Network Security

Chapter 8

Cryptography

- Introduction
- Substitution ciphers
- Transposition ciphers
- One-time pads
- Fundamental cryptographic principles

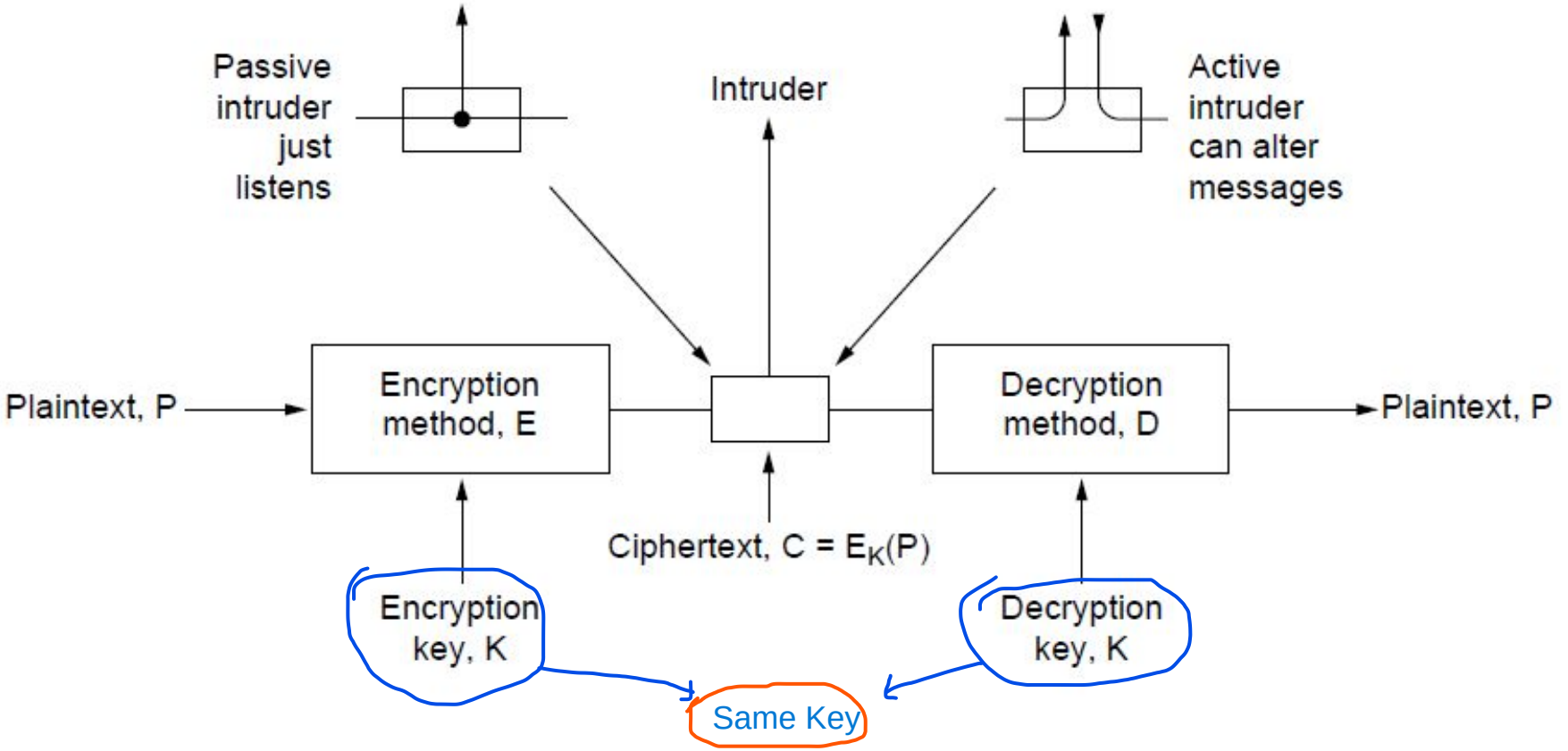
- **Encryption:** The process of transforming data or information into something random or meaningless.
- **Decryption:** The process of transforming random or meaningless data into pure data.
- **Symmetric key cryptography**

Symmetric key cryptography is an **encryption** system in which the sender and receiver of a message share a single, common **key** that is used to encrypt and decrypt the message.

- **Asymmetric key cryptography**

Asymmetric key cryptography is a system that uses pairs of *keys*(public and private) to encrypt and decrypt data. Public keys can be shared to everyone and private are known only to the owner.

Introduction



The encryption model (for a symmetric-key cipher).

Substitution Ciphers

plaintext:	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:	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

Monoalphabetic substitution

Transposition Ciphers

Key

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

Random Alphabet

Rearrange the order of plain text

1. Rail fence cipher 2. Row transposition cipher

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

1 2

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Public-key Algorithms

Assymmetric Key Encription

- RSA
  - Authors: *R*ivest, *S*hamir, *A*dleman
- Other Public-Key Algorithms

RSA (1)

Method Summary

1. Choose two large primes, *p* and *q*
2. Compute
   $n = p \times q$ *and* $z = (p - 1) \times (q - 1)$.
3. Assume e such that gcd(e,z)=1
4. *Assume d such that d*e mod z=1*

   public key={e,n}

   Private key={d,n}

RSA (2)

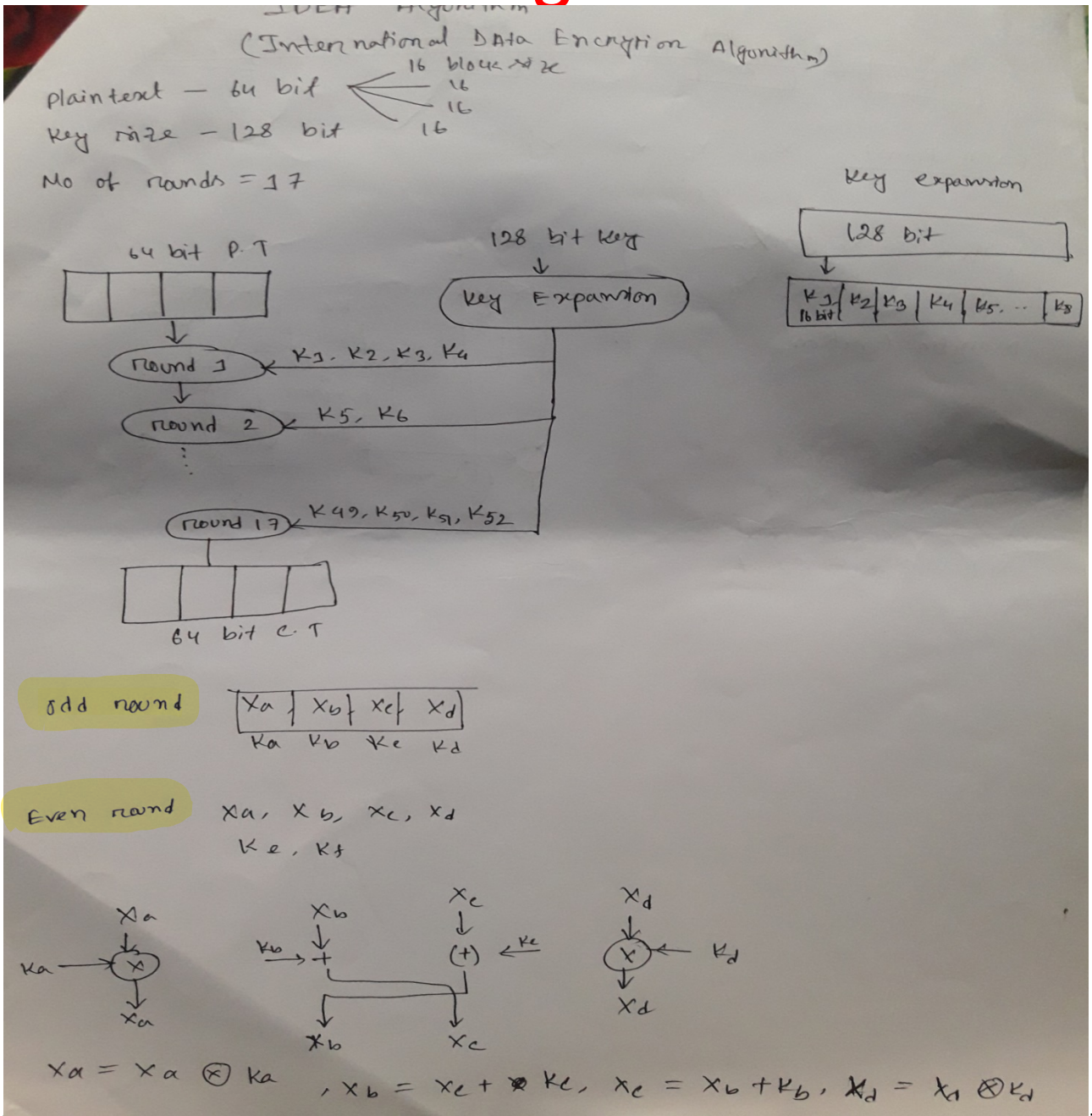
Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

Receiver's computation

An example of the RSA algorithm

IDEA Algorithm



Even Round: X_a X_b X_c X_d K_e K_f

$y_{in} = X_a \oplus X_b$

$z_{in} = X_c \oplus X_d$

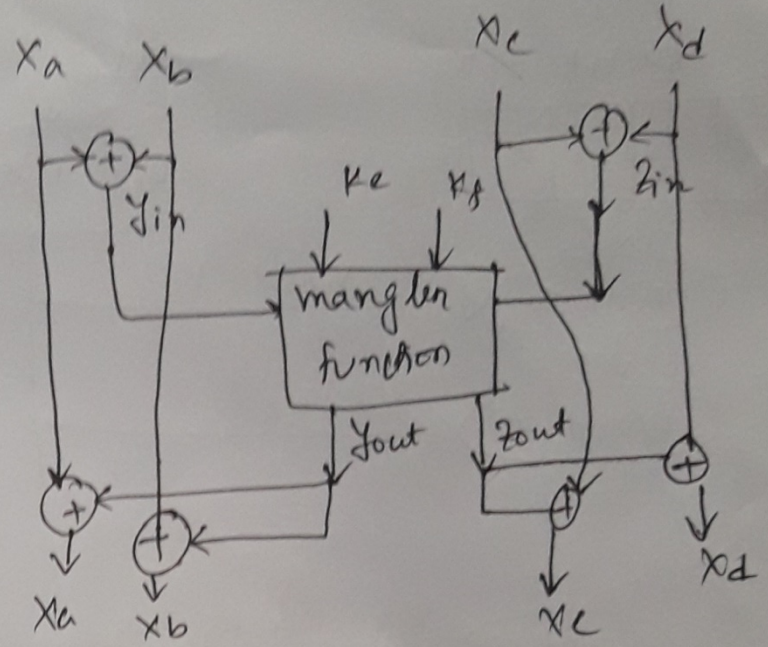
Mangler function

$X_a = X_a \oplus Y_{out}$

$X_b = X_b \oplus Y_{out}$

$X_c = X_c \oplus Z_{out}$

$X_d = X_d \oplus Z_{out}$



Digital signatures

- Digital signature is an authentication technique that combines user authentication and message authentication using public key cryptography.

- Sender A calculates a message digest from the communication text
- Sender A encrypts the message digest using sender A's private key
- Sender A sends the communication text and cipher text to recipient B
- Recipient B decrypts the cipher text using sender A's public key
- Recipient B calculate message digest from received communication text
- Recipient B compares the message digest decrypted in (4) with the message digest calculated in (5). If these two are the same, it is confirmed that A is the sender and the communication text is not falsified