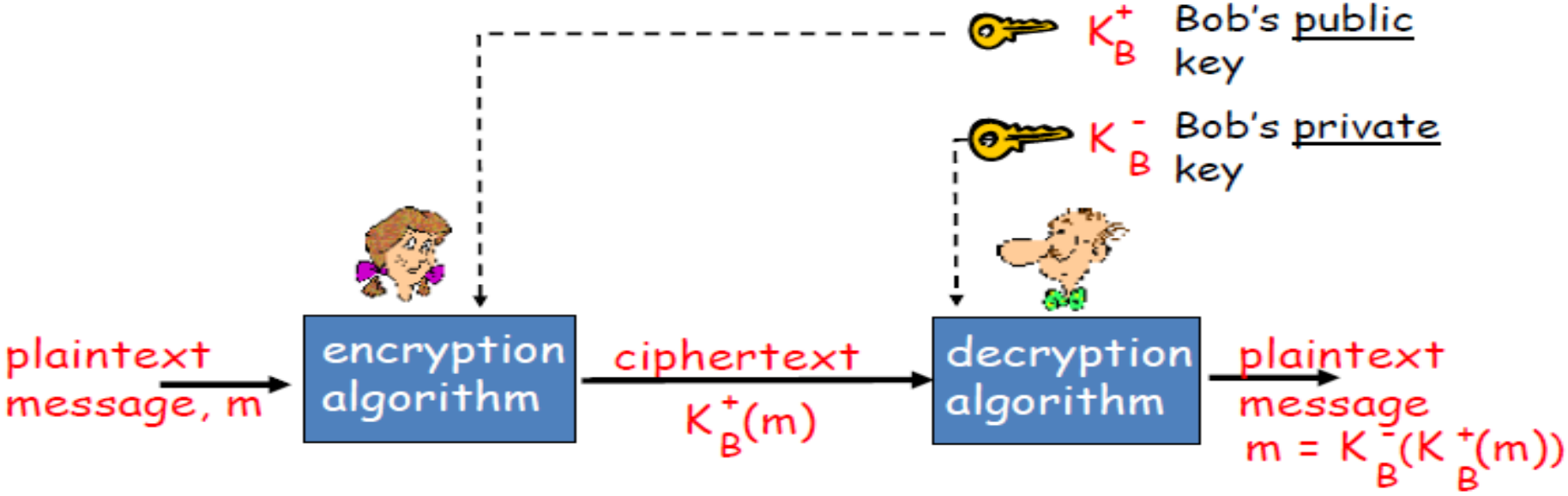
b. Decryption Triple DES

DES Modes : Chain Block Coding



Public/ Asymmetric Key Encryption

- **Two keys:** Encryption and decryption keys are different
  - **Public encryption key**: known and made public
  - **Private decryption key**: secret and is held by owner
- **To encrypt a message**: The recipient's public key along with the sender's private key are used.
- **To decrypt a message** the receiver's private key along with the sender's public key are used.



Public Key Cryptography: RSA

- Public key algorithm invented in 1977 and Most widely used Algorithm
- Proposed by Ron **Rivest,** Adi **Shamir**, and Leonard **Adelman** in 1977 and a paper was published in The Communications of ACM in 1978
- **Algorithm Steps:**
  1. Choose two large primes, p and q (typically 1024 bits).
  2. Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$. ’
  3. Choose a number, e, relatively prime to *z such* that *GCD(e, z) = 1*.
  4. Find d such that $d \times e = 1 \ mod \ z$.
  5. Publish ***e and n as the Public Key***
  6. Keep ***d and n as the Private Key***

Public Key Cryptography: RSA

- Select primes: p=17 & q=11
- Compute n = p*q =17×11=187
- Compute z(n)=(p–1)(q-1)=16×10=160
- Select e : GCD(e,160)=1; choose e=7
- Determine d: de=1 mod 160 and d < 160
  - Value is d=23 since 23×7=161= 10×160+1
- Publish public key e and n={7,187}
- Keep secret private key d and n={23, 187}

RSA Encryption and Decryption

- ***To encrypt** a message, P, compute* $C = P^e \pmod n$.
- ***To decrypt** C, compute* $P = C^d \pmod n$.

Plaintext: 5

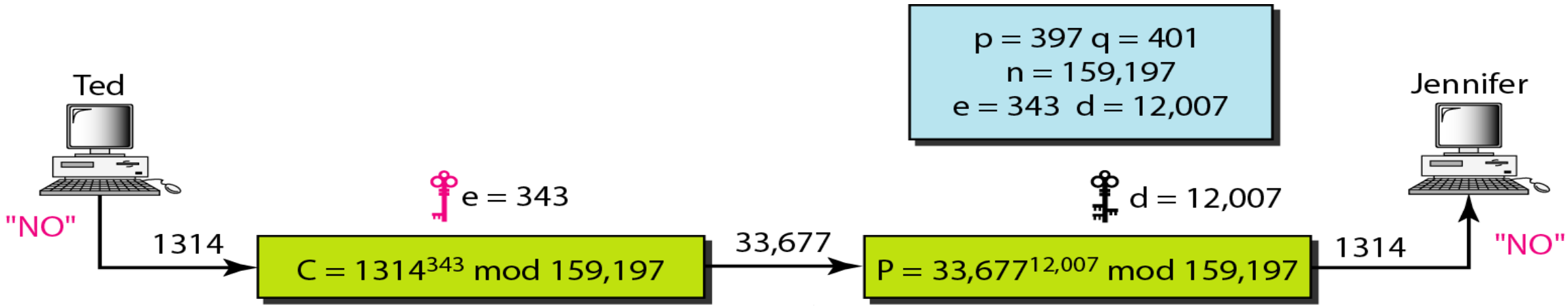
$C = 5^{13} = 26 \bmod 77$

Ciphertext: 26

Ciphertext: 26

$P = 26^{37} = 5 \bmod 77$

Plaintext: 5



- Let us give a realistic example. We randomly chose an integer of 512 bits. The integer **p is a 159-digit number**. *The integer **q is a 160-digit** number. We calculate n. **It has 309 digits**. We calculate F. It **has 309 digits**.*
- Alice wants to send the message **"THIS IS A TEST"** which can be changed to a numeric value by using the 00–26 encoding scheme (26 is the space character). **Message:**

P = 19070818260818260026190418 19

p = 96130345313583504574191581280615427909309845594996215822583150879647940
45505647063849125716018034750312098666606492420191808780667421096063354
219926661209

q = 12060191957231446918276794204450896001555925054637033936061798321731482
14848376465921538945320917522527322683010712069560460251388714552496900
0359660045617

n = 11593504173967614968892509864615887523771457375454144775485526137614788
54083263508172768788159683251684688493006254857641112501624145523391829
27162507656772727460097082714127730434960500556347274566628060099924037
10299142447229221577279853172703383938133469268413732762200096667667183
183108837342082344437095 3

e = 35535

d = 5800830286003776393609366128967791759466906208965096218042286611138059385282235873170628691003002171085904433840217072986908760061153062025249598844480475682409662470814858171304632406440777048331340108509473852956450719367740611973265574242372176176746207763716420760033708533328853214470885955136670294831

The ciphertext calculated by Alice is $C = P^e$, which is

C = 4753091236462268272063655506105451809423717960704917165232392430544529606131993285666178434183591141511974112520056829797945717360361012782188478927415660904800235071907152771859149751884658886321011483541033616578984679683867633765777465625079280521148141844048141844308127730590046928742485591664621086 56

Bob can recover the plaintext from the ciphertext by using $P = C^d$, which is

P = 1907081826081826002619041819

The recovered plaintext is THIS IS A TEST after decoding.

Diffie-Hellman Key Exchange Properties

- **Used in:** SSL, SSH, IPSec, Cisco encrypting routers, Sun secure RPC and etc.
- The protocol that allows strangers to establish a shared secret key is called the **Diffie-Hellman key exchange** (Diffie and Hellman, 1976) and works as follows.
  - Alice and Bob have to **agree on two large numbers, *n* and *g***, where *n* is a prime, (*n* - 1)/2 is also a prime and certain **conditions apply to *g*. These numbers may be public**, so either one of them can just pick ***n* and *g* and tell the other openly.**
  - Now **Alice picks** a large (say, 512-bit) **number, *x*, and keeps it secret**.
  - Similarly, **Bob picks a large secret number, *y***.
  - **Alice initiates the key** exchange protocol by sending Bob a **message containing (n, g, g^x mod n).**
  - **Bob responds** by sending Alice a **message containing g^y mod n.**

Diffie-Hellman Key Exchange Properties

- Now **Alice raises the number Bob sent** her to the x^{th} power modulo n to get **$(g^y \bmod n)^x \bmod n$**.
- **Bob performs** a similar operation to get **$(g^x \bmod n)^y \bmod n$**. By the laws of modular arithmetic, both calculations yield **$g^{xy} \bmod n$.**
- **Alice and Bob suddenly share a secret key, $g^{xy} \bmod n$.**

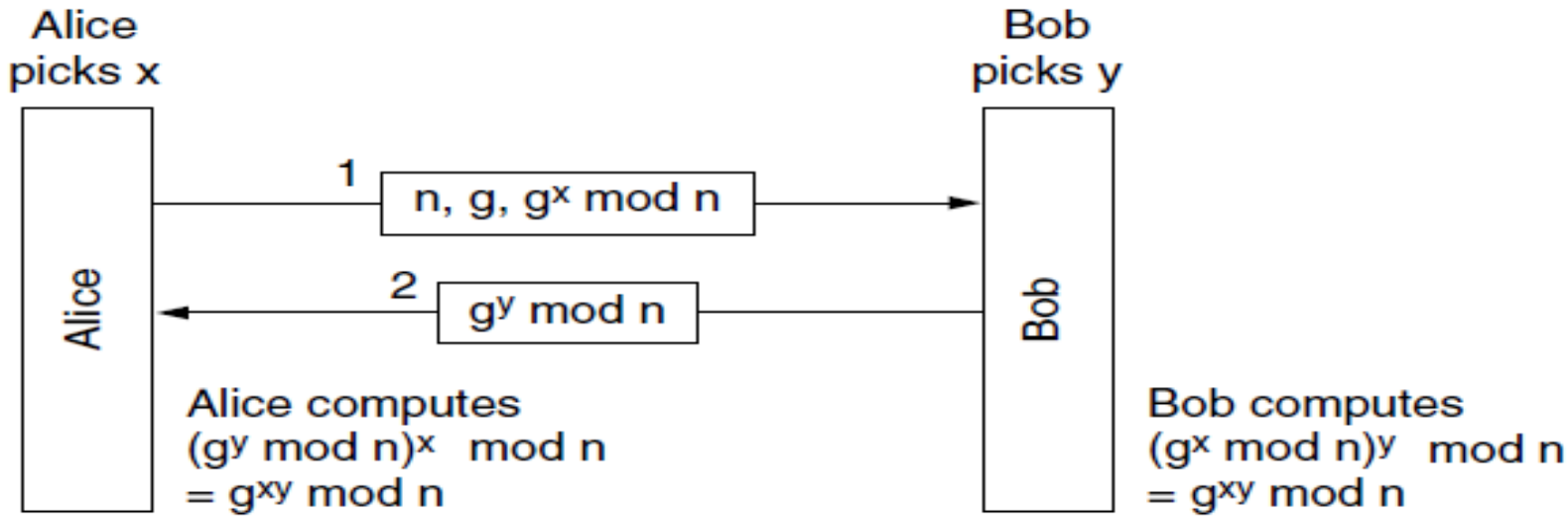


Figure 8-37. The Diffie-Hellman key exchange.

Diffie-Hellman Key Exchange Properties

- To make an Example,, we will use the values of ***n* = 47 and *g* = 3**.
- Alice picks ***x* = 8** and Bob picks ***y* = 10**. **Both of these are kept secret.**
- Alice's message to Bob is **(47, 3, 28) because 38 mod 47 is 28.**
- **Suppose Bob's message to Alice is (17).**
- Alice computes **$(g^y \bmod n)^x \bmod n$** i.e. **$g^y \bmod n=17$**, and $(g^y \bmod n)^x \bmod n$ = **$(17)^8 \bmod 47$, which is 4.**
- Bob computes **$(g^x \bmod n)^y \bmod n$** i.e. **$g^x \bmod n=28$** and $(g^x \bmod n)^y \bmod n$ = **2810 mod 47, which is 4.**
- Alice and Bob have independently **determined that the secret key is now 4.**
- **Trudy has to solve the equation $3^x \bmod 47 = 28$**, which can be done by exhaustive search for small numbers like this, but not when all the numbers are hundreds of bits long.
- **All currently-known algorithms simply take too long, even on massively parallel supercomputers.**

Digital Signature

- Digital Signature is an Electronic **Analogue of a written signature.**
- A digital signature is a technique that **binds a person/entity to the digital data**. This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a **secret key known only by the signer.**
- **Importance of Digital Signature**
  - **Message authentication**: When the verifier validates the digital signature using public key of a sender, he is assured that **signature has been created only by sender** who possess the corresponding **secret private key and no one else**.
  - **Non-repudiation**: Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party **as evidence if any dispute arises in the future.**

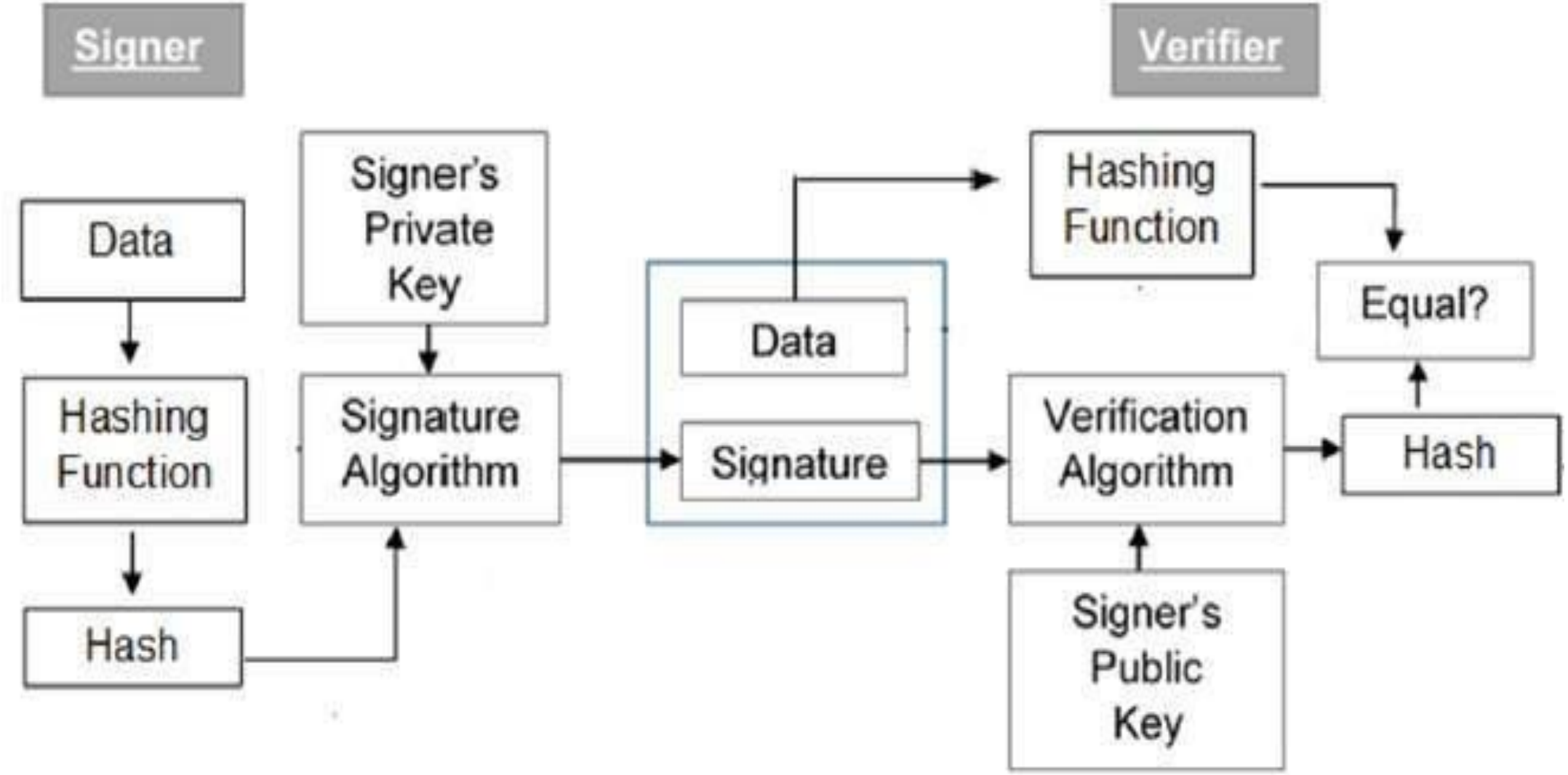
Digital Signature

- **Data Integrity**: In case an attacker has access to the data and modifies it, **the digital signature verification at receiver end fails.** The hash of modified data and the output provided by the **verification algorithm will not match.** Hence, **receiver can safely deny the message** assuming that data integrity has been breached.

- In many digital communications, it is desirable to **exchange an encrypted messages** than plaintext to achieve confidentiality. In public key encryption scheme, **a public (encryption) key of sender is available in open domain**, and hence anyone **can spoof his identity** and **send any encrypted message to the receiver**.
- This makes it essential for users employing **PKC for encryption to seek digital signatures along with encrypted data** to be assured of **message authentication and non-repudiation.**

Model of Digital Signature

- The model of digital signature scheme is depicted in the following illustration:



Digital Signature

- The **private key used for signing** is referred to as the **signature key** and the **public key as the verification key.**
- Signer **feeds data to the hash function** and generates **hash of data**.
- **Hash value and signature** key are then fed **to the signature algorithm** which produces the **digital signature on given hash**. **Signature is appended to the data** and then both are **sent to the verifier**.
- Verifier **feeds the digital signature** and the **verification key into the verification algorithm**. The verification algorithm gives some value as output.
- Verifier also runs **same hash function** on received data **to generate hash value**.
- **For verification**, this hash value and **output of verification algorithm are compared**. Based on the **comparison result**, verifier decides **whether the digital signature is valid.**
- Since **digital signature is created by 'private' key of signer** and **no one else can have this key**; the **signer cannot repudiate signing the data in future**.

Securing e-mail (PGP)

- Pretty Good Privacy (PGP) is e-mail **an encryption scheme** that has become a **de-facto standard**, with thousands of users all over the globe.
- PGP encrypts data by using a block cipher called **IDEA** (**International Data Encryption Algorithm**), which uses 128-bit keys.
- In addition, **PGP provides data compression**.
- When **PGP is installed**, the software **creates a public key pair for the user**.
- The public key can be **posted on the user's Web site** or placed in a public key server.
- The **private key is protected by the use of a password**. The password has to be entered every time the user accesses the private key.
- PGP gives the user the **option of digitally signing the message**, encrypting the message, or **both digitally signing and encrypting.**

PGP Operation

- ***Authentication***
  - Sender creates message
  - Make SHA-1 160-bit hash of message
  - Attached RSA signed hash to message
  - Receiver decrypts & recovers hash code
  - Receiver verifies received message hash
    - if match, message is accepted as authentic

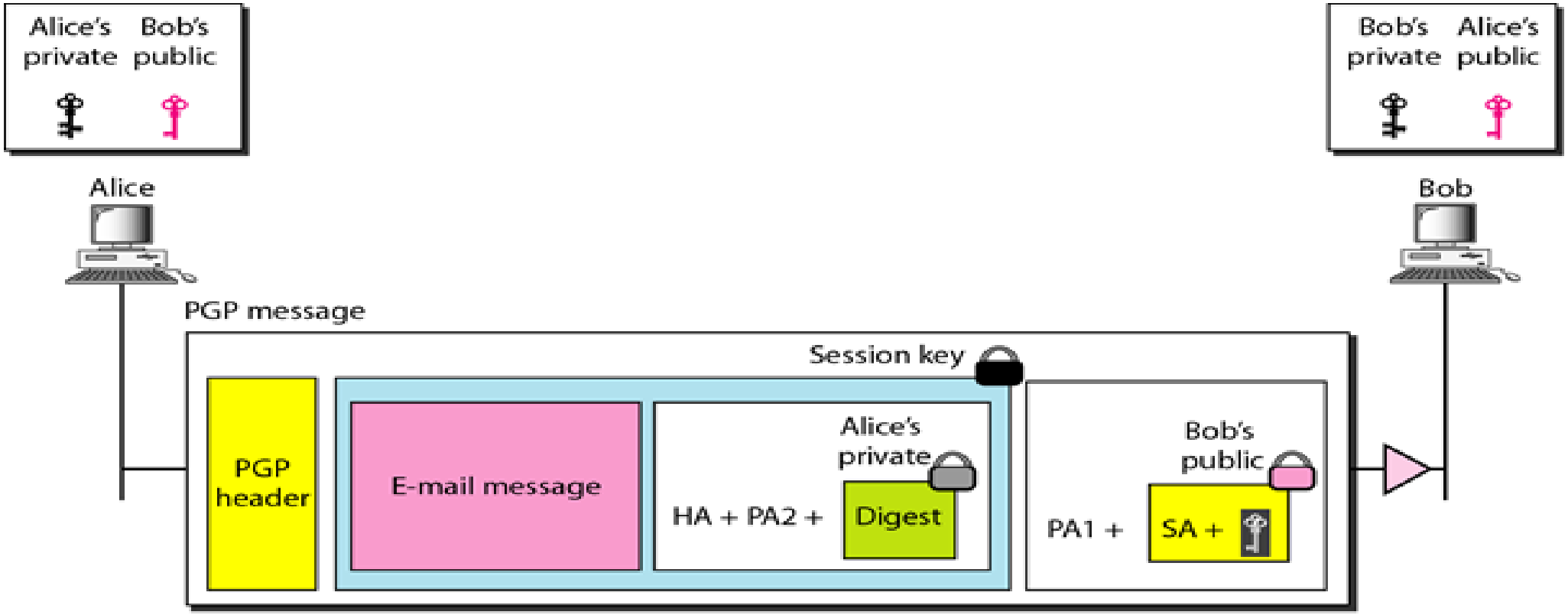
- ***Confidentiality***
  - Sender forms 128-bit random session key
  - Encrypts message with session key
  - Attaches session key encrypted with RSA
  - Receiver decrypts & recovers session key
  - Session key is used to decrypt message

PGP Operation

- ***Compression***
  - By default PGP compresses message after signing but before encrypting
  - Uses ZIP compression algorithm
- ***Email Compatibility***
  - PGP will have binary data to send (encrypted message etc.)
  - However email was designed only for text
  - Hence PGP must encode raw binary data into printable ASCII characters
  - Uses radix-64 algorithm

- ***Segmentation***
  - Another constraint of e-mail is that there is usually a maximum message length.
  - PGP automatically segments an encrypted message into blocks of an appropriate length.
  - On receipt, the segments must be re-assembled before the decryption process

A scenario in which an e-mail message is authenticated and encrypted



PA1: Public-key algorithm 1 (for encrypting session key)
PA2: Public-key algorithm (for encrypting the digest)
SA: Symmetric-key algorithm identification (for encrypting message and digest)
HA: Hash algorithm identification (for creating digest)

PGP Algorithms

Algorithm	*ID*	*Description*
Public key	1	RSA (encryption or signing)
	2	RSA (for encryption only)
	3	RSA (for signing only)
	17	DSS (for signing)
Hash algorithm	1	MD5
	2	SHA-1
	3	RIPE-MD
Encryption	0	No encryption
	1	IDEA
	2	Triple DES
	9	AES

PGP

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash:  SHA1
Bob:
Can I see you tonight?
Passionately yours, Alice
-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset:  noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gv
-----END PGP SIGNATURE-----
```

Figure A PGP signed message

Securing TCP connections (SSL)

- Secure sockets layer (SSL), originally **developed by Netscape**, is a protocol designed to provide **data encryption and authentication** between a **Web client and a Web server.**
- TCP & SSL: **provides a reliable & secure end-to-end service**.
- HTTPS: **HTTP over SSL (or TLS).Typically on port 443**.
- SSL is widely used in Internet commerce, being implemented **in almost all popular browsers and Web servers.**
- **SSL provides network connection security through:**
  - **Confidentiality**: Information is exchanged in an encrypted form.
  - **Authentication**: Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.
  - **Reliability**: Maintains message integrity checks.

Securing TCP connections (SSL)

- The protocol **begins with a handshake phase that negotiates an encryption algorithm** (e.g. DES or RSA) and keys, and authenticates the server to the client.
- Optionally, the client can also be authenticated to the server.
- **Once the handshake is complete and the transmission of application data begins**, and all data is encrypted using session keys negotiated during the handshake phase.
- **SSL builds a secure connection between two sockets, including**
  1. **Parameter negotiation** between client and server.
  2. **Authentication** of the server by the client.
  3. **Secret communication.**
  4. **Data integrity protection**

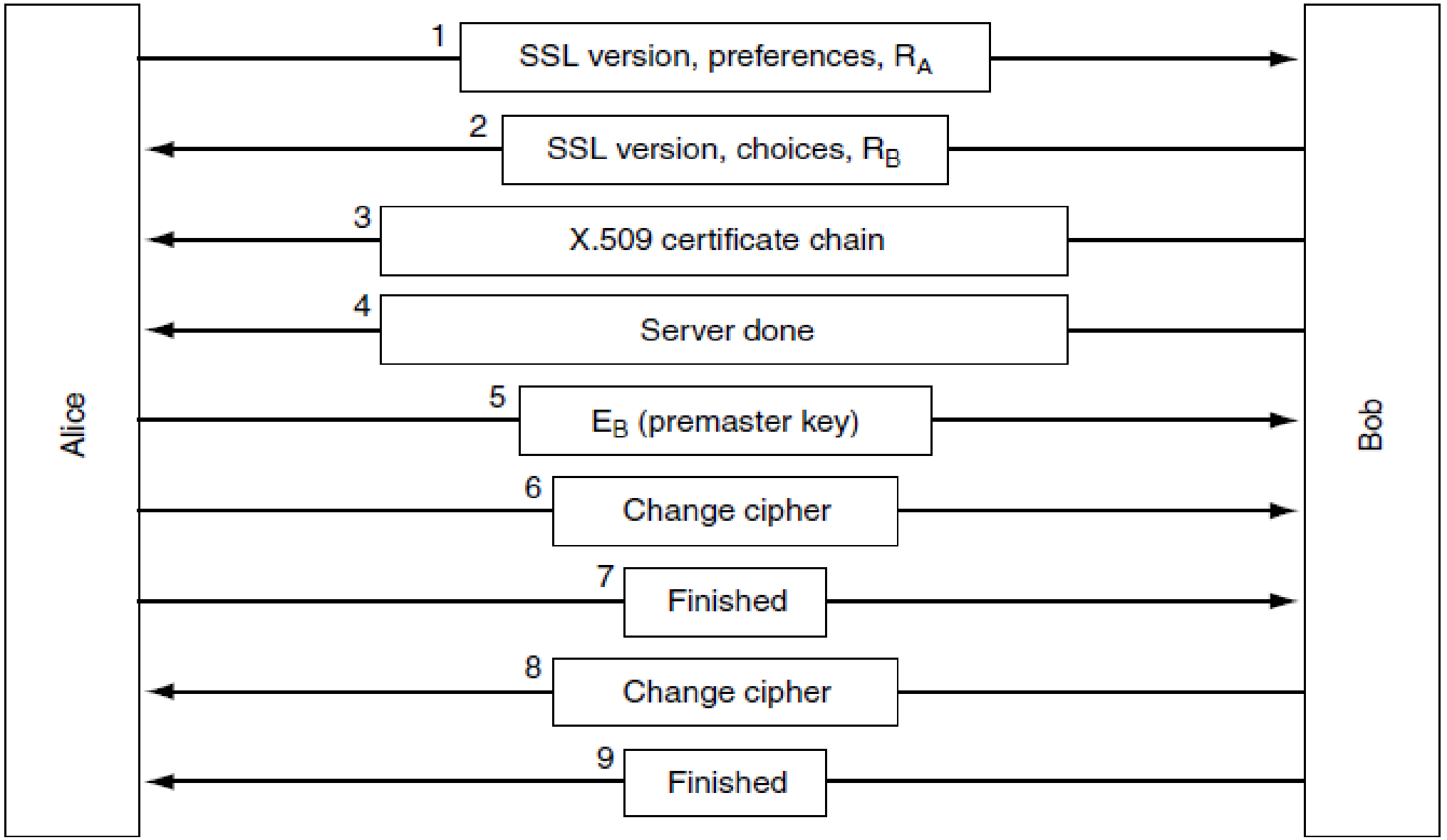


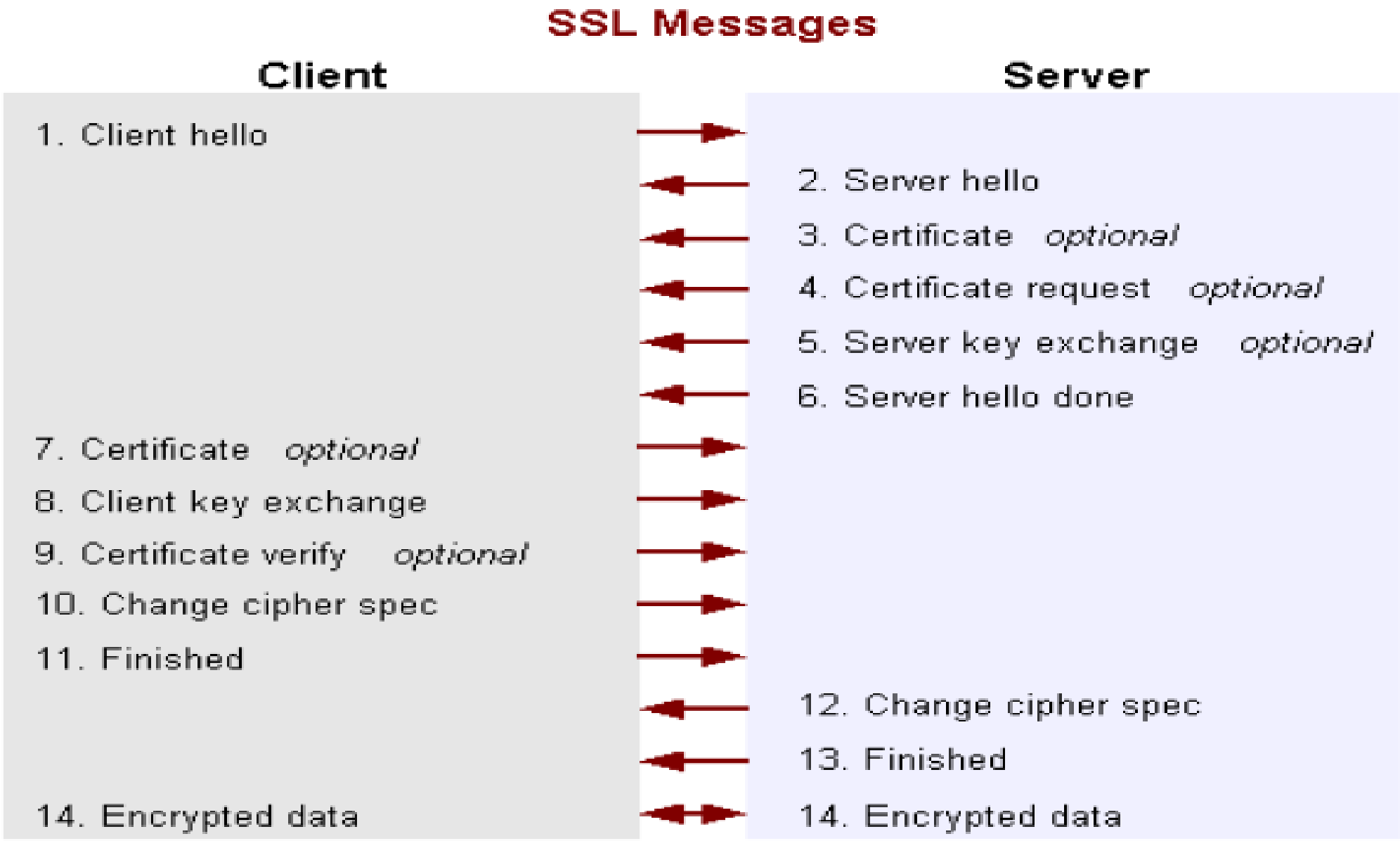
Figure 8-50. A simplified version of the SSL connection establishment subprotocol.

SSL connection establishment subprotocol

1. Alice sends a request to Bob to establish a connection. The request specifies the SSL version Alice has and her preferences with respect to compression and cryptographic algorithms. It also contains a nonce, R_A, to be used later.
2. Bob makes a choice among the various algorithms that Alice can support and sends his own nonce, R_B.
3. Bob sends a certificate containing his public key.
4. When Bob is done, he sends **message 4** to tell Alice it is her turn.
5. Alice responds by choosing a **random 384-bit premaster key** and sending it to Bob encrypted with his public key.

- **After message 5 has been received**, both Alice and Bob are able **to compute the session key**. For this reason, **Alice tells Bob** to switch **to the new cipher** (message 6) and also that **she is finished with the establishment subprotocol** (message 7). **Bob then acknowledges her (messages 8 and 9).**

How SSL Works: The *Handshake* in Detail



Network layer security – IPSec.

- **IPSecurity (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 to **create authenticated and confidential** packets for the IP layer.
- ***IPsec Communication Modes:*** ***Transport and Tunnel mode***
  - **Transport mode**:
    - the **IPsec header is inserted** just after the IP header.
    - The ***Protocol*** **field in the IP header is changed** to indicate that an IPsec header follows the normal IP header (before the TCP header).
    - The IPsec header contains **security information**, a new sequence number, and possibly an integrity check of the payload.

Network layer security – IPSec.

- **Tunnel mode**
  - **AH or ESP fields are added to the IP packets**, the entire packet
  - The entire packet **travel through the tunnel** from **source** address to the **destination address**.
  - Tunnel mode is used **when both ends or one ends uses firewall** or router that implements IPSec .
  - **The unprotected packets can pass through external networks.**
  - Tunnel mode is also useful when the tunnel ends at a location other than the final destination.
  - **The disadvantage of tunnel mode is that it adds an extra IP header, thus increasing packet size substantially.**
  - **In contrast, transport mode does not affect packet size as much.**

Network layer security – IPSec.

- There are **two security protocols** defined by IPsec — **Authentication Header (AH) and Encapsulating Security Payload (ESP).**
- **AH** can provide **integrity protection for packet headers and data**, but it cannot encrypt them.
- The ESP protocol provides **data integrity and secrecy**. Providing more services, the ESP protocol is **naturally more complicated and requires more processing** than the AH protocol.
- **ESP can provide encryption and integrity protection for packets**, but it **cannot protect** the outermost IP header**, as AH can**.
  - However, this protection is not needed in most cases.
  - Accordingly, **ESP is used much more frequently** than AH because of **its encryption capabilities.**
  - **For a VPN**, which requires confidential communications, **ESP is the natural choice.**

Virtual Private Network

- A virtual private network (VPN) is a **private network that interconnects remote** (and often geographically separate) **networks through primarily public communication** infrastructures such as the Internet.
- VPNs provide security **through tunneling protocols and security procedures** such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.
- This is **often less expensive than alternatives**
  - such as dedicated private telecommunications lines between organizations or branch offices.
- Firewalls, VPNs, and IPsec with ESP in tunnel mode are a natural combination and widely used in practice
- VPNs can use **both symmetric and asymmetric forms of cryptography**.

VPN Architecture: Host-to-Gateway

- Protects communications between one or more individual hosts and a specific network belonging to an organization.
- Eg., traveling employees to gain access to internal organizational services, such as the organization's e-mail and Web servers.

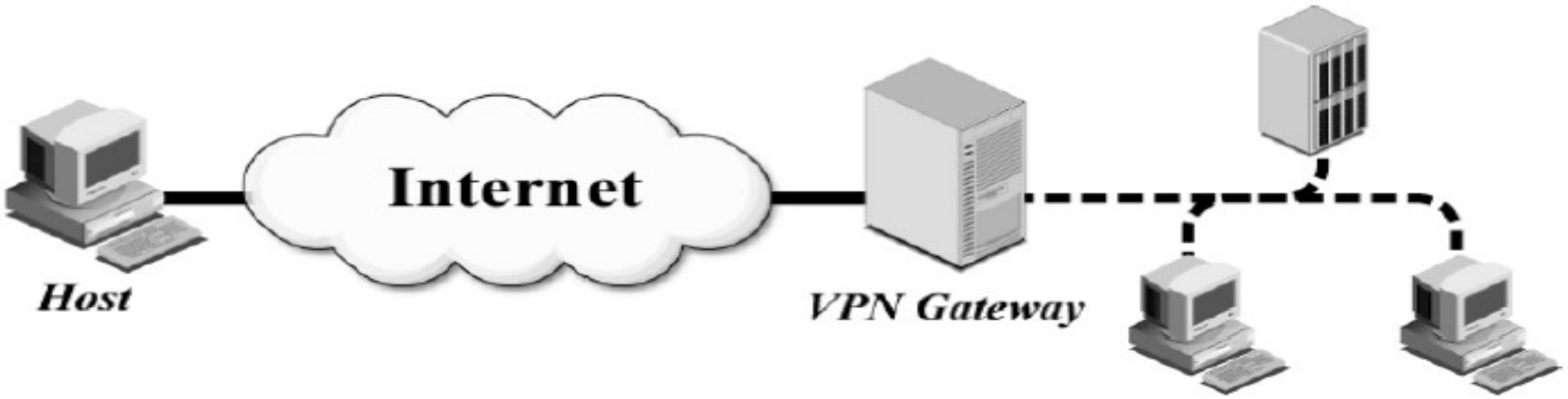


Figure: Host-to-Gateway Architecture Example

VPN Architecture: Gateway-to-Gateway

- Gateway-to-gateway:
  - Protects communications between two specific networks
  - Eg., an organization's main office network and a branch office network, or two business partners networks.

Figure : Gateway-to-Gateway Architecture Example

Firewall

- A **firewall** is a **network security** system that **monitors and controls incoming and outgoing network traffic** based on **predetermined security rules**.
- A firewall typically establishes a **barrier between a trusted internal network and untrusted external network**, such as the Internet.
- Firewalls are often categorized as either **network firewalls** or **host-based firewalls**.
- **Network firewalls** filter traffic **between two or more networks** and **run on network hardware.**
- **Host-based firewalls** run on **host computers** and **control network traffic** in and out of those machines.
- A **firewall** is a **combination of hardware and software** that isolates an **organization's internal network from the Internet at large**, allowing specific connections to **pass and blocking others.**

Firewall

- **Organizations employ firewalls** for one or more of the **following reasons**:
  - To prevent intruders from **interfering with the daily operation** of the internal network.
  - To prevent intruders from **deleting or modifying information** stored within the internal network.
  - To prevent intruders from **obtaining secret information**.
  - To preserve **customer and partner confidence**
  - To prevent **viruses and worms on your network**
  - To prevent **malicious attackers** from getting into your network
- **Firewall Types**
  - Packet Filtering
  - Application Level Gateway

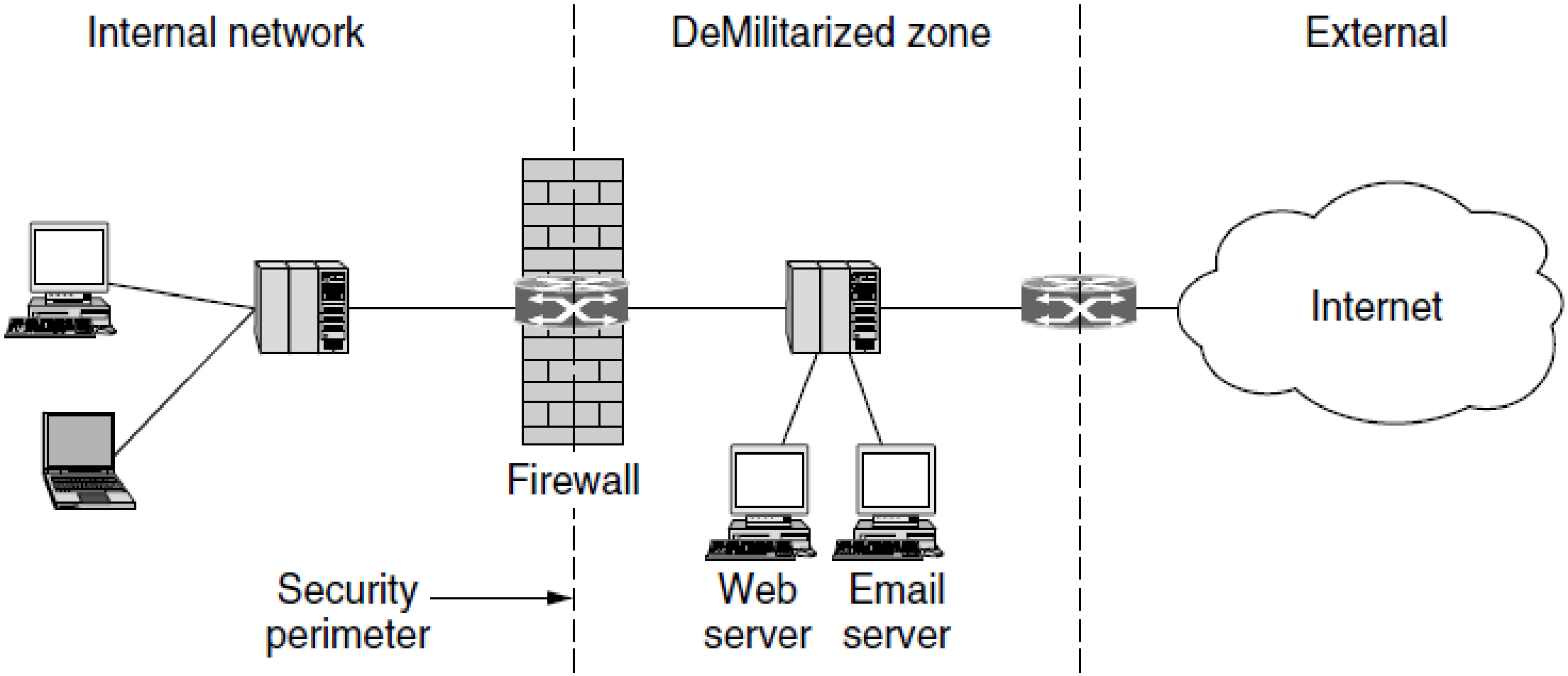


Figure 8-29. A firewall protecting an internal network.

Firewall: Packet Filtering

- A **packet-filter firewall** is **a router** that uses a **filtering table** to decide which packets **must be discarded** (not forwarded).
- It can **forward or block packets** based on the information in the **network layer and transport layer headers**:
  - source and destination IP addresses,
  - source and destination port addresses,
  - ICMP message type
  - TCP SYN and ACK bits
  - and type of protocol (TCP or UDP).
- **Example:** block incoming and outgoing datagram with IP protocol field = 17 and with either source or destination port = 23.
  - **All incoming and outgoing UDP flows and telnet connections are blocked.**

Firewall: Application Level Gateway

- They are **called Proxy Servers** and acts as a relay of application level traffic.
- In order to have a **finer level security**, firewalls must **combine packet filters with application gateways.**
- Application gateways **look beyond the IP/TCP/UDP headers** and actually make **policy decisions based on application data**.
- When the **user client process sends a message**, the proxy firewall **runs a server process to receive the request.** The server opens the packet at the application level and **finds out if the request is legitimate**.
- **If it is**, the server acts as a client process and **sends the message to the real server** in the corporation. **If it is not**, the **message is dropped and an error message** is sent to the external user.
- **In this way,** the requests of the **external users are filtered** based on the contents at the application layer.

Firewall: Application Level Gateway

- **Example: allow selected internal users to telnet outside**
  - Can be accomplished by implementing a **combination of a packet filter (in a router) and a Telnet application gateway.**
  - The filter is configured **to block all Telnet connections** except those that originate form the **IP address of the application gateway**.
  - **All outbound Telnet** connections **pass through the application gateway**.
  - When **a internal user wants** to Telnet to the outside world, it **first sets up a Telnet session with the gateway.**
  - The gateway prompts Firewalls the user **for its user id and password**; when the user supplies this information, the gateway **checks to see if the user has permission** to Telnet to the outside world. **If not**, the **gateway terminates the Telnet session**. If **the user has permission,** then the **gateway sets up a Telnet session** between the gateway and the external host
- **Thus the Telnet application gateway not only performs user authorization but also acts as a Telnet server and a Telnet client.**

Limitations of firewalls and gateways

- **IP spoofing**: router can't know if data "really" comes from claimed source
- The firewall **cannot protect against attacks that bypass the firewall**.
  - Internal systems may have dial-out capability to connect to an ISP.
- The **firewall does not protect against internal threats**,
  - such as a dishonest employee
  - or an employee who unwittingly cooperates with an external attacker.
- The firewall **cannot protect against the transfer of virus-infected programs** or files.
- ***Impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.***

Intrusion Detection Systems (IDS)

- **Intrusion :** Attempting **to break into or misuse** your system. Intruders may be **from outside** the network or **legitimate users of the network**.
- Intrusions are the **activities that violate the security policy of system.**
- **Intrusion Detection** is the process used to **identify and respond to intrusions**.
- Intrusion Detection Systems look **for attack signatures, which are specific patterns** that usually indicate **malicious or suspicious intent**.
- Used to monitor for "**suspicious activity**" on a network
- IDSs serve three essential security functions: **monitor, detect and respond to unauthorized activity**
- **Types of IDS:** *Host-based IDS*, ***Network-based IDS***, *Anomaly detection*, ***Signature base***

Type of IDS

- ***Host Based IDS***
  - A host based intrusion detection system **monitors the security event logs or checks the changes to the system.**
  - These audit information includes events like the use of identification and **authentication mechanisms** (logins etc.) , **file opens and program** executions, **admin activities etc**.
- ***Network-based IDS***
  - A filter is usually applied **to determine which traffic will be discarded or passed** on to an attack recognition module. This helps to filter out **known un-malicious traffic.**
  - System which **monitors packets** on the network wire and attempts to discover if **a hacker/cracker is attempting** to break into a system (or cause a denial of service attack).

Type of IDS

- ***Anomaly based IDS***
  - Anything **distinct from the noise** is assumed to be an **intrusion activity**.
    - **E.g. flooding a host with lots of packet.**
  - The **primary strength** is its ability **to recognize novel attacks**.
- ***Signature based IDS***
  - This IDS possess **an attacked description** that can be matched **to sensed attack manifestations.**
  - Most signature analysis systems are based off of simple **pattern matching algorithms**. In most cases, the IDS simply **looks for a sub string** within a **stream of data** carried **by network packets**.
  - When it finds this sub string (for example, **the ``phf'' in** ``GET /cgi-bin/phf?''), it identifies those network packets as **vehicles of an attack.**

Securing Wireless LANs

- Wireless networks more vulnerable
  - No inherent physical protection: sending/receiving messages do not need physical access to network infrastructure
- As a consequence
  - Eavesdropping is easy
  - Injecting bogus messages is easy
  - Replaying previously recorded messages is easy
  - Illegitimate access to network & services is easy
  - Denial of service is easy (jamming)

Wireless Security using WEP

- **WEP**: Wired equivalent privacy
- It is the original wireless security protocol for the 802.11 standard.
- The stated goal of WEP is to make wireless LAN as secure as a wired LAN.
- **Protocol goals**
  - **Confidentiality:** prevent eavesdropping
  - **Access control**: prevent unauthorized access
  - **Data integrity:** prevent tampering of messages
- It uses the **RC4 stream cipher**, using a 64-bit key. **In WEP, RC4** generates a key stream that is **XORed with the plaintext** to form the **cipher text.**
- It also employs a **CRC integrity checksum**.

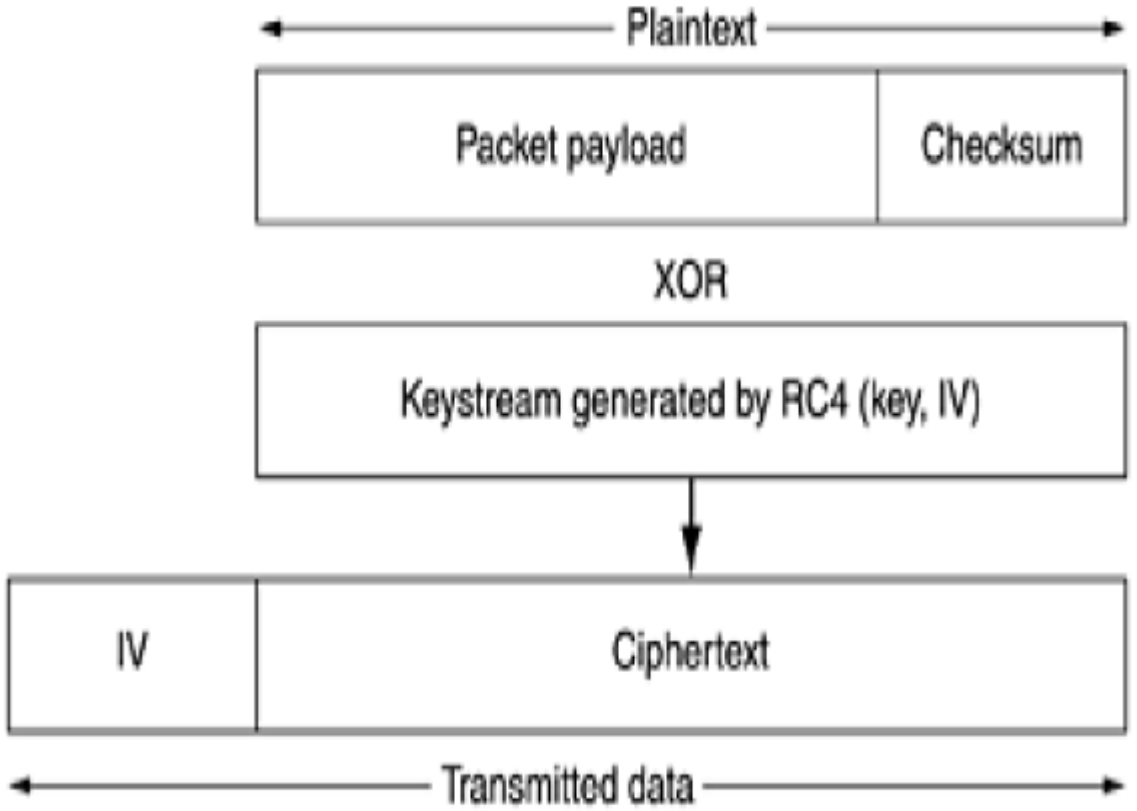
WEP Encryption

- **Message:** What you're encrypting
- **CRC:** To verify the integrity of the message
- **Plaintext:** The message + CRC
- **Initialization vector (IV):** A 24-bit number.
  - It's carried in plaintext in the "encrypted" message!
  - There are no restrictions on IV reuse!
  - The IV forms a significant portion of the "seed" for the RC4 algorithm!

Message	CRC
IV	Key
Keystream	
Ciphertext	

WEP Encryption

- **Key:** A 104-bit number which is used to build the keystream
- **Keystream:** What is used to encrypt the plaintext
  - **RC4 is a stream cipher**
  - The key is used by a p**seudo-random number** generator to generate a keystream
  - The **keystream is XORed with the plaintext** and checksum to **produce the ciphertext**.
- **Ciphertext:** What we end up post-encryption



Thank You
???

References:

- Data Communications and Networking " Behrouz A. Forouzan"
- Computer Networks "A. S. Tanenbaum" Fifth Edition
- Data and Computer Communications "William Stallings" Tenth Edition.