UNIT V

CRYPTOGRAPHY & DIGITAL SIGNATURE

What happens in real life?

- We have universal electronic connectivity via networks of our computers so allowing viruses and hackers to do eavesdropping.

- So both the organizations and individuals need to protect data and resources from such disclosure.

Goals of network security

- **Authentication -** assurance that the communicating entity is the one that it claims to be.
- **Access Control -** prevention of the unauthorized use of a resource.
- **Data Confidentiality** –protection of data from unauthorized disclosure.
- **Data Integrity -** assurance that data received is as sent by an authorized entity.
- **Non-Repudiation** - protection against denial(disagreement) by one of the parties in a communication.

Cryptography

- The term Cryptography is related to the **ideas and techniques** to avoid such network generated problems.
- cryptography is the study of
  - **secret** (crypto-)
  - **writing** (-graphy)

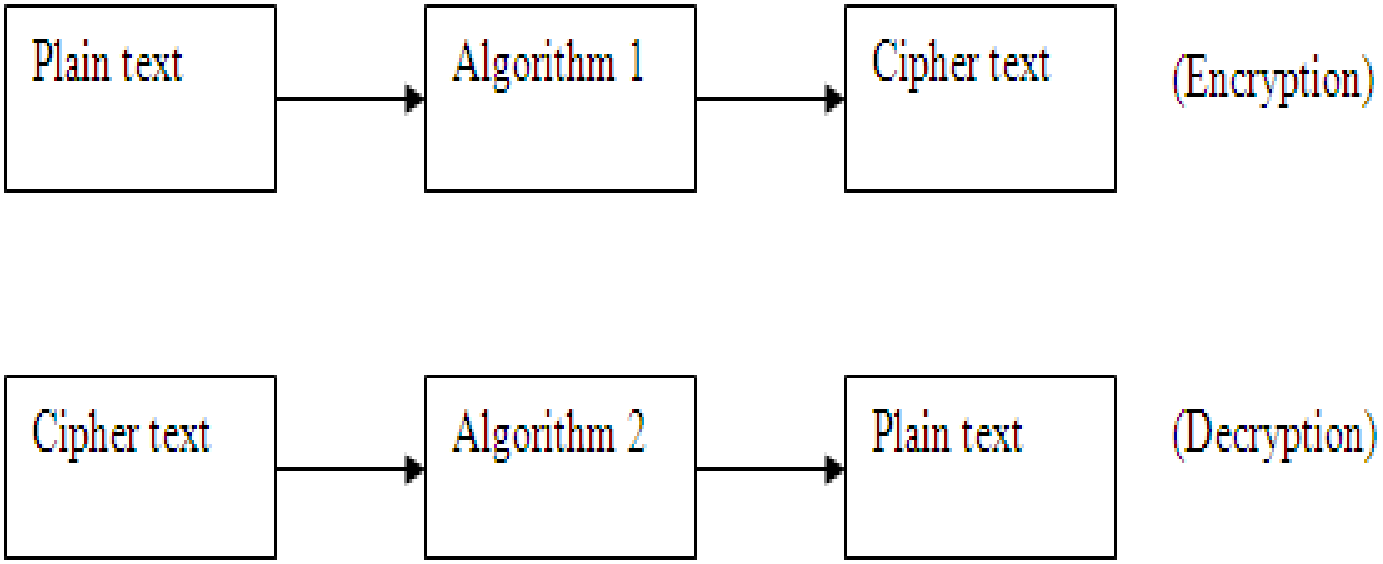
Definition

- **Cryptography** is the study of message secrecy.
- Cryptography is about communication in the presence of adversaries.
- One of cryptography's primary purposes is hiding the meaning of messages, but not usually their existence.
- Cryptography is used in many applications examples include security of ATM cards, computer passwords, and electronic commerce all depends on cryptography.

Components of Cryptography

- **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key**: The secret key is also input to the encryption algorithm.
- **Cipher text**: This is the scrambled message produced as output.
- **Decryption algorithm**: This is essentially the encryption algorithm run in reverse.

Encryption and Decryption



Plain text: a b c d e f g h I j k l m n o p r s t u v w x y z
Cipher text: q w e r t y u i o p a s d f g h j k l z x c v b n m

Basic Terminology

- **Plaintext** - the original message
- **Cipher text** - the coded message
- **Cipher** - algorithm for transforming plaintext to cipher text
- **key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to cipher text
- **Decipher (decrypt)** - recovering plain text from ciphertext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)** - the study of principles/ methods of deciphering cipher text *without* knowing key
- **Cryptology** - the field of both cryptography and cryptanalysis
- **Cryptogram(Cipher Text)**

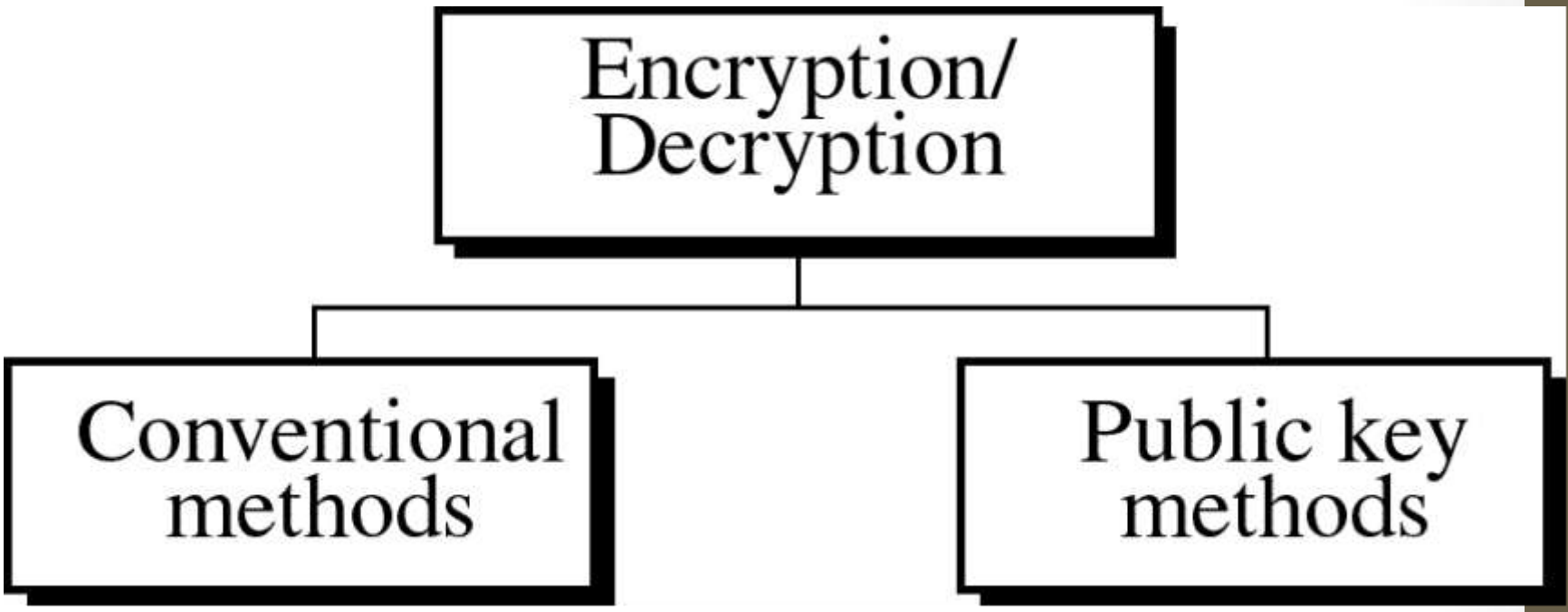
Security attacks

- **Passive attacks(passive intruder**)

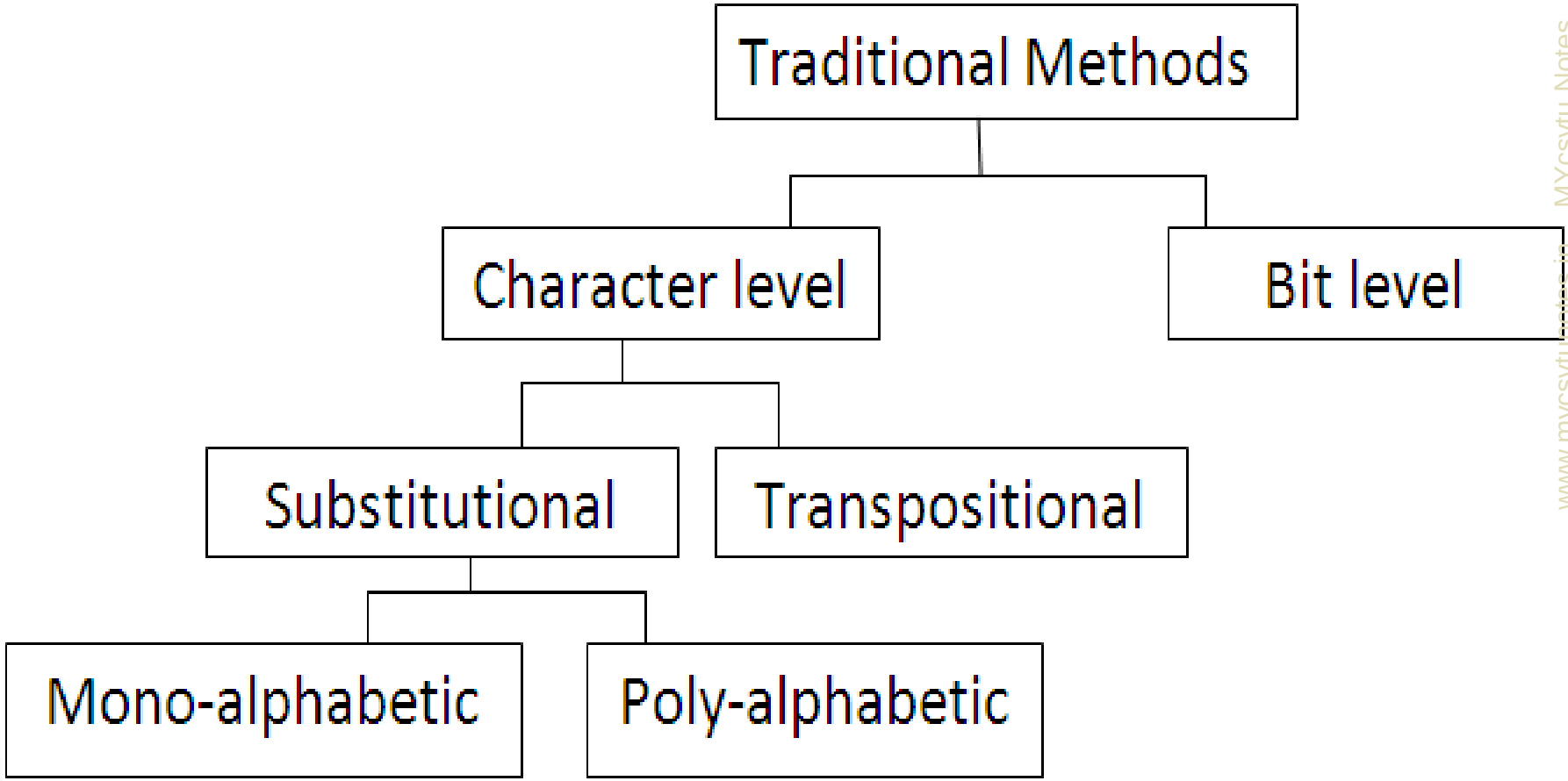
  It attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent is to obtain information that is being transmitted.

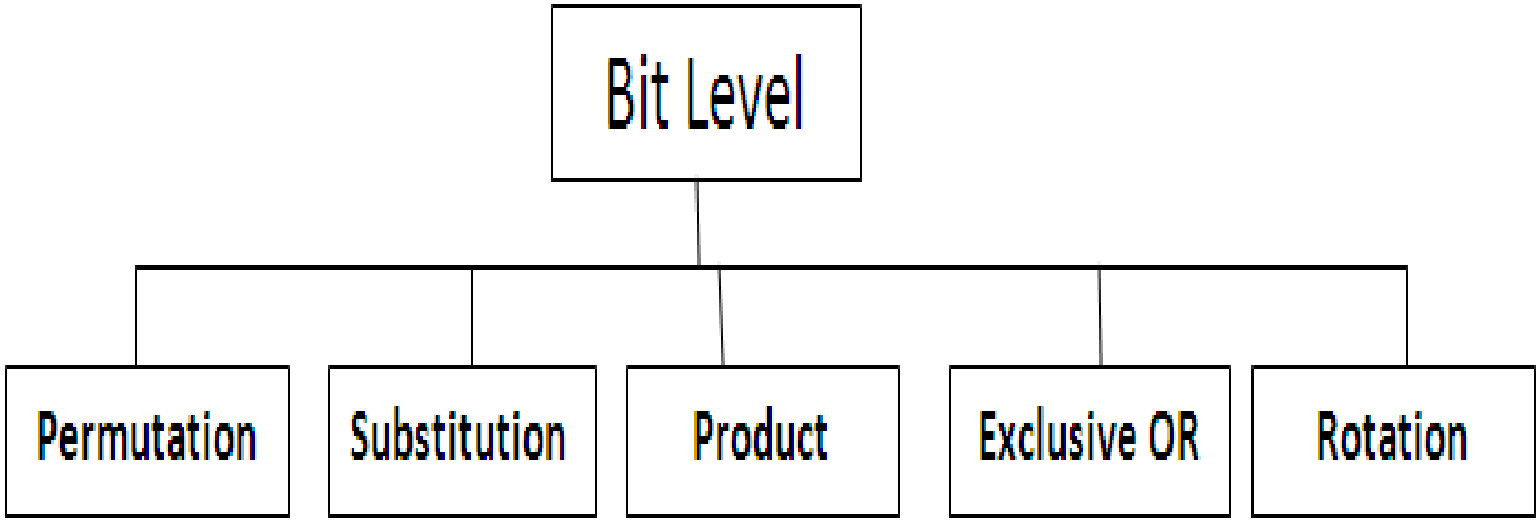
- **Active attacks (active intruder)**

  It attempts to alter system resources or affect their operation by modification of data stream or by the creation of a false stream.



Conventional methods/Traditional Method





Substitution

- Each letter or group of letters is replaced by another letter or group to disguise it. Example: mono-alphabetic substitution.
- For Eg: We can replace character A with Z, character T with W. If the symbols are digits then we can replace 3 with 7, 2 with 6 and so on.

Mono-alphabetic Substitution

- The ciphers in this substitution section replace each letter with another letter according to the cipher alphabet.
- Ciphers in which the cipher alphabet remains unchanged throughout the message are called Mono-alphabetic Substitution Ciphers.

Example

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

"meet me at nine." would become "pxxe px ye jmjx."

Poly-alphabetic Substitution:

- In this method each occurrence of a character can have a different substitute. The relationship between the character in the plain text to the character in the cipher text is one to many.
- **The Vigenere Tableau**

	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

Example

- “TO BE OR NOT TO BE THAT IS THE QUESTION”
- Using the keyword RELATIONS.

Keyword:	RELAT IONSR ELATI ONSRE LATIO NSREL
Plaintext:	TOBEO RNOTT OBETH ATIST HEQUE STION
Ciphertext:	KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Transposition

- It reorder the letters but do not disguise them.

Example:Please transfer one million dollars to my swiss bank account

Transposition cipher

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

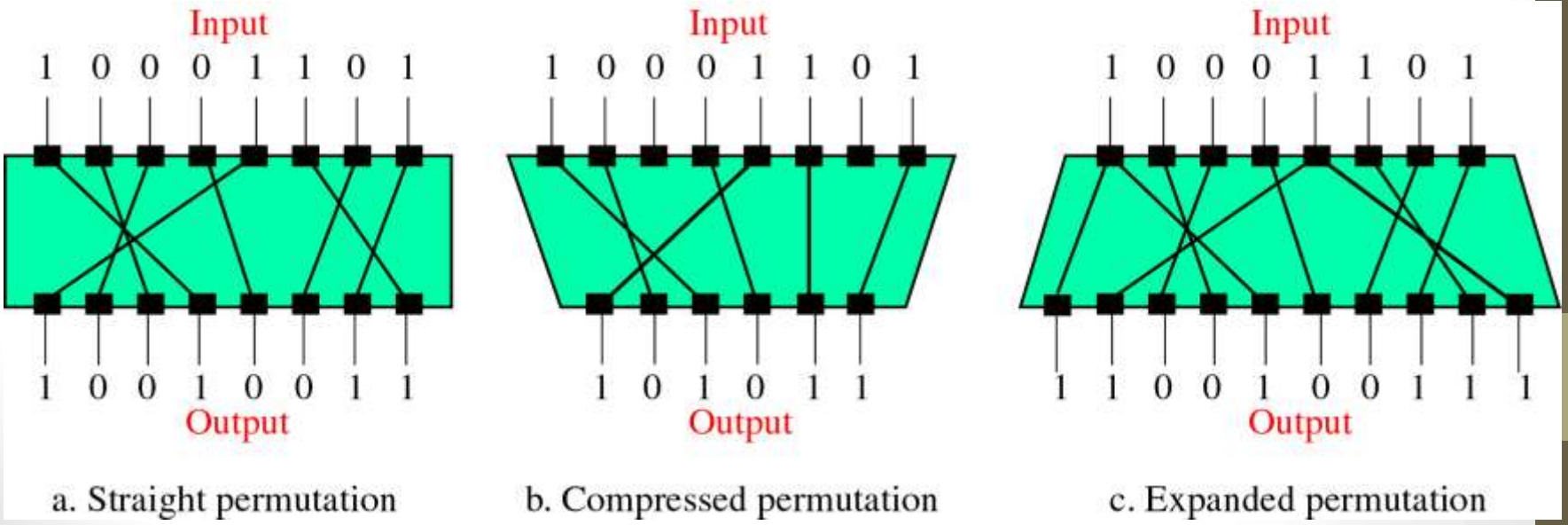
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Bit level encryption

- Permutation (P-box)
- Substitution (S-Box)
- Product
- Exclusive-OR
- Rotation

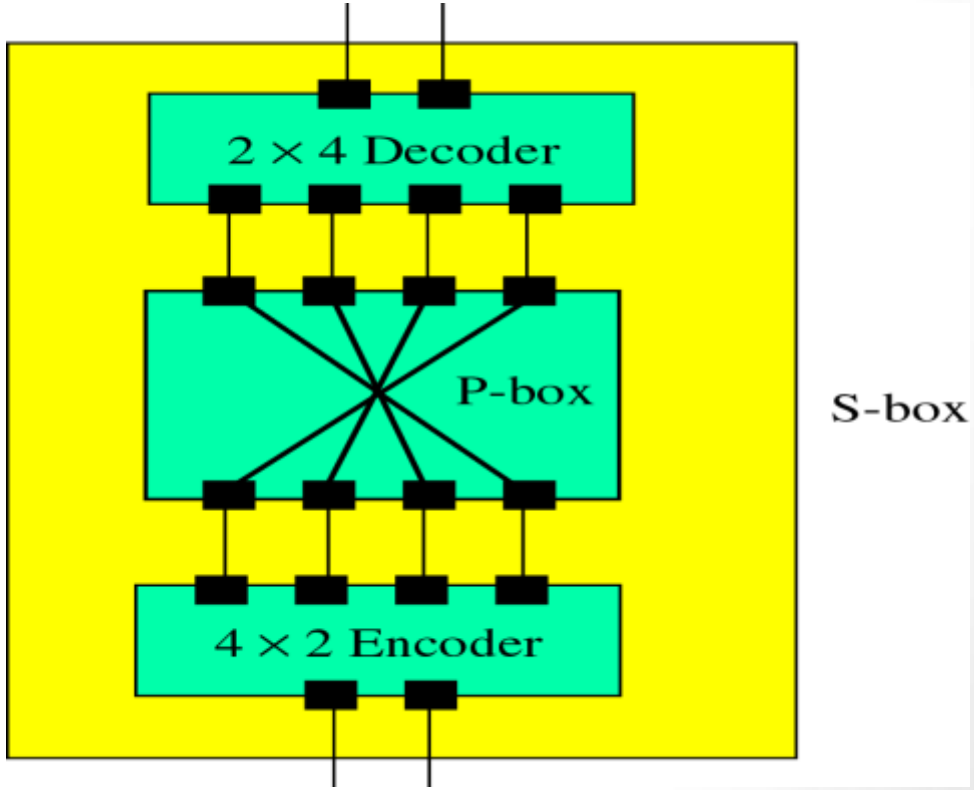
Permutation

- A permutation can easily be performed by creating a hardware circuit with internal wiring so that operations can be performed very quickly. These units are referred to as a P-Boxes.



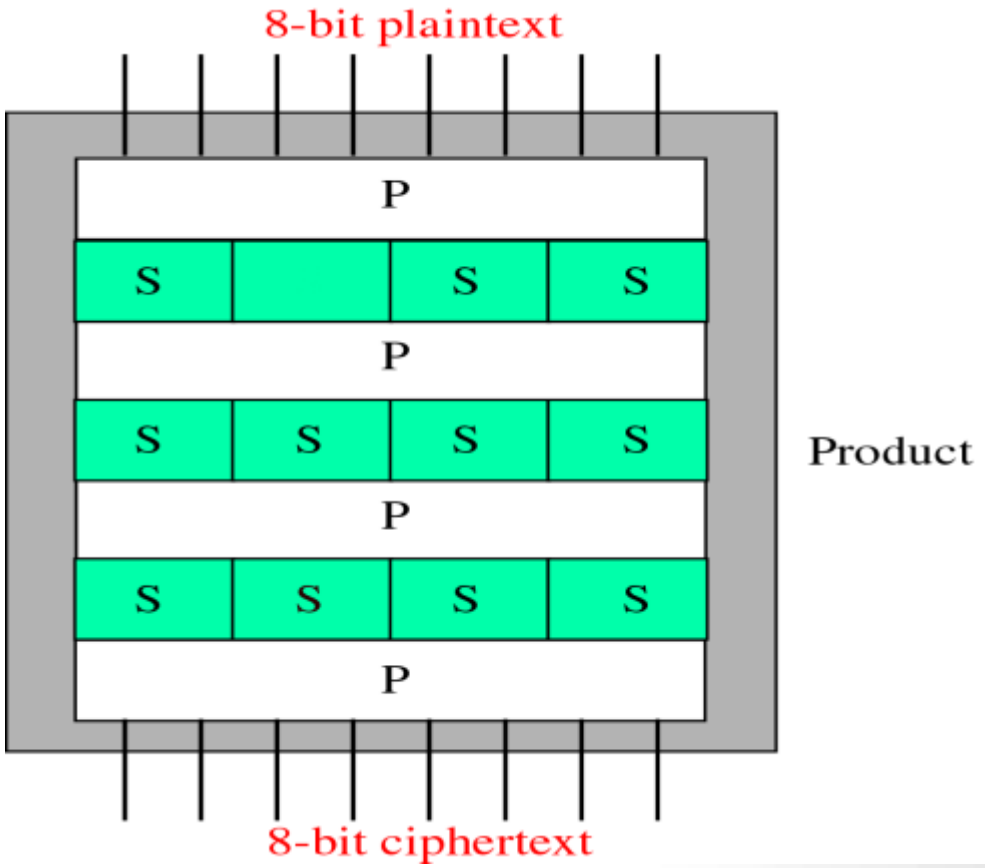
Substitution

- Substitution of n bits can be achieved by using the combination of :
  - Decoder
  - Encoder



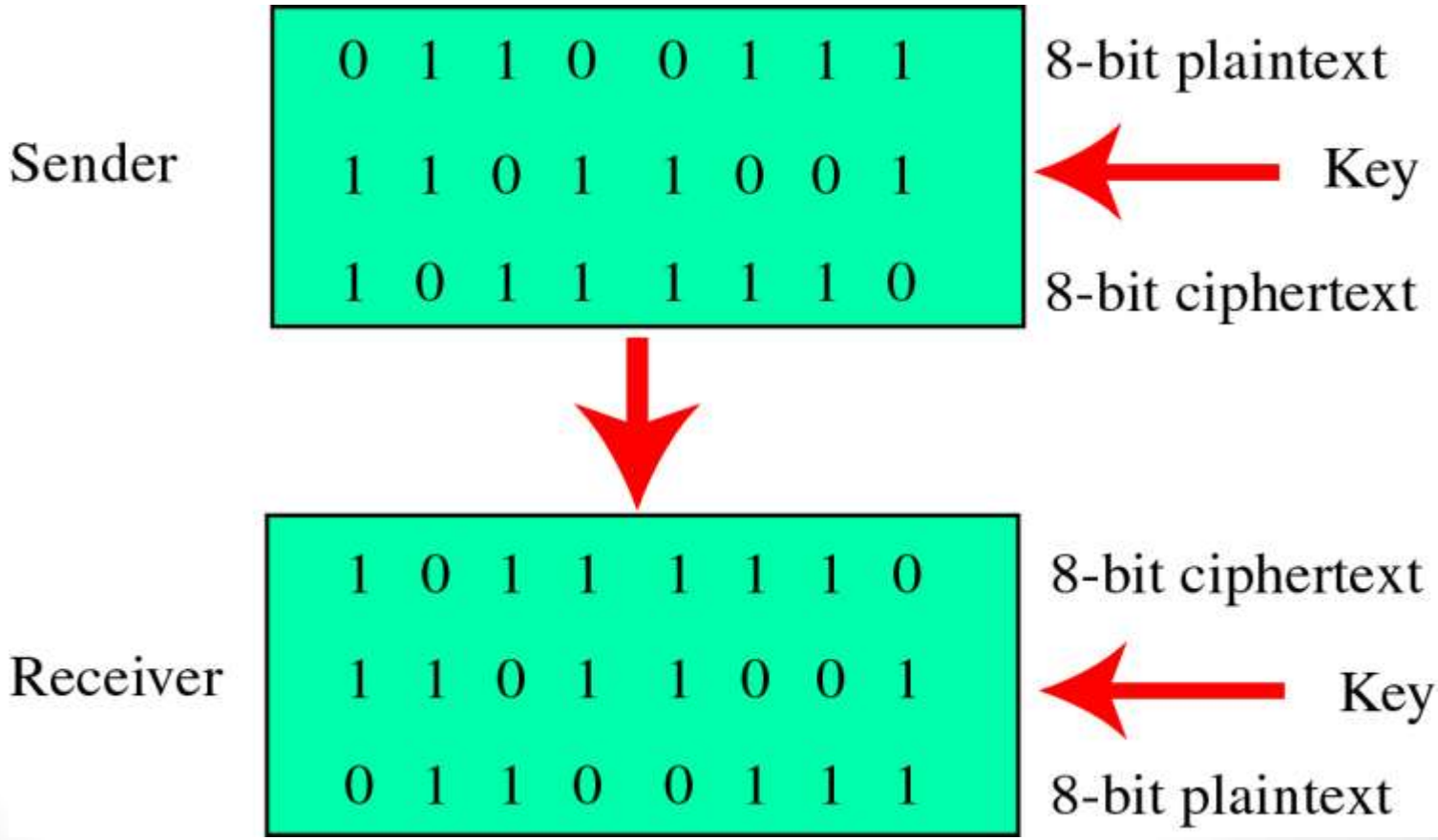
Product

- The P-Boxes & S-Boxes can be combined and called a product.



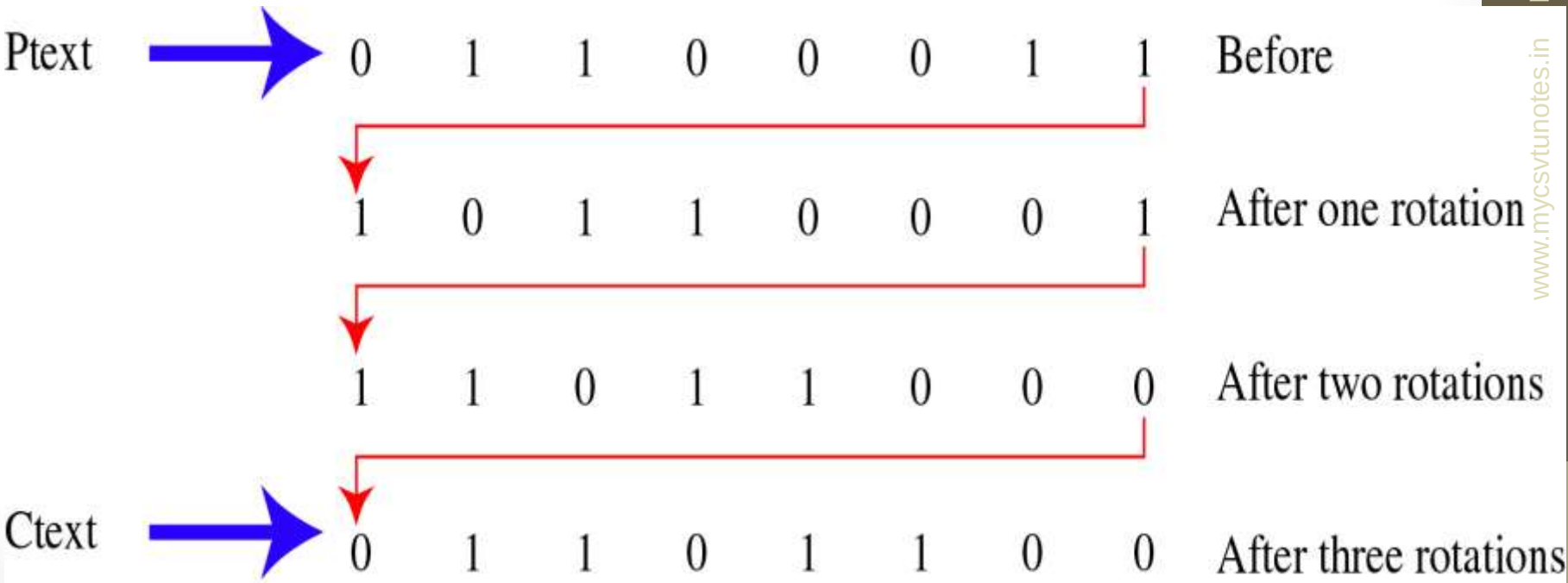
Exclusive-OR

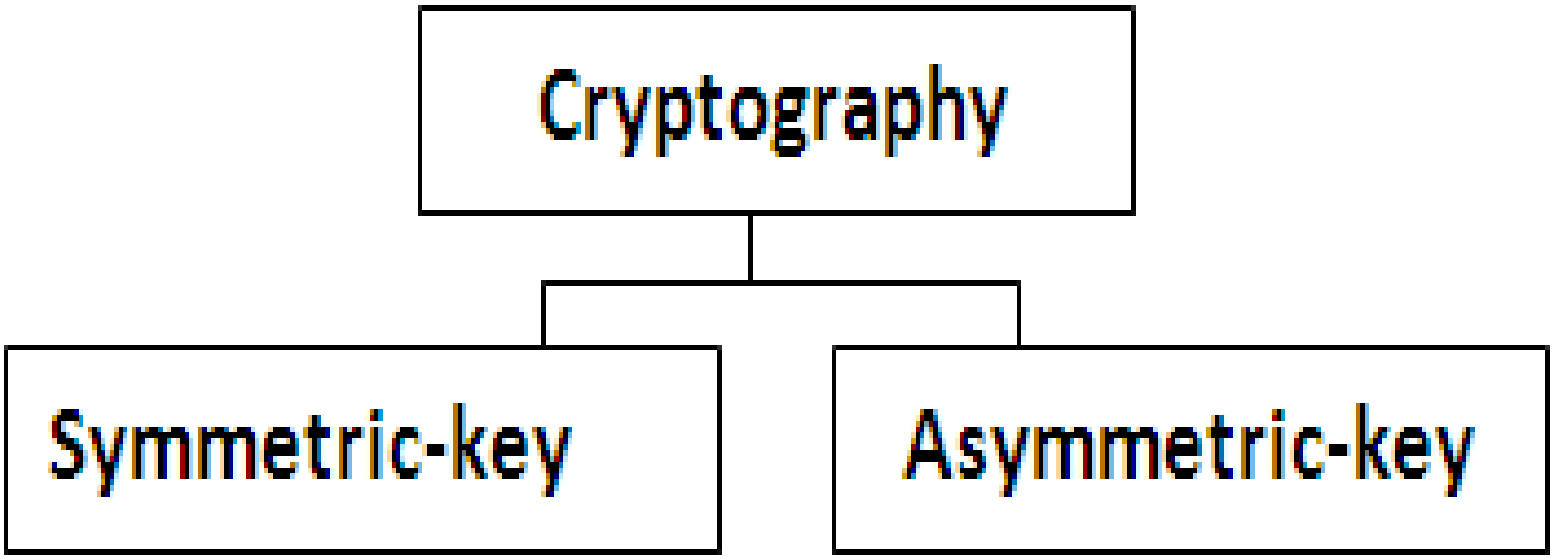
- In this method the plaintext value are exclusive-ORed with the key value and the output will be the cipher text:



Rotation

- To encrypt the bit pattern we can also rotate the bits to the right or to the left.



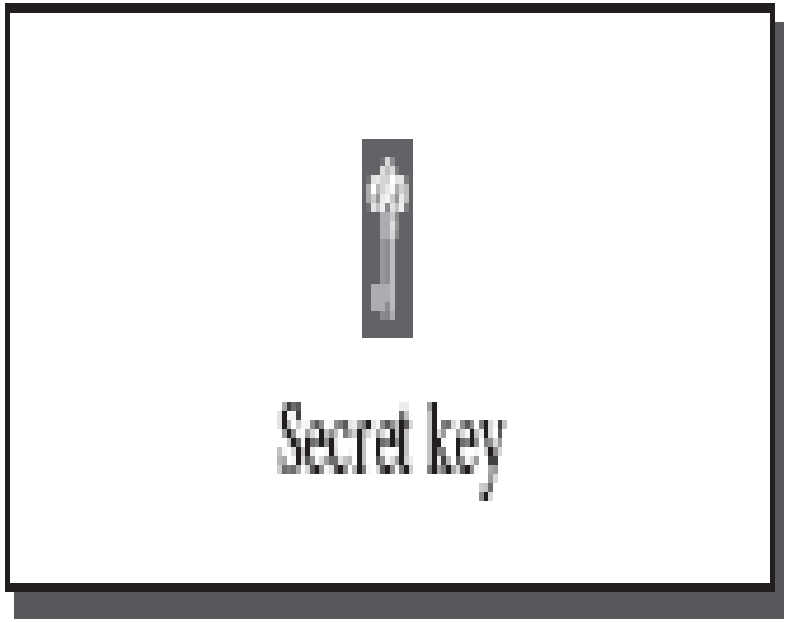


Secret-key

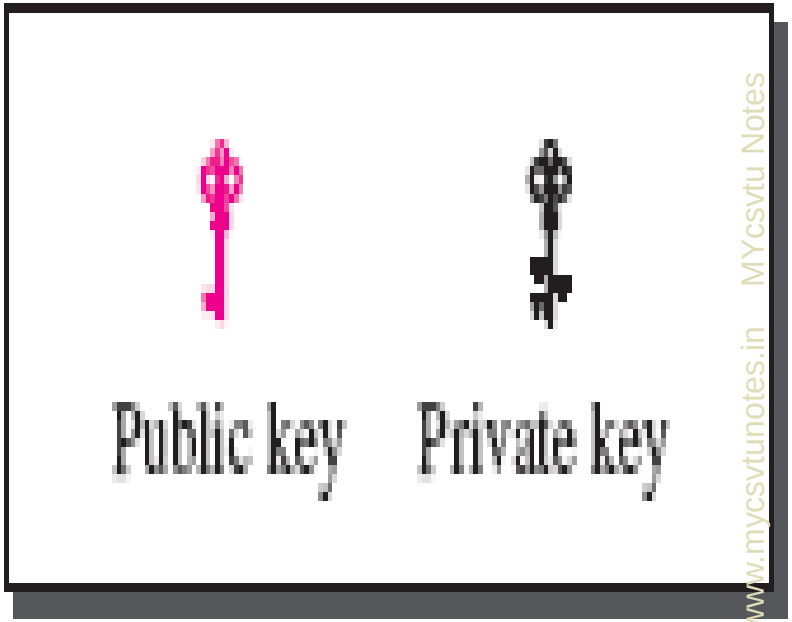
Public-key

Types of Encryption/Cryptography

- **Symmetric (Single/secret/private/shared/one key)**
- **Asymmetric (Two key/public key)**



Symmetric-key cryptography

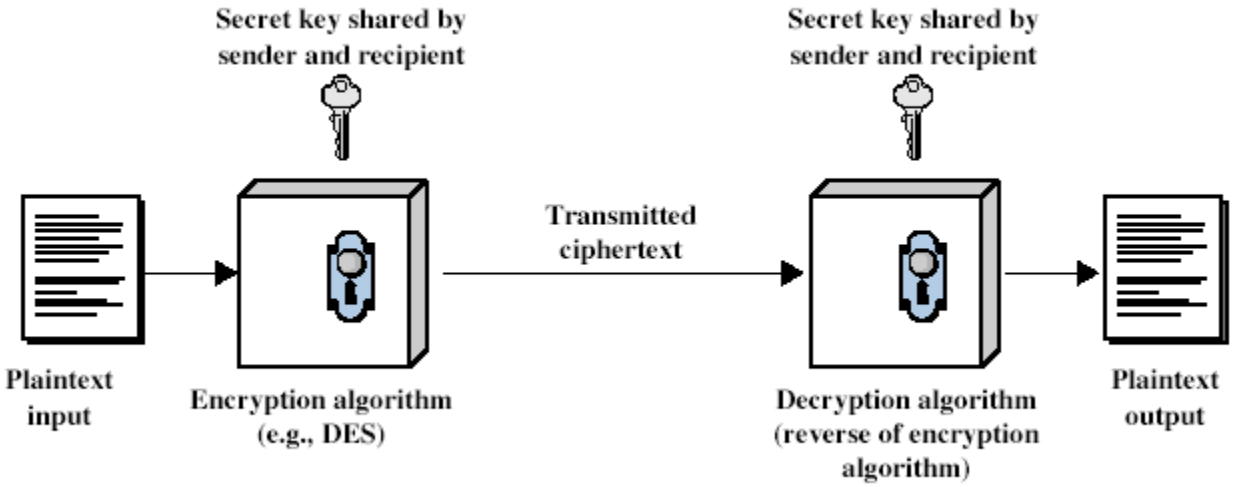


Asymmetric-key cryptography

Symmetric key Method

- Symmetric key Method uses same key, called secret key, for both encryption and decryption.
- Message encrypted with a secret key can be decrypted only with the same secret key.
- The algorithm used for symmetric key encryption is called secret-key algorithm.
- The major vulnerability of secret-key algorithm is the need for sharing the secret-key.
- One solution is to securely send the secret-key from one end to other end.
- Strength of the symmetric key encryption depends on the size of the key used.
- DES is the symmetric key encryption.

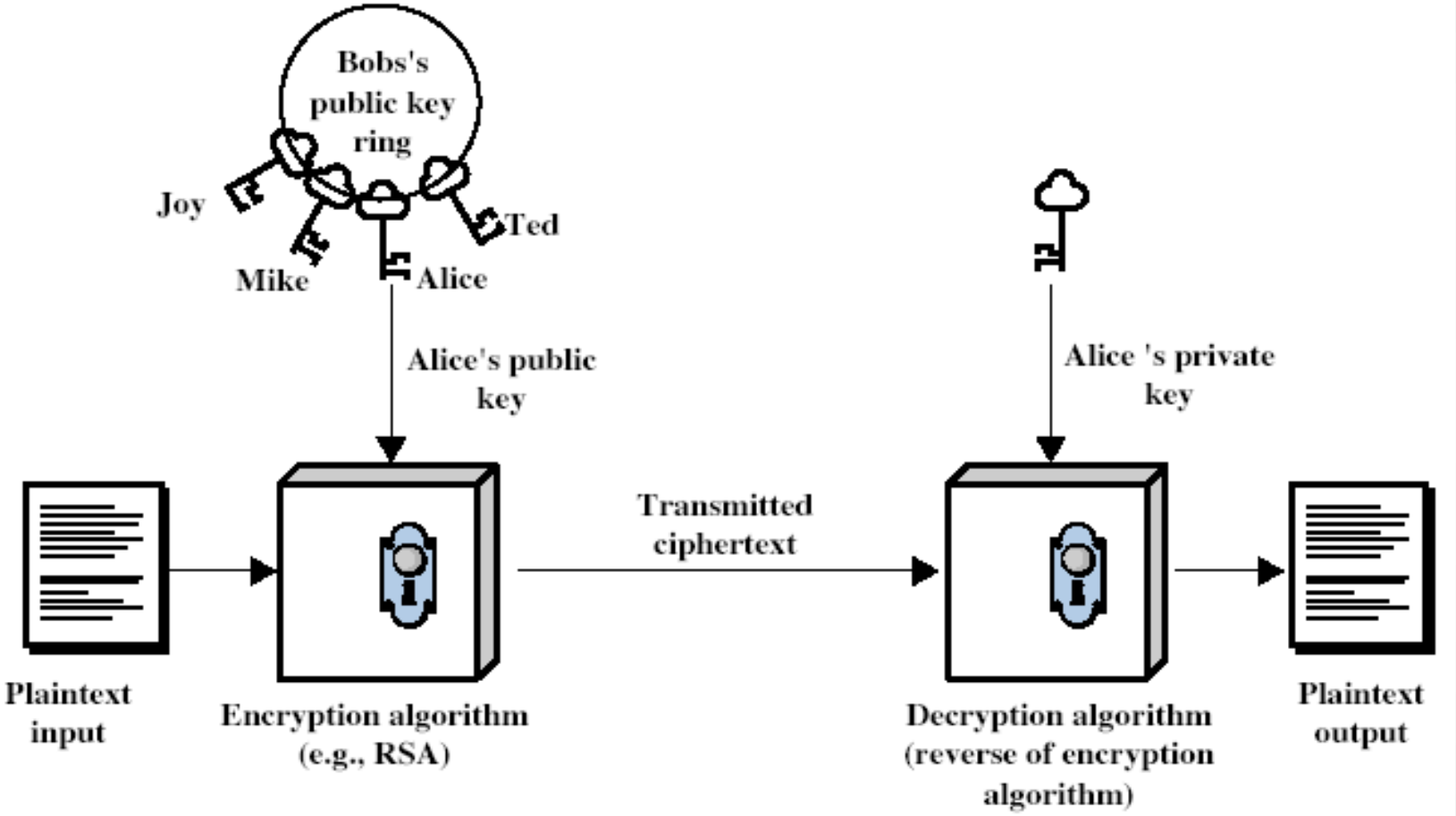
Symmetric key Model



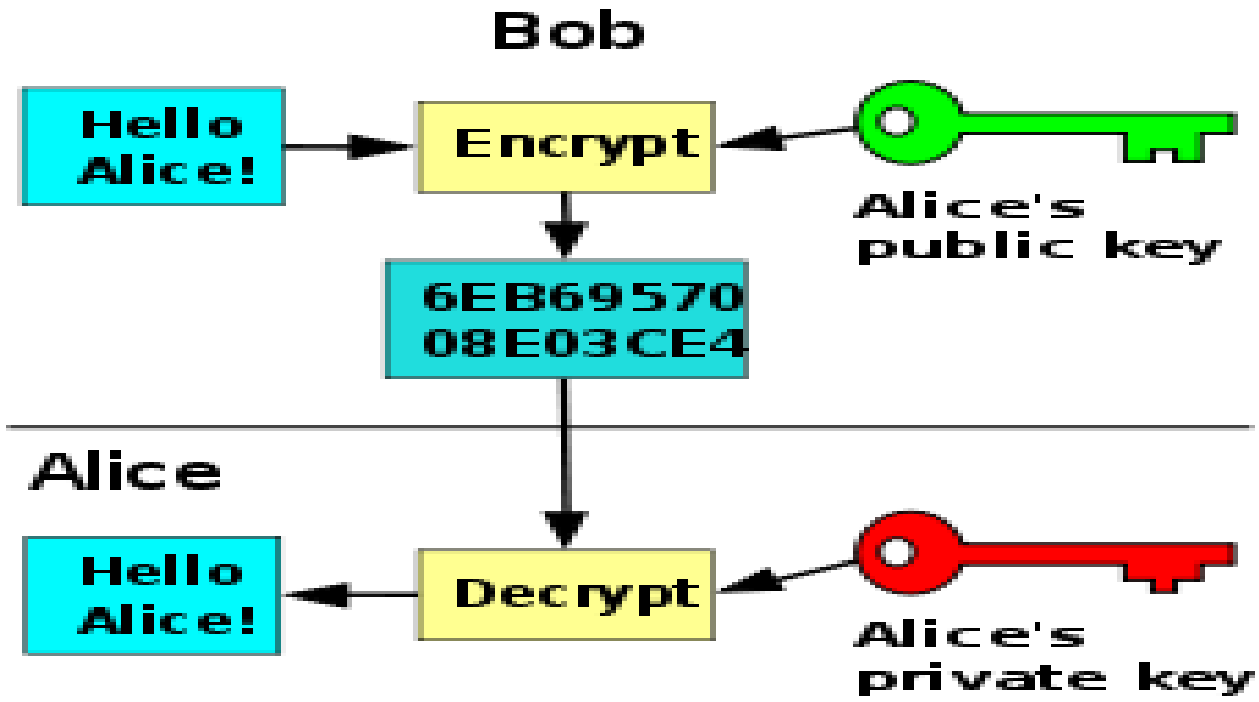
Asymmetric key Method

- Asymmetric key method uses different keys for encryption and decryption.
- These two keys are mathematically related and they form a key pair.
- One of these two keys should be kept private, called private-key, and the other can be made public, called public-key. Hence this is also called Public Key Encryption.
- Popular private-key algorithms are RSA (invented by Rivest, Shamir and Adlemen) and Diffie-Hellman.

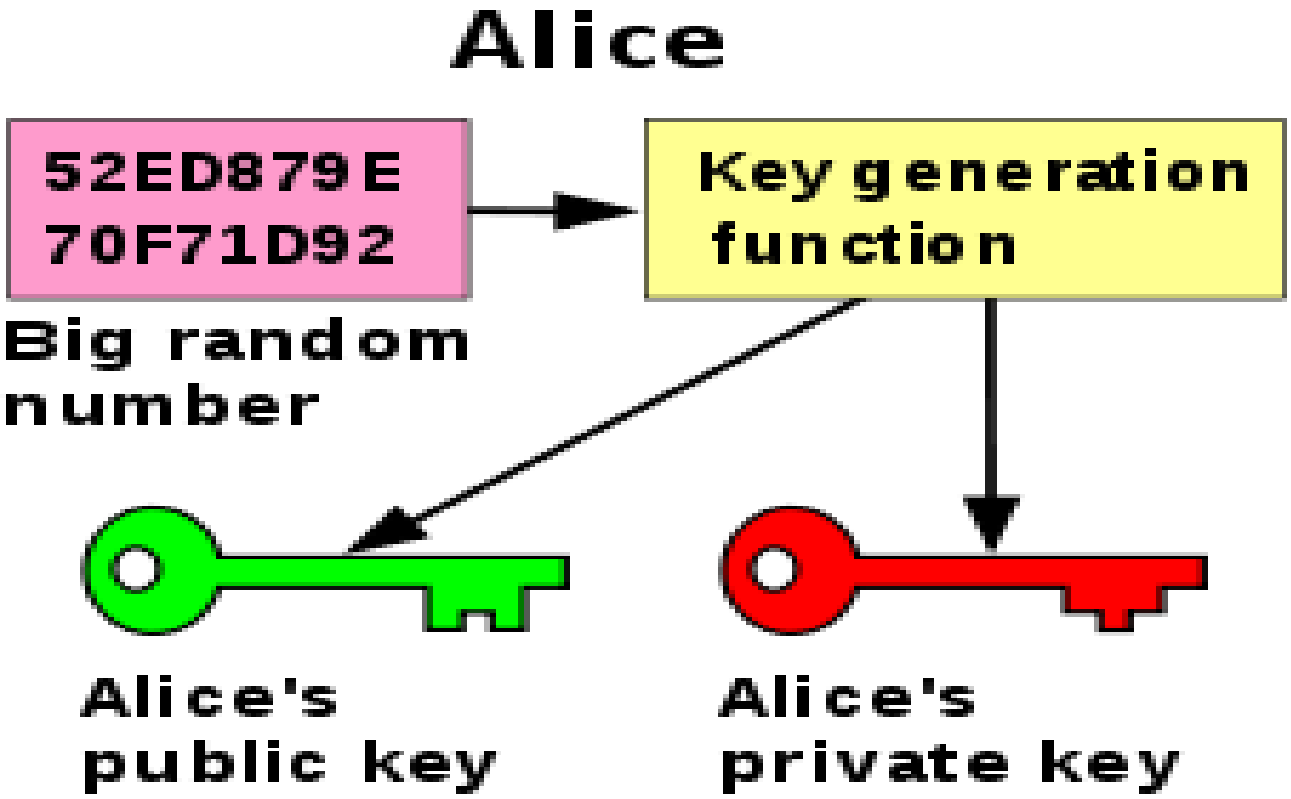
Asymmetric key encryption



Asymmetric key encryption



Key Generation



Data Encryption Standard (DES)

- DES (Data Encryption Standard) was designed by IBM.
- **Plain text =64 bits**
- **Cipher text= 64 bits**
- **Key = 56 bits**
- 56 bits key generate 16 different sub keys (48 bits).
- **Distinct stages=19.**
- The first stage is a key-independent transposition on the 64-bit plaintext.
- The last stage is the exact inverse of this transposition.
- The stage prior to the last one exchanges the leftmost 32 bits with the rightmost 32 bits.
- The remaining 16 stages are functionally identical but are parameterized by different functions of the key.

64 bits

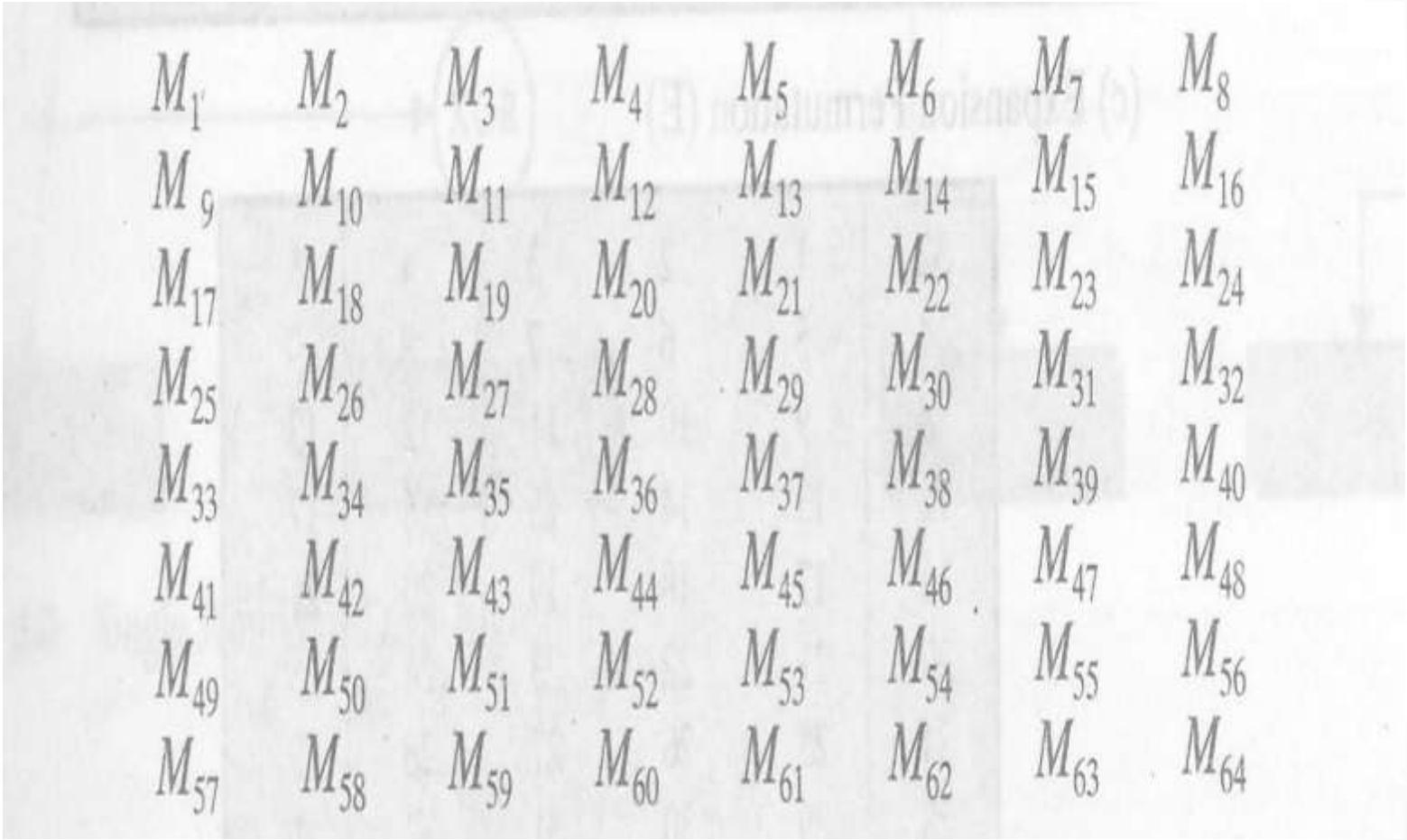


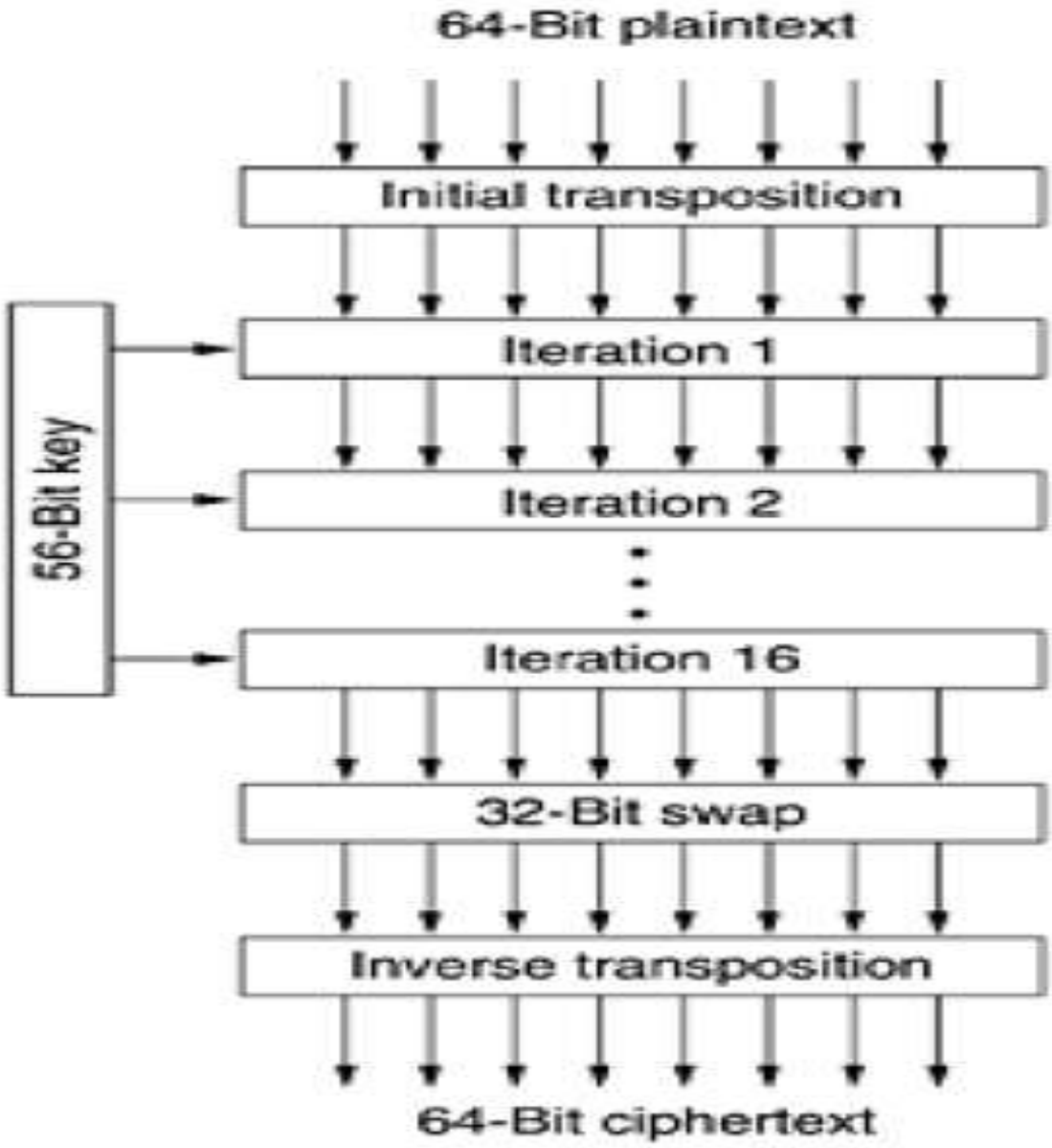
Table 3.2 Permutation Tables for DES

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

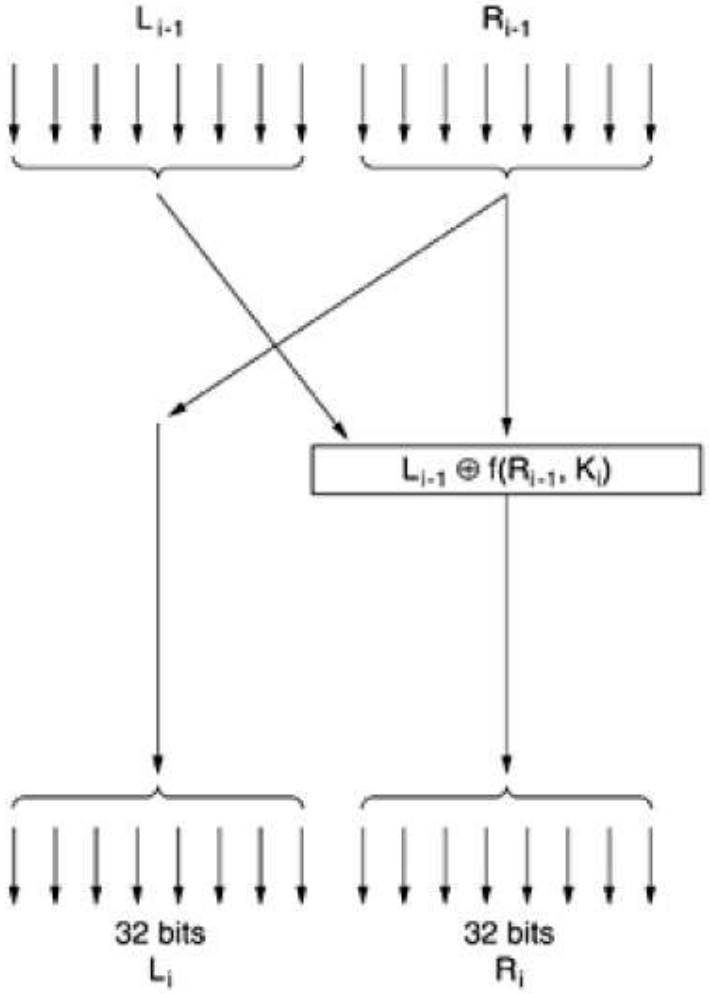
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



Detail of one iteration

- Each stage takes two 32-bit inputs and produces two 32-bit outputs.
- The left output is simply a copy of the right input.
- The right output is the bitwise XOR of the left input and a function of the right input and the key for this stage, *Ki.*
- All the complexity lies in this function.

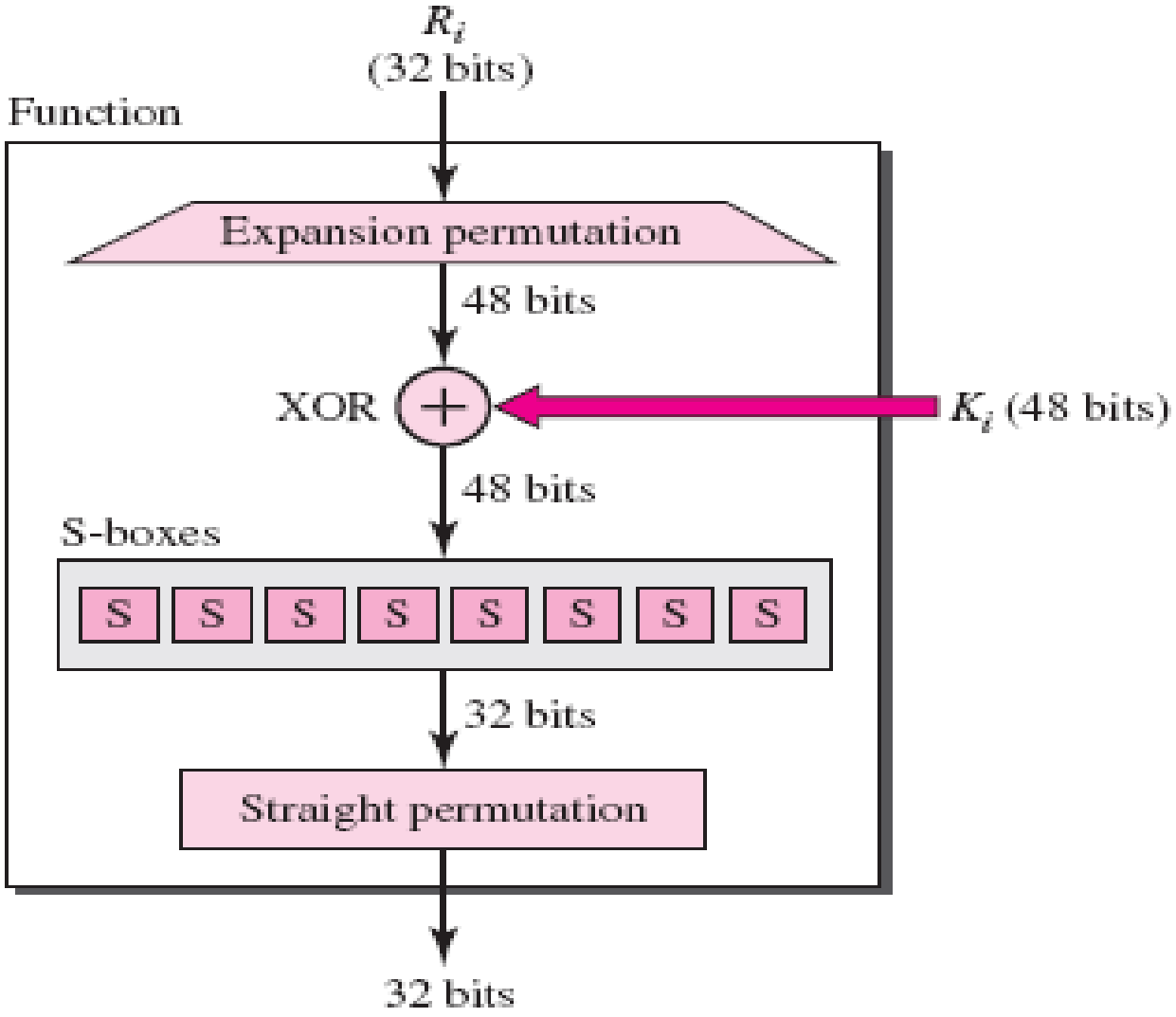
Round (iteration)



Function

- The function consists of four steps, carried out in sequence.
- First, a 48-bit number, E, is constructed by expanding the 32-bit $R_{i-1.}$
- 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 6 inputs to an S-box is mapped onto a 4-bit output.
- Finally, these 8 x 4 bits are passed through a P-box.

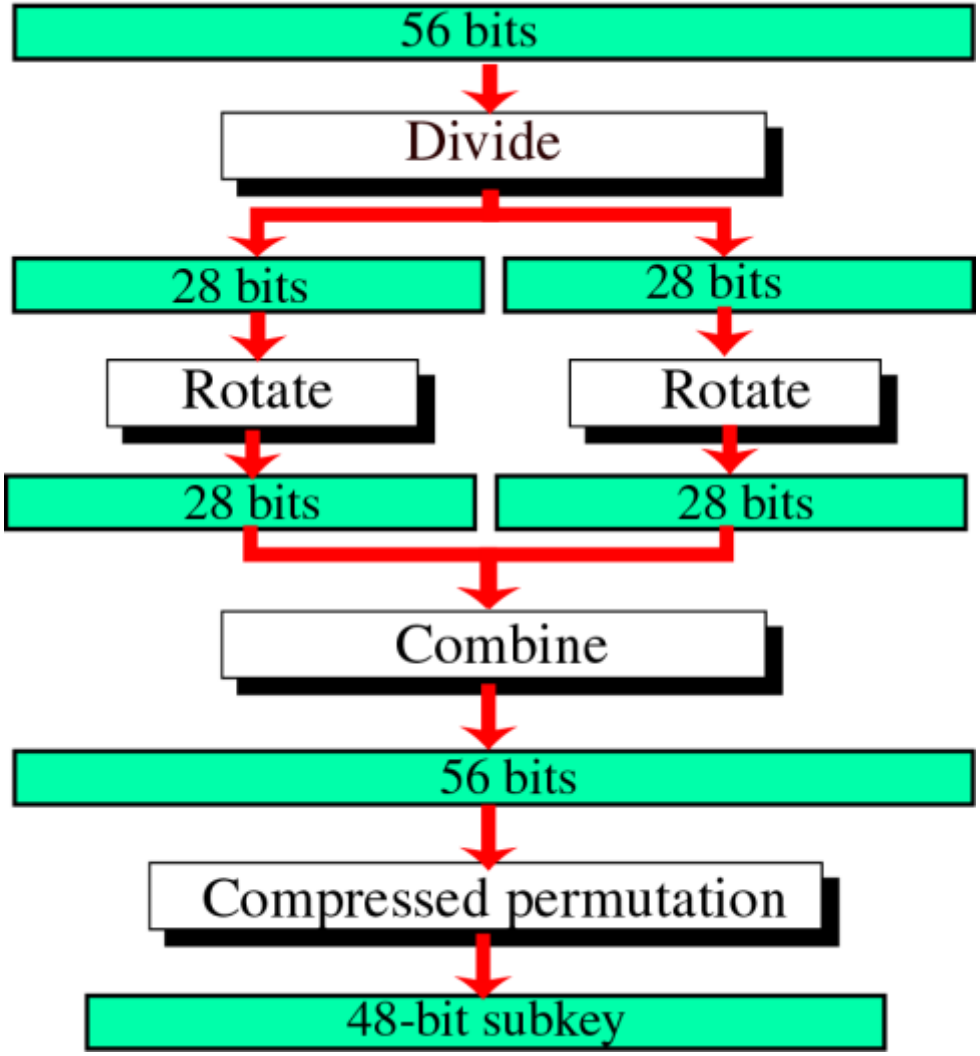
Function Defines



Sub-key generation

- 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.
- K_i is derived from this rotated key by applying yet another 56-bit transposition to it.
- A different 48-bit subset of the 56 bits is extracted and permuted on each round.

Subkey Generation in DES



Whitening

- A technique that is sometimes used to make DES stronger is called **whitening.**
- **It consists of** XORing a random 64-bit key with each plaintext block before feeding it into DES and then XORing a second 64-bit key with the resulting cipher text before transmitting it.
- Whitening can easily be removed by running the reverse operations (if the receiver has the two whitening keys).
- Since this technique effectively adds more bits to the key length, it makes exhaustive search of the key space much more time consuming.
- Note that the same whitening key is used for each block (i.e., there is only one whitening key).

Double DES

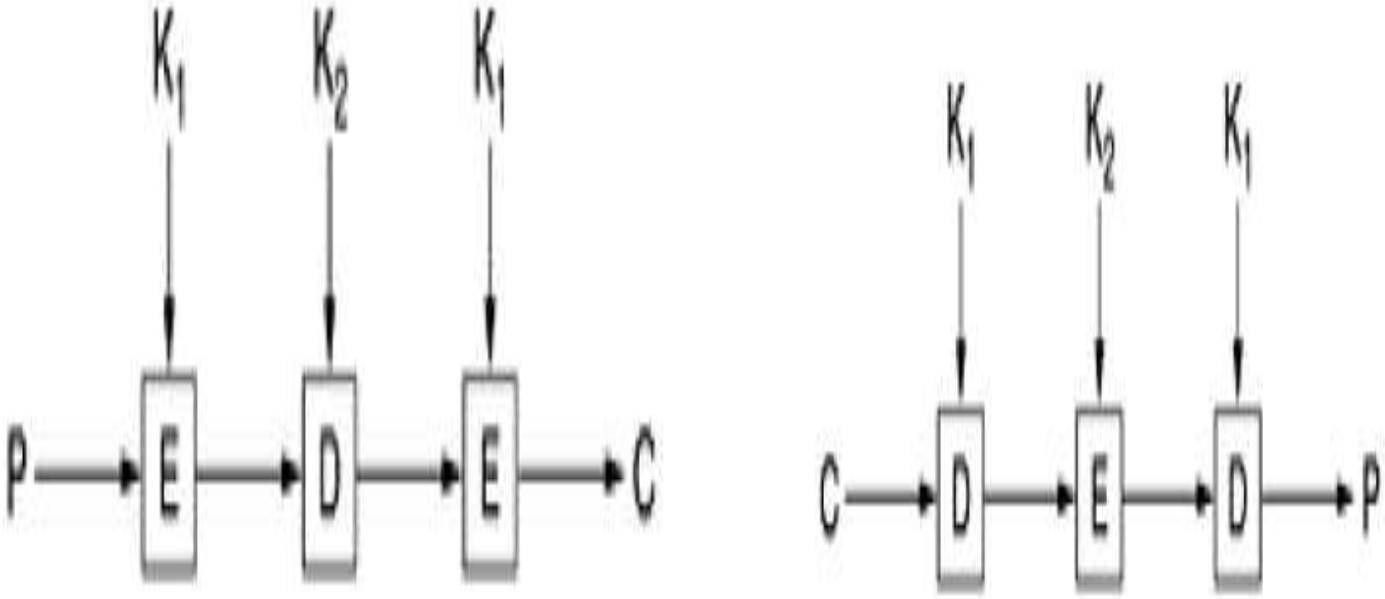
- Multiple encryption with DES and multiple keys gave the answer to many of the shortcomings of DES.
- The simplest form of multiple encryption has two encryption stages and two keys.
- Given a plaintext P and two encryption keys K_1 and K_2, cipher text C is generated as

$$C = E (K_2, E (K_1, P))$$

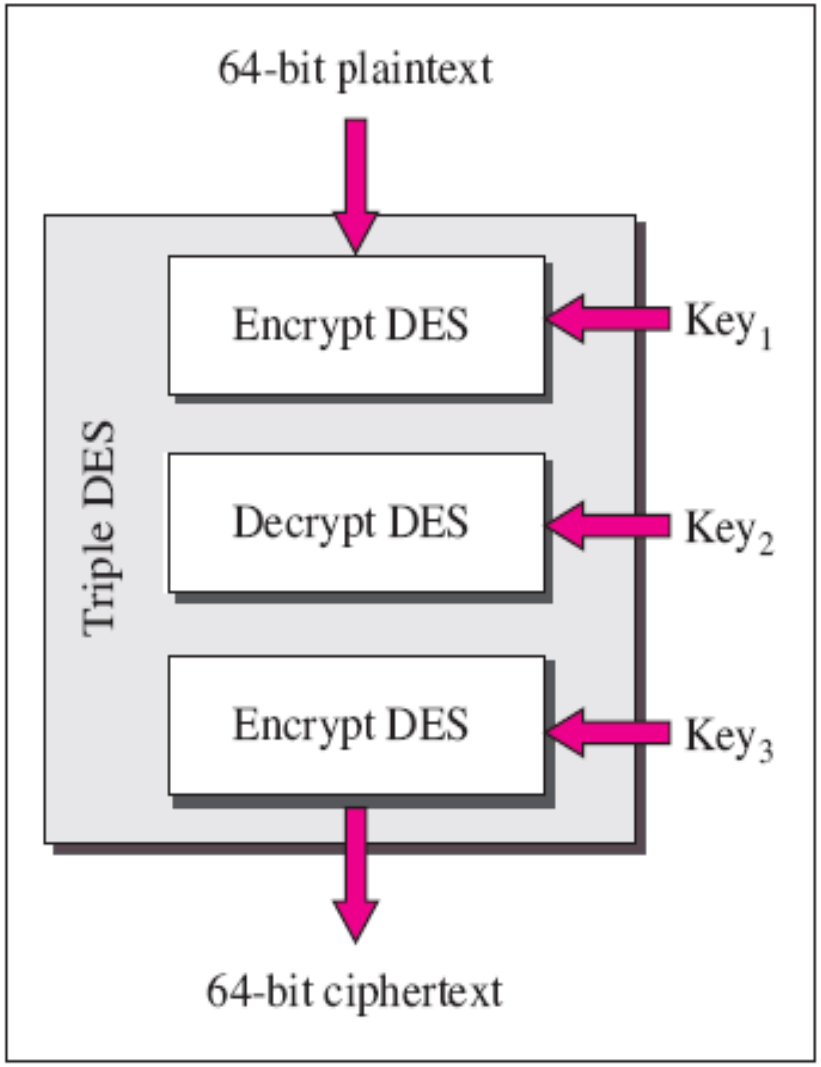
- Decryption requires that the keys be applied in reverse order:

$$P = D (K_1, D(K_2, C))$$

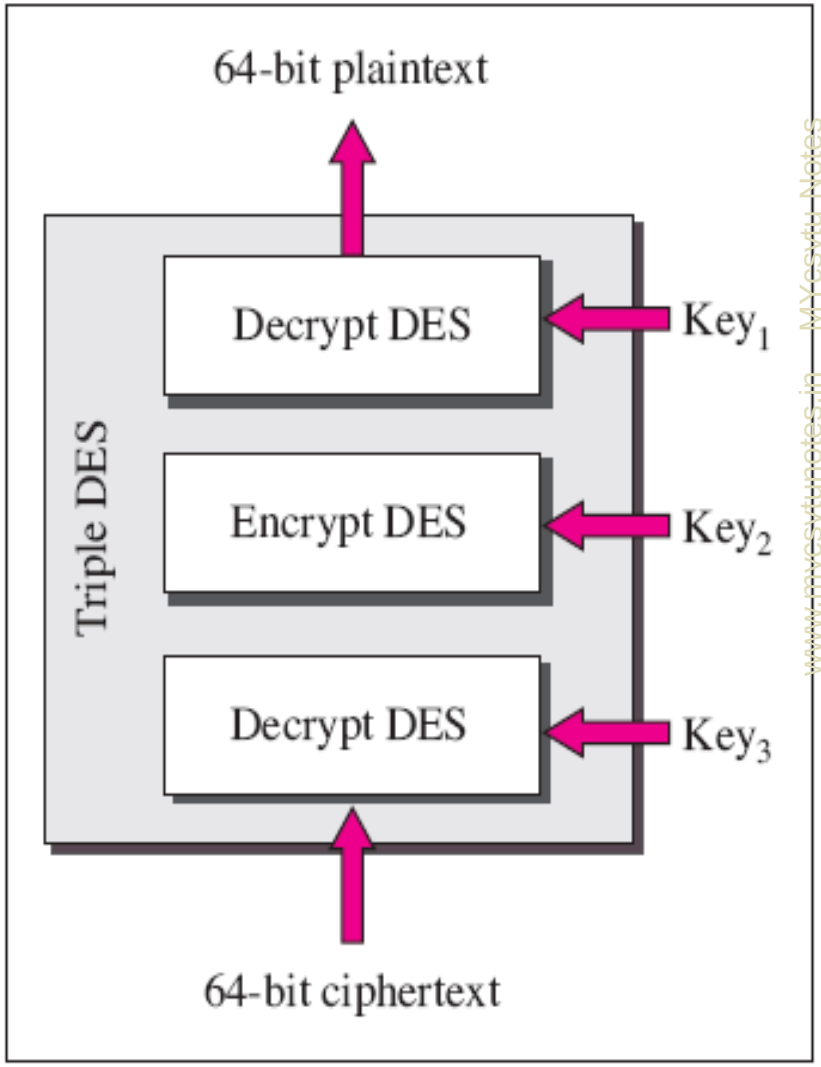
Triple DES with two key



Triple DES with three key



a. Encryption Triple DES



b. Decryption Triple DES

RSA

- Developed by Rivest, Shamir & Adleman in 1977 and first published in 1978.
- The best known & widely used public-key encryption.

Key Generation

1. Select p, q — p and q both prime, $p \neq q$
2. Calculate $n = p \times q$
3. Calculate $z=(p-1)(q-1)$
4. Select integer e — $GCD(z, e)=1;\ 1 < e < z$
5. Calculate d — $e \times d = 1 \bmod z$
6. Public key — $PU= \{e, n\}$
7. Private key — $PR= \{d, n\}$

Encryption

- Plaintext: $M < n$
- Cipher text: $C=M^e \bmod n$

Decryption

- Cipher text: C
- Plaintext: $M=C^d \bmod n$

How RSA algorithm works

- we have chosen

p = 3

q = 11

n= p × q = 33

z=(p-1)(q-1) = 20

GCD(z, e)=1; 1 < e < z

GCD(20,e)=1

A suitable value for e is e = 3, since 3 and 20 have no common factors.

Continue…

With these choices, d can be found by solving the equation

$3d = 1 \pmod{20}$, which yields $d = 7$.

$C = P^3 \pmod{33}$.

$P = C^7 \pmod{33}$.

The figure shows the encryption of the plaintext "SUZANNE" as an example.

Modular Arithmetic

- Define **modulo operator** a mod n to be remainder when a is divided by n
- use the term **congruence** for: a ≡ b mod n
  - when divided by *n*, a & b have same remainder
  - eg. 100 = 34 mod 11
- b is called the **residue** of a mod n

Example

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

Receiver's computation

Example

- Select primes: p=17 & q=11
- Compute $n = pq$ =17×11=187
- Compute z=(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= 10×16+1
- Publish public key KU={7,187}
- Keep secret private key KR={23,187}

Diffie-Hellman

- It is a practical method for public exchange of a secret key.
- The purpose of this algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.

Global public elements

- If A and B want to communicate, then they have to agree on two large prime numbers, n and g
- where (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.

key generation

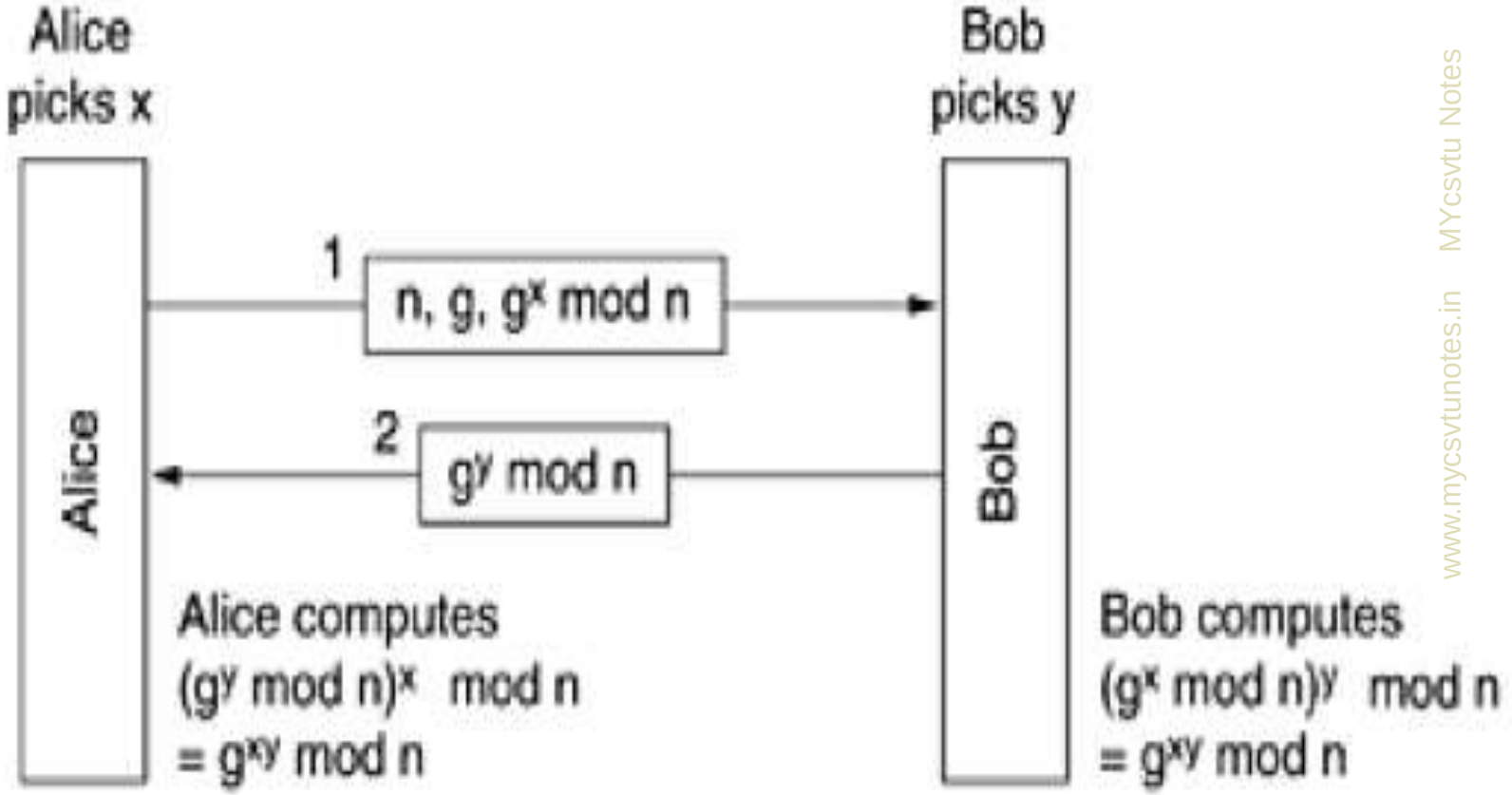
User A

- Select private key X X < n
- Calculate public key $g^X \bmod n$

User B

- Select private key Y Y < n
- Calculate public key $g^Y \bmod n$

The Diffie-Hellman key exchange



Calculation of Secret Key

- $K = (g^Y \bmod n)^X \bmod n = g^{XY} \bmod n$ (User A)
- $K = (g^X \bmod n)^Y \bmod n = g^{XY} \bmod n$ (User B)

Example

n= 47 and g = 3.

Alice picks x = 8

Bob picks y = 10.

Both of these are kept secret.

Alice‘s message to Bob is (47, 3, 3^{8} mod 47=28)

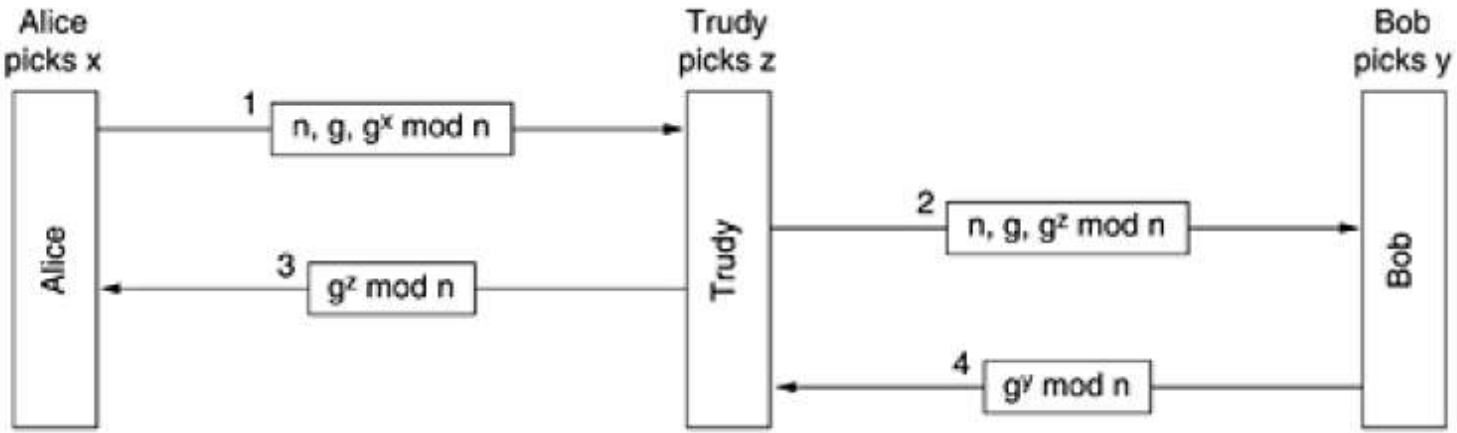
Bob's message to Alice is (3^{10} mod 47=17).

Alice computes 17^{8} mod 47, which is 4.

Bob computes 28^{10} mod 47, which is 4.

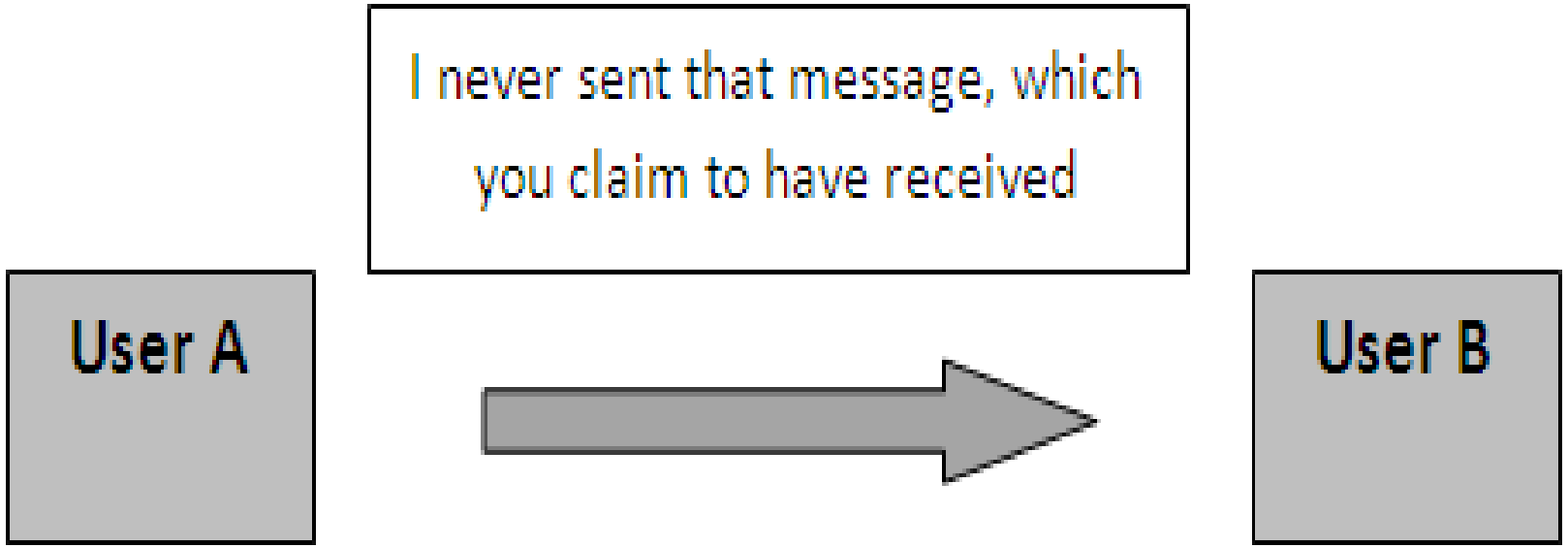
Alice and Bob have independently determined that the secret key is now 4.

The bucket brigade or man-in-the-middle attack

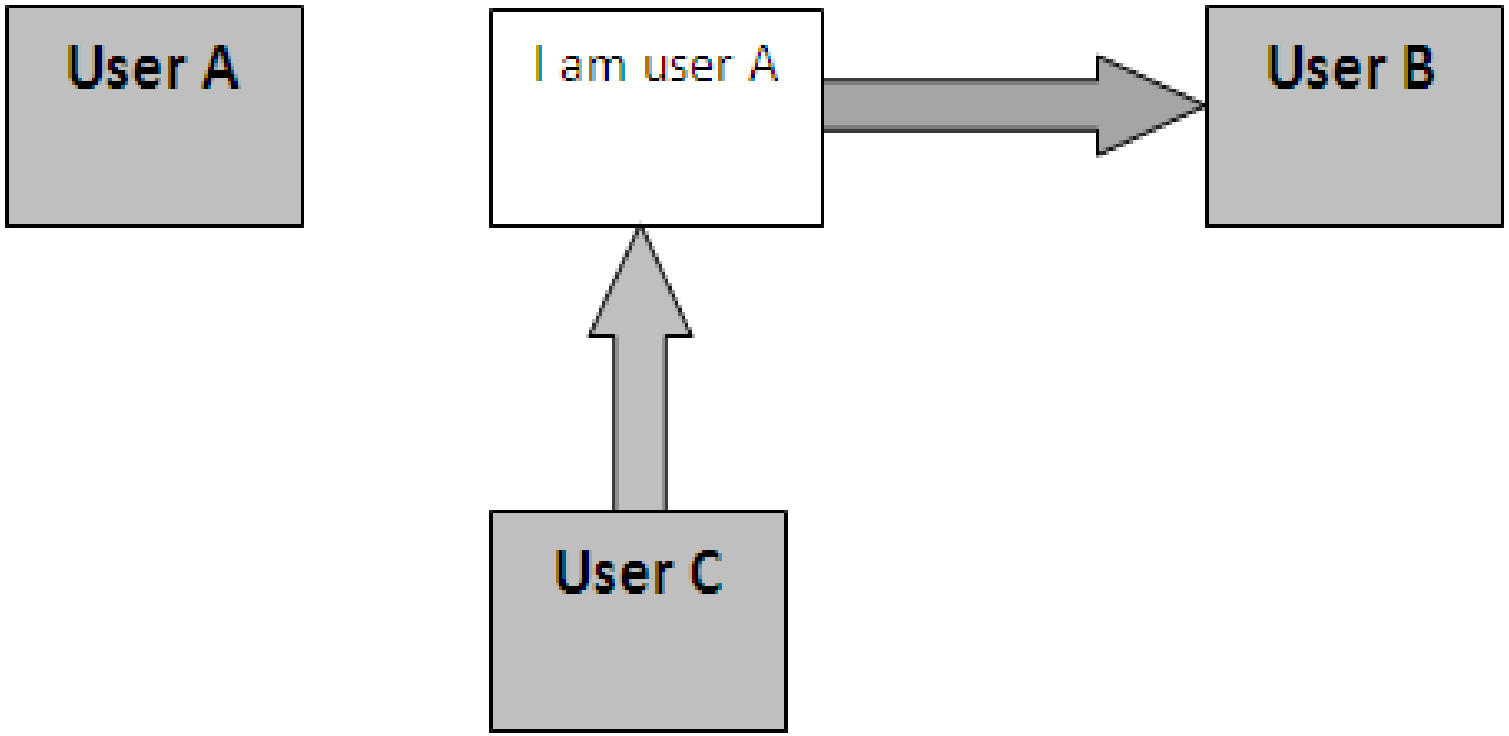


- Alice computes the secret key as $g^{XZ} mod\ n$, *and* so does Trudy (for messages to Alice).
- Bob computes $g^{YZ} mod\ n$ *and so does Trudy (for* messages to Bob).
- Alice thinks she is talking to Bob so she establishes a session key (with Trudy).
- So does Bob.
- Every message that Alice sends on the encrypted session is captured by Trudy, stored, modified if desired, and then (optionally) passed on to Bob.
- Similarly, in the other direction.
- Trudy sees everything and can modify all messages at will, while both Alice and Bob are under the illusion that they have a secure channel to one another.

Non- repudiation



Absence of authentication



Digital Signature

- A signature is a technique for non-repudiation based on the public key cryptography.
- The creator of a message can attach a code, the signature, which guarantees the source and integrity of the message.
- When we send a document electronically, we can also sign it. Here we have 2 choice:
  - Either we can sign the entire document
  - or we can sign the digest or condensed version of the document.

Digital signatures provide the ability to

- verify author, date & time of signature.
- authenticate message contents at the time of signature.

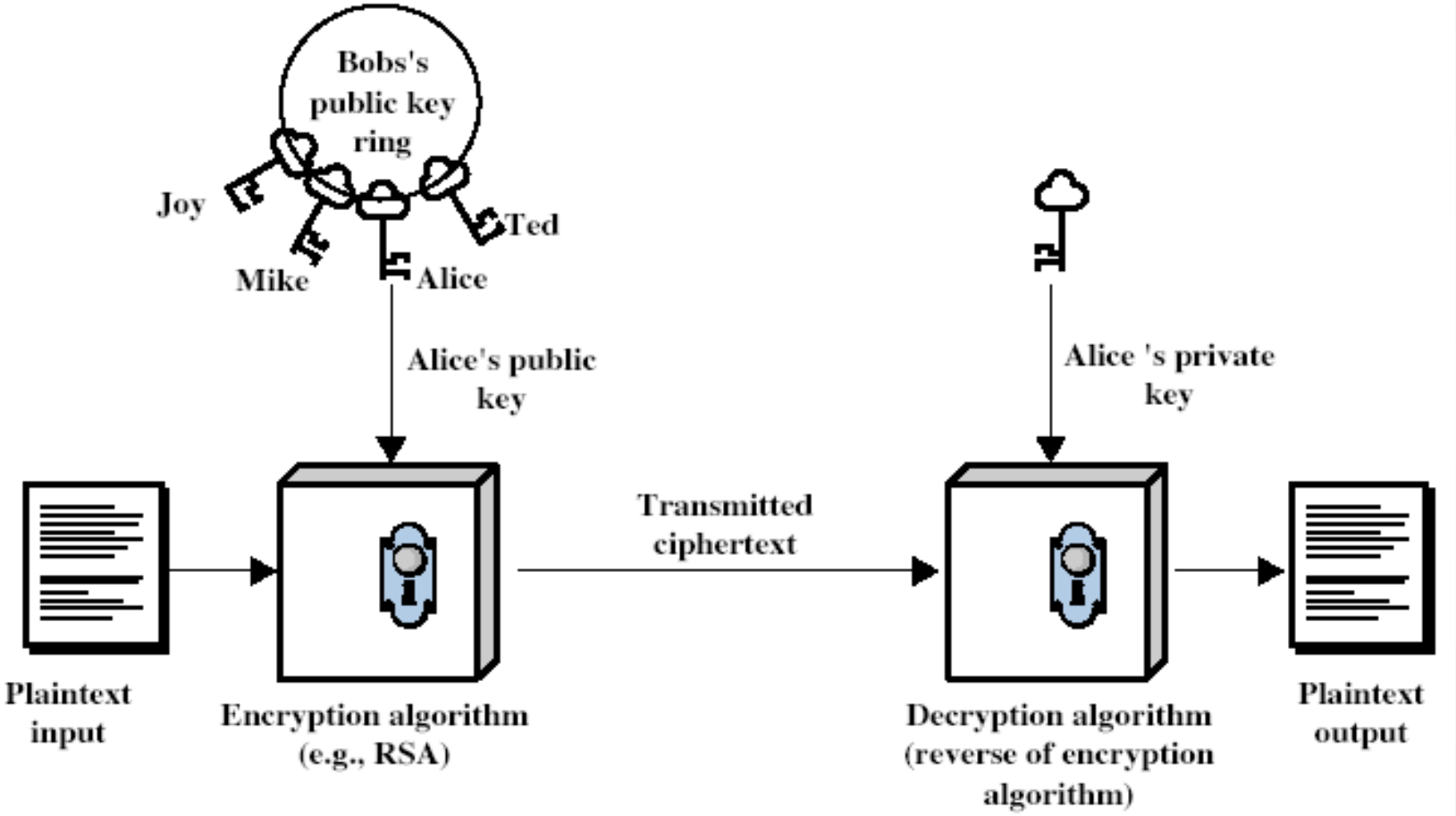
Digital Signature Properties

- must depend on the message signed
- must use information unique to sender
  - to prevent both forgery and denial
- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
  - with new message for existing digital signature
  - with fraudulent digital signature for given message
- be practical save digital signature in storage

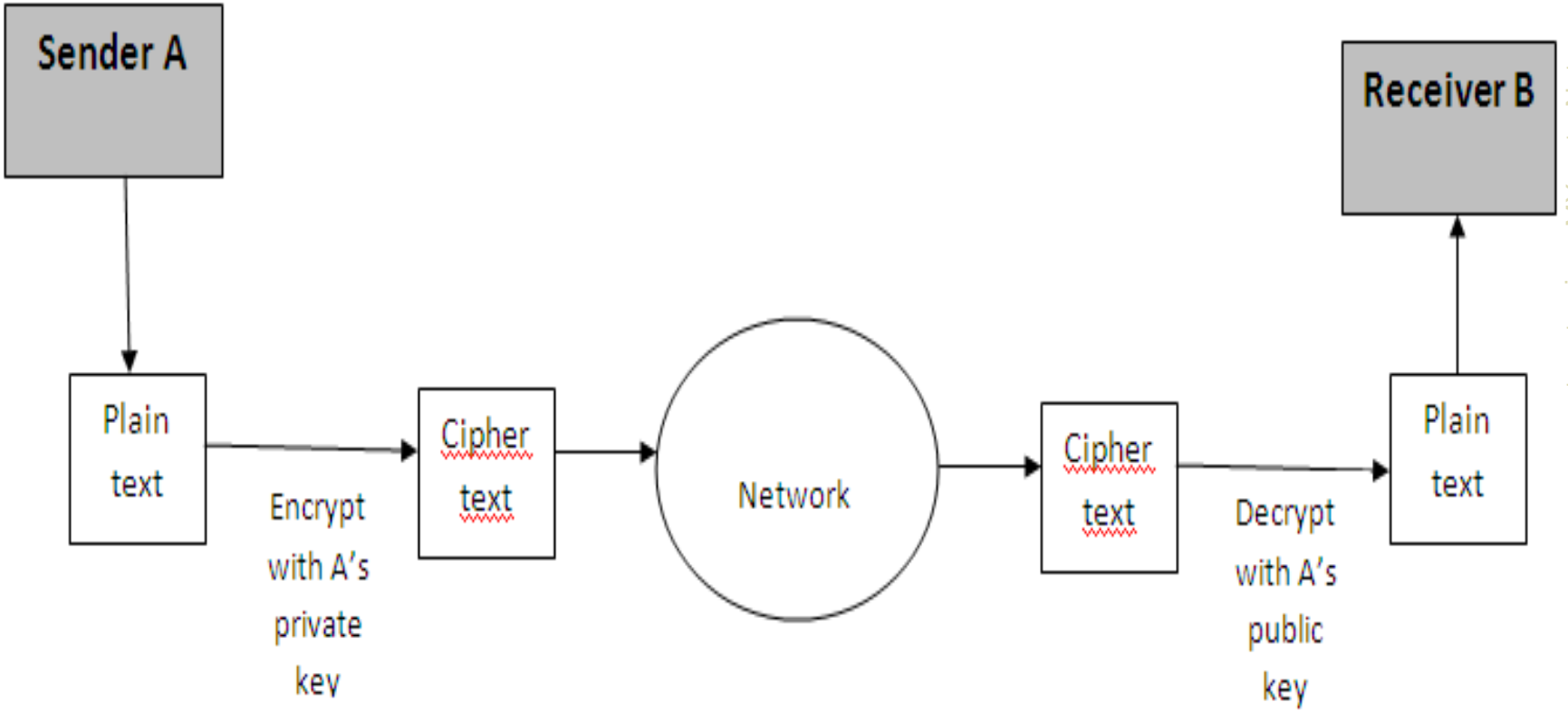
Signing The Whole Document

- Public Key encryption can be used to sign a document.
- In digital signature the private key is used for encryption and the public key is used for decryption.

Asymmetric key encryption



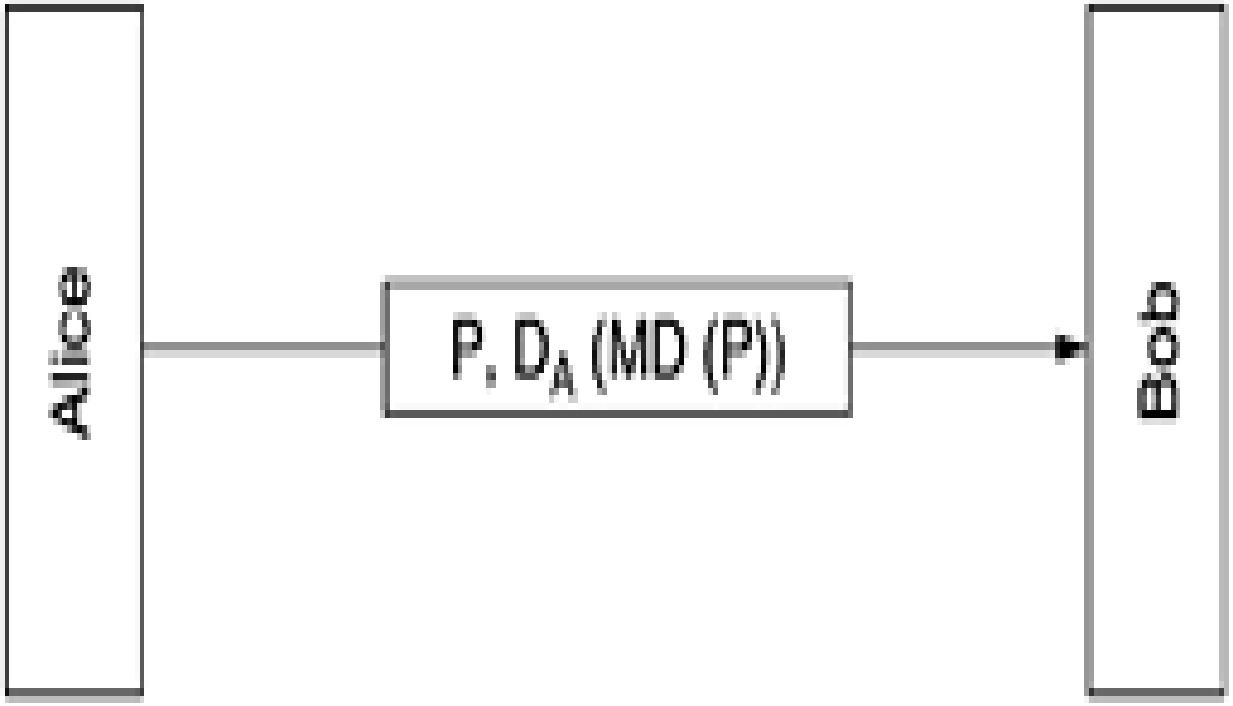
Digital signature



Signing The Digest

- In this method the sender creates a miniature version of the document and signs it. After that the receiver can checks the signature on the miniature.
- To create a digest of the message we use hash function.
- The 2 most common hash function are MD5 (120 bit digest) & SHA-1 (160 bit digest).

Digital signatures using message digests



Message Digest

- Alice first computes the message digest of her plaintext.
- She then signs the message digest and sends both the signed digest and the plaintext to Bob.
- If Trudy replaces P underway, Bob will see this when he computes MD(P) himself.

Types of digital signature

- **Symmetric-Key Signatures**
- **Public-Key Signatures**

Symmetric-Key Signatures

- One approach to digital signatures is to have a central authority that knows everything and whom everyone trusts, say Big Brother (BB).
- Each user then chooses a secret key and carries it by hand to BB's office.
- Thus, only Alice and BB know Alice's secret key, K_A, and so on.

Digital signatures with Big Brother

- When Alice wants to send a signed plaintext message, P, to her banker, Bob, she generates $K_A(B, R_A, t, P)$, where

B -> Bob's identity,

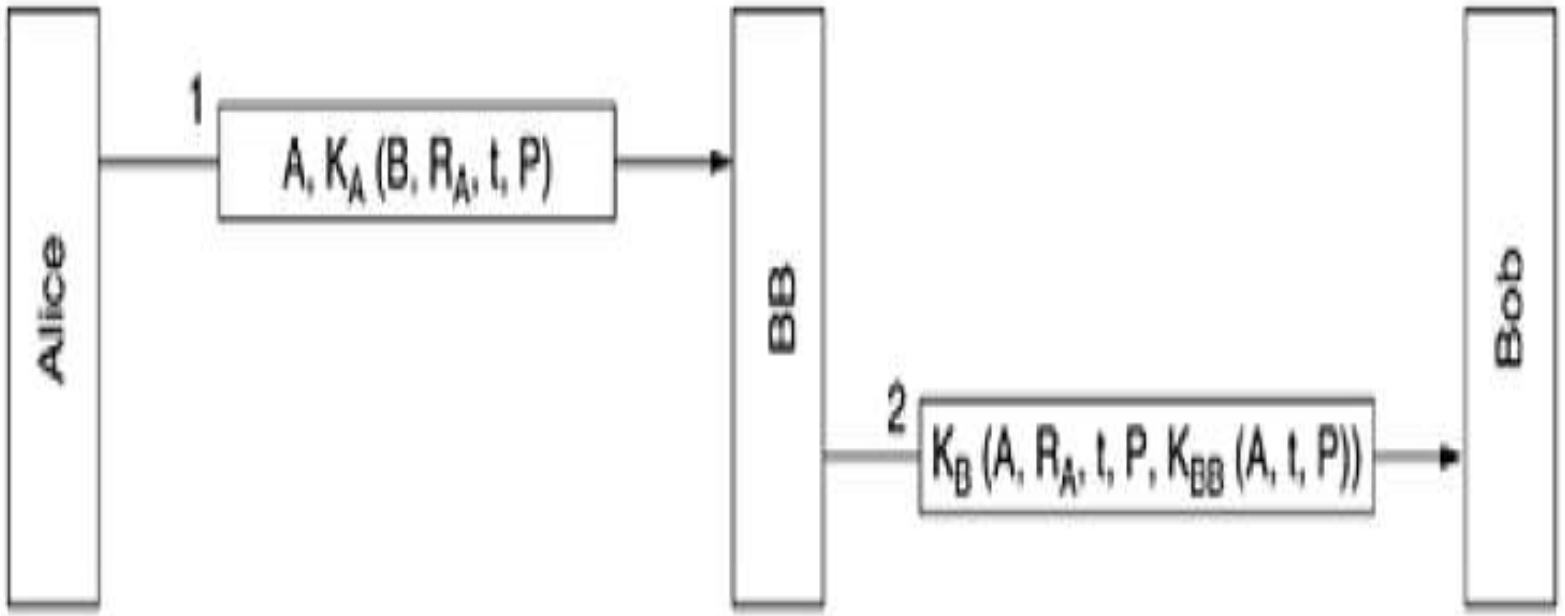
R_A -> is a random number chosen by Alice

t -> a timestamp to ensure freshness,

$K_A(B, R_A, t, P)$ is the message encrypted with her key, K_A.

- Then she sends it.
- BB sees that the message is from Alice, decrypts it using A's private key, and again encrypt with B's private key sends a message to Bob as shown.
- The message to Bob contains the plaintext of Alice's message and also the signed message $K_{BB}(A, t, P)$. Bob then decrypt it with own private key.
- Bob now carries out Alice's request.

Digital signatures with Big Brother



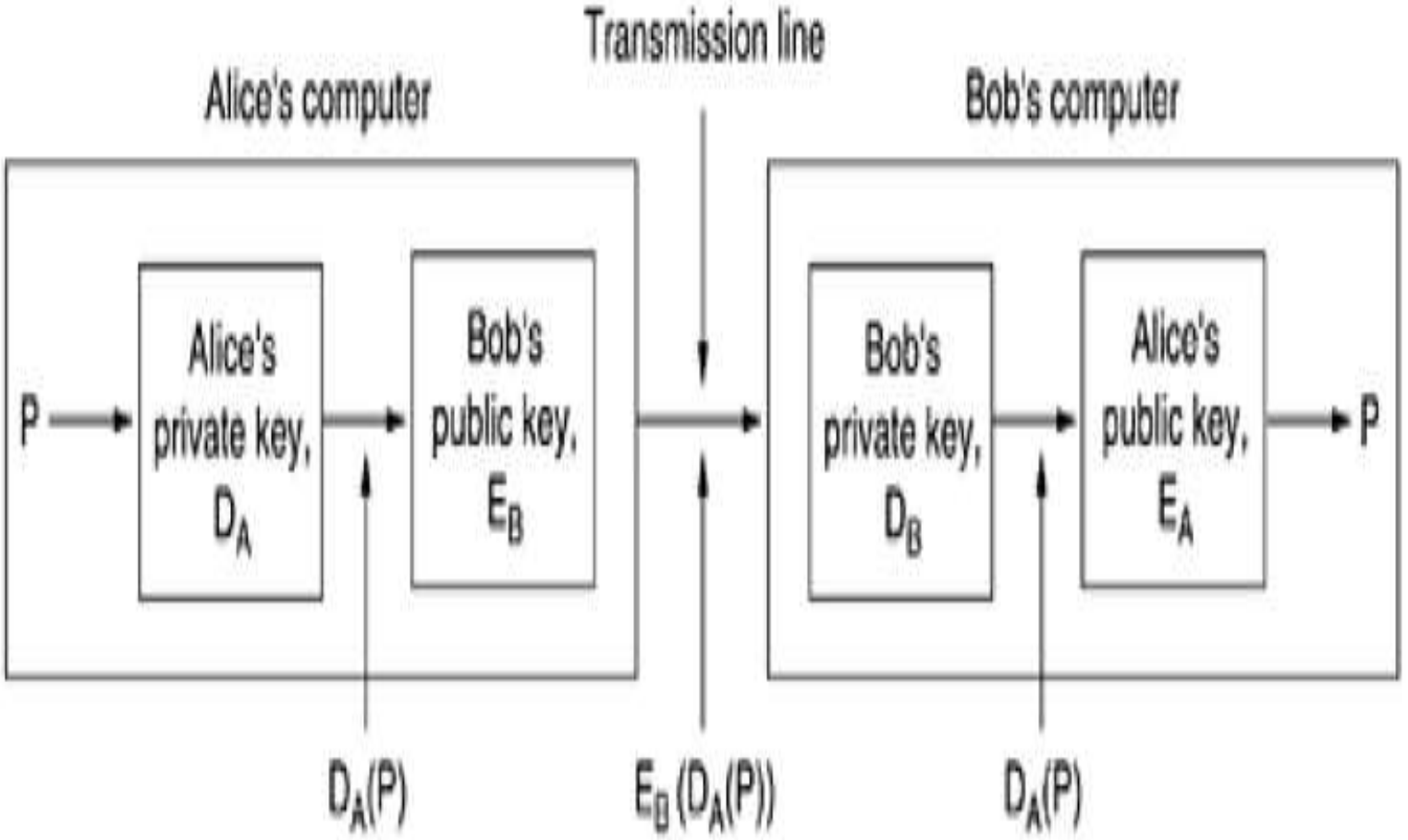
Public-Key Signatures

- A structural problem with using symmetric-key cryptography for digital signatures is that everyone has to agree to trust Big Brother.
- Furthermore, Big Brother gets to read all signed messages.

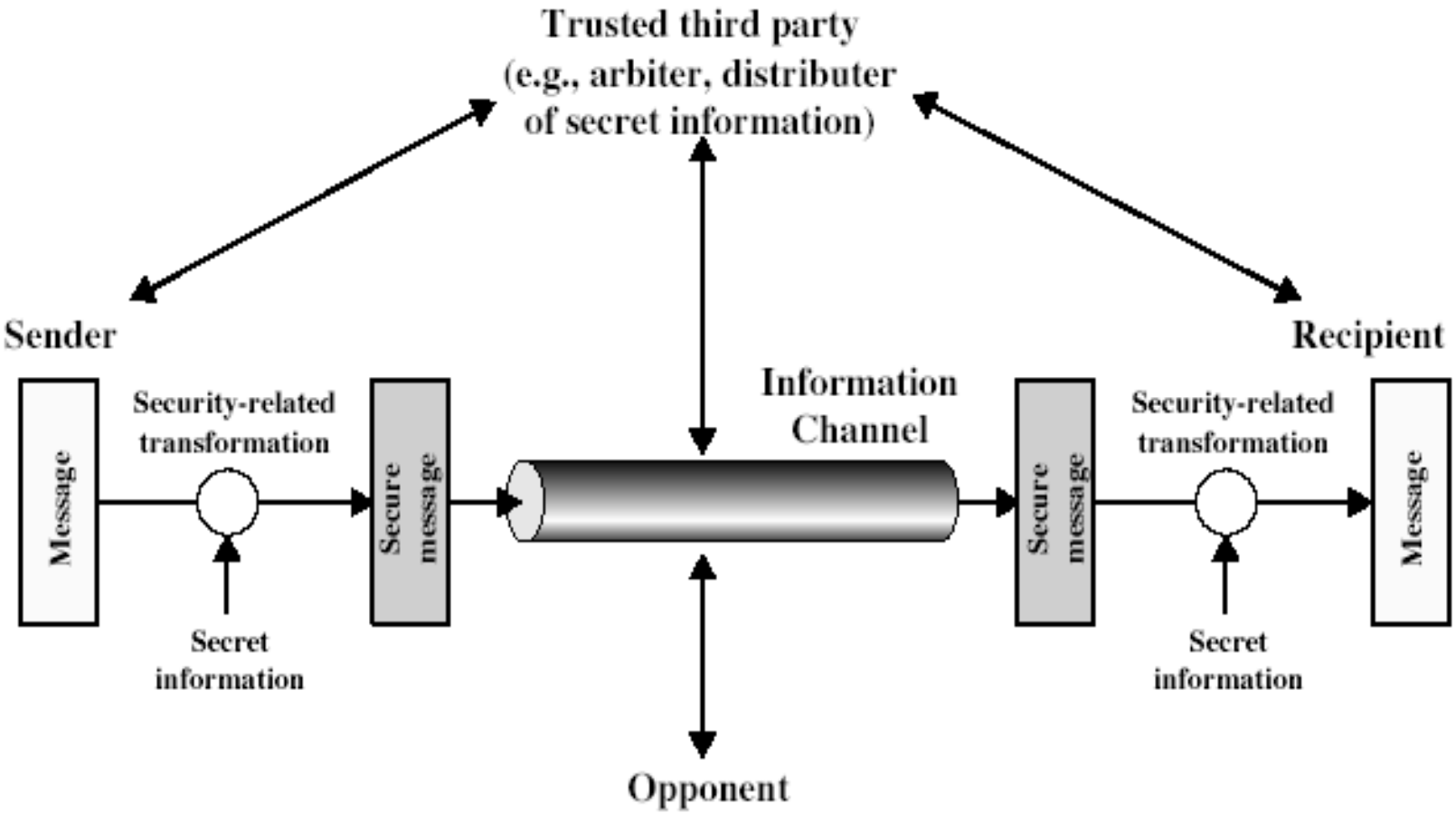
Continued……..

- Alice can send a signed plaintext message, P, to Bob by transmitting $E_B(D_A(P))$.
- Note carefully that Alice knows her own (private) key, D_A, as well as Bob's public key, E_B, so constructing this message is something Alice can do.
- When Bob receives the message, he transforms it using his private key, as usual, yielding $D_A(P)$.
- He stores this text in a safe place and then applies E_B to get the original plaintext.

Public-Key Signatures



Model for Network Security



- Any security providing technique has following two basic components,
  - Security related transformation
  - Secret information

Security related transformation

- A Security related transformation is done on the information to be sent i.e. encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

Secret Information

- Some secret information shared by the two parties and it is hoped, that it is unknown to the opponent.
- Example is the encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Trusted third party

- A third party here is responsible for **distributing the secret information** to the two parties while keeping away it from the opponent.

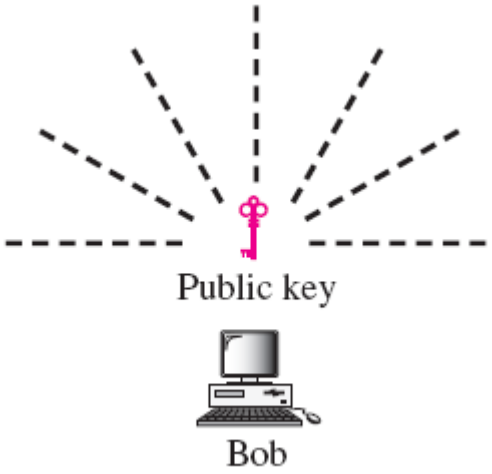
Model for Network Security

- Using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Public-Key Distribution

- In asymmetric-key cryptography, public keys, like secret keys, need to be distributed .

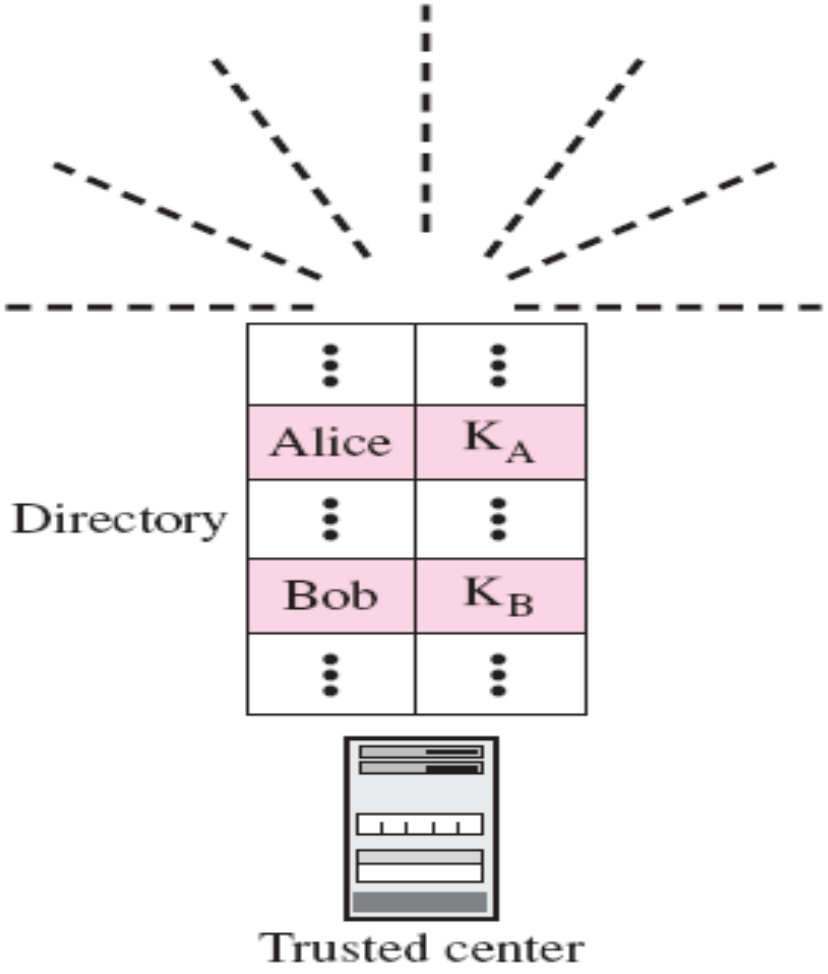
Announcing a public key



Trusted Center

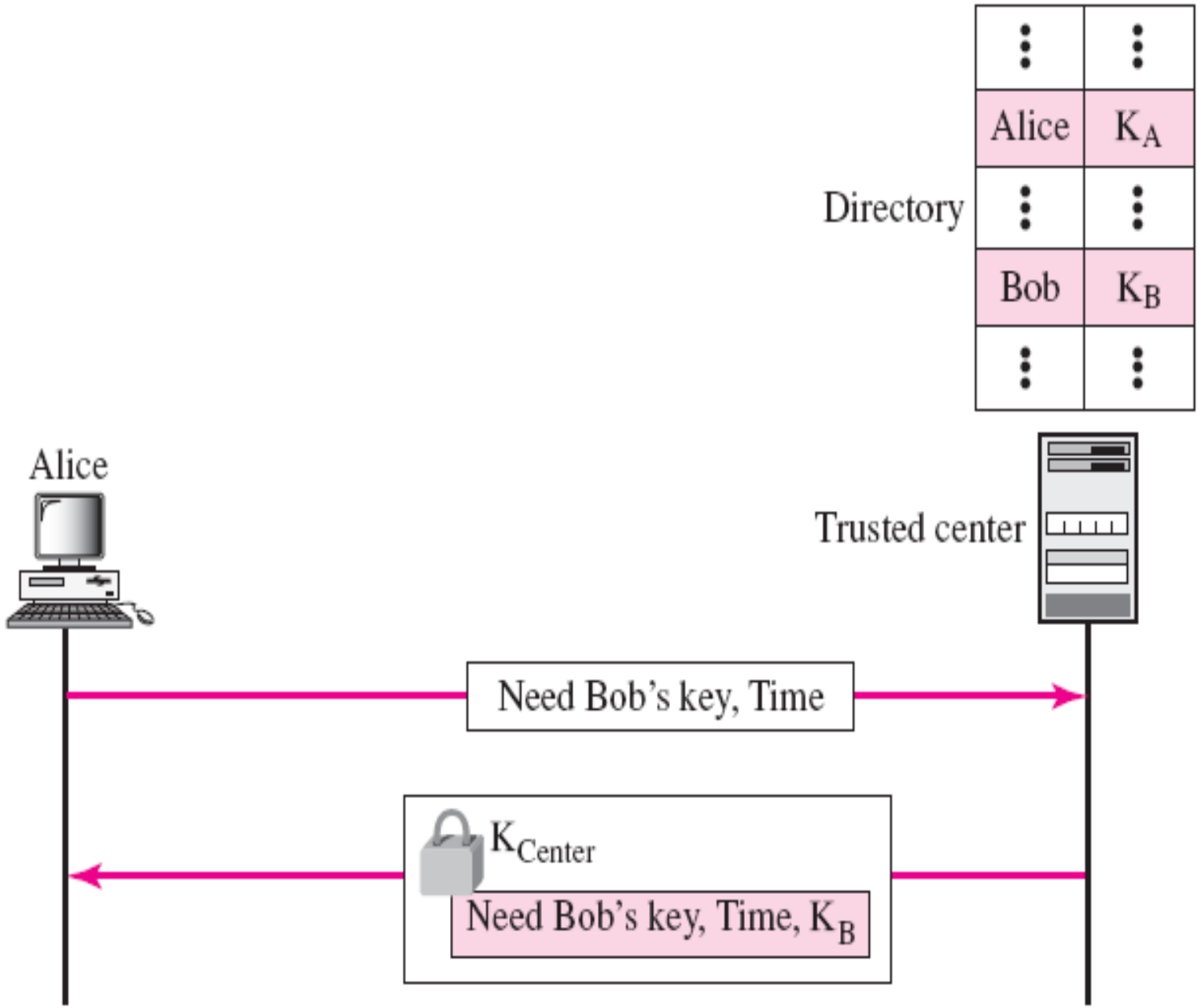
- A more secure approach is to have a trusted center retain a directory of public keys.
- The directory, like the one used in a telephone system, is dynamically updated.
- Each user can select a private/public key, keep the private key, and deliver the public key for insertion into the directory.
- The center requires that each user register in the center and prove his or her identity.
- The directory can be publicly advertised by the trusted center.
- The center can also respond to any inquiry about a public key.

Trusted center



Controlled Trusted Center

- The public-key announcements can include a timestamp and be signed by an authority to prevent interception and modification of the response.
- If Alice needs to know Bob's public key, she can send a request to the center including Bob's name and a timestamp.
- The center responds with Bob's public key, the original request, and the timestamp signed with the private key of the center.
- Alice uses the public key of the center, known by all, to decrypt the message and extract Bob's public key.

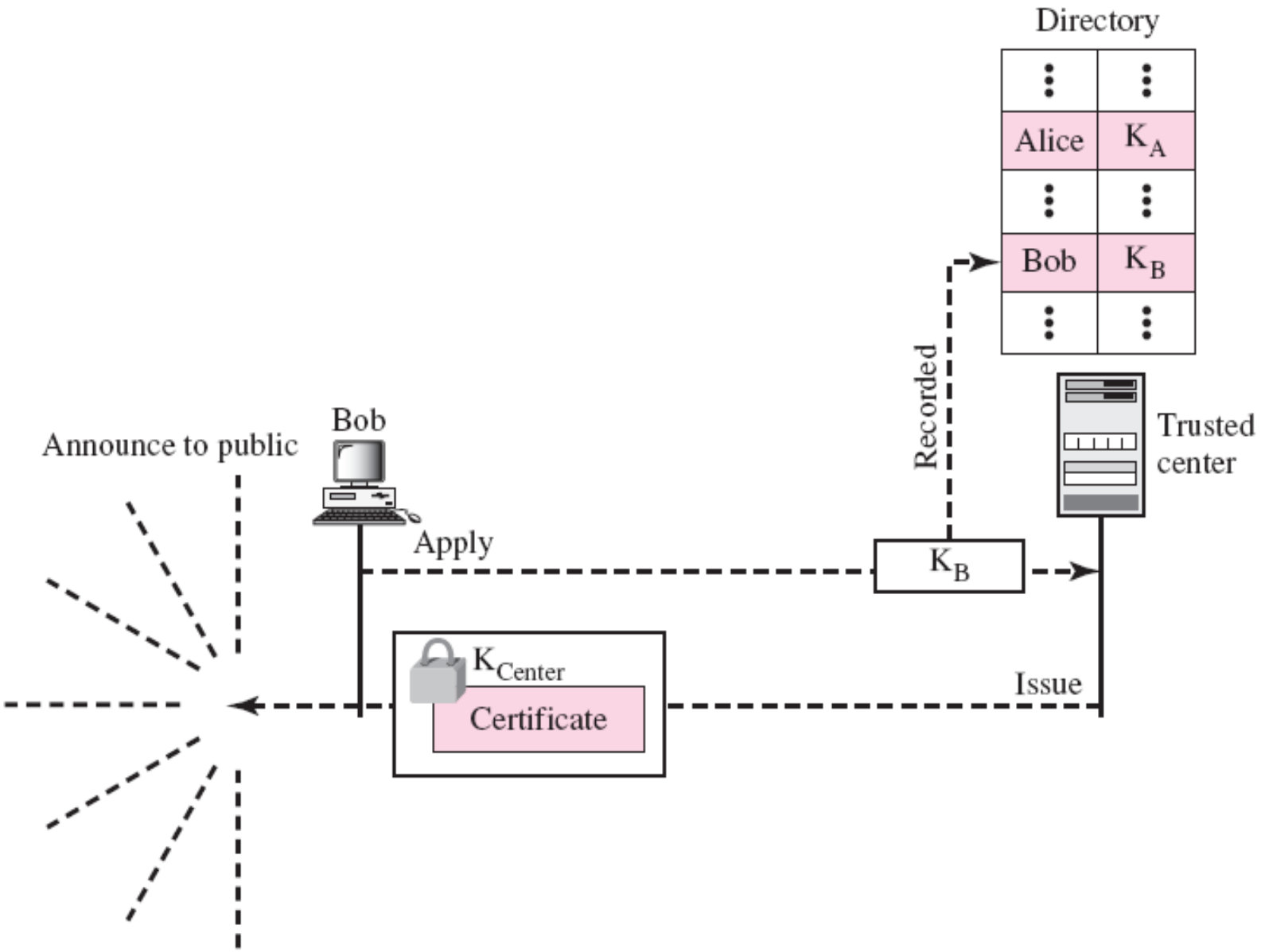


Certification authority

- The previous approach can create a heavy load on the center if the number of requests is large.
- The alternative is to create public-key certificates.
- Bob can go to a **certification authority (CA)—a federal or state organization** that binds a public key to an entity and issues a certificate.
- The CA has a well-known public key itself that cannot be forged.
- The CA checks Bob's **identification (using a** picture ID along with other proof).
- It then asks for Bob's public key and writes it on the certificate.

- To prevent the certificate itself from being forged, the CA signs the certificate with its private key.
- Now Bob can upload the signed certificate. Anyone who wants Bob's public key downloads the signed certificate and uses the public key of the center to extract Bob's public key.

Certification authority



X.509

- **Although the use of a CA has solved the problem of public-key fraud, it has** created a side effect.
- Each certificate may have a different format.
- One certificate may have the public key in one format and another in another format.
- The public key may be on the first line in one certificate and on the third line in another.
- Anything that needs to be used universally must have a universal format.

Certificate format

- **Version: This field defines the version of X.509 of the certificate.**
- **Serial number: This field defines a number assigned to each certificate. The value** is unique for each certificate issued.
- **Signature: This field, identifies the algorithm** used to sign the certificate.
- **Issuer: This field identifies the certification authority that issued the certificate.**
- **Period of validity: This field defines the earliest and the latest times the certificate** is valid.

Continued…

- **Subject:** **This field defines the entity to which the public key belongs.**
- **Extension:** **This field allows issuers to add more private information to the certificate.**
- **Subject's public key:** **This field defines the subject's public key, the heart of the** certificate.