KLE TECH.

KLE Technological University

Creating Value
Leveraging Knowledge

Chapter 2: Crypto Primitives

Crypto Basics

- Introduction to Information Security
- Overview of Cryptography
- Substitution Ciphers
- Transposition and Product Ciphers
- Taxonomy of Cryptography

Introduction

- Need for Information Security
  - Information is an Asset
  - A security attack can cause serious damage to reputation.
- Information Security requirements have changed with technology
  - Physical files
  - Computer Systems
  - Distributed and Internet
  - Cloud, mobile and IoT

Information Security Goals

- What is Information Security?

  Information security is the practice of protecting information by mitigating information risks.

- Information Security Goals
  - Confidentiality
  - Integrity
  - Availability

Aspects of Information Security

1. Security Attack

Any action that compromises the security of information.

2. Security Service

A service that enhances the security of data processing systems and information transfers.

3. Security Mechanism

A process that is designed to detect, prevent, or recover from a security attack.

1. Security Attacks

- **Passive Attacks**
  - Attacker goal is just to obtain the data
  - Attacker does not modify or harm the system

- **Active Attacks**
  - Attacker tries to Modify the content of message.
  - Easy to detect than prevent

Passive Attacks

- **Release of message content**
  - Unauthorised access to sensitive or confidential information.
  - Use encryption

- **Traffic Analysis**
  - Attacker can observe the pattern of messages in ciphertext.

Active Attacks

- Masquerade

One entity pretends to be different entity.

- Replay

Passive capture of data unit and its subsequent transmission to produce unauthorised effect.

Active Attacks

- Modification of Messages

Portion of legitimate message is altered to produce unauthorised effect.

- Denial of Service

Disruption of service to intended users.

Security Services

- X.800 divides the services into five categories
  - Data Confidentiality
  - Data Integrity
  - Authentication
  - Access Control
  - Non-repudiation

Security Services

- **Data Confidentiality**
  The protection of data from unauthorized disclosure

- **Data Integrity**
  Protection of data from modification, insertion, deletion etc.

- **Authentication**
  The assurance that the communicating entity is the one who it claims to be.

Security Services

- **Access Control**
  Protection from unauthorized use of service.

- **Non Repudiation**
  Protection against denial by one of the entities.

- **Availability**
  Protection against disruption of service.

KLE Technological University
Creating Value
Leveraging Knowledge

Overview of Cryptography

Basic Terminology

- **Cryptography**

  Making “secret codes”

- **Cryptanalysis**

  Breaking “secret codes”

- **Cryptology**

  Making and breaking secret codes.

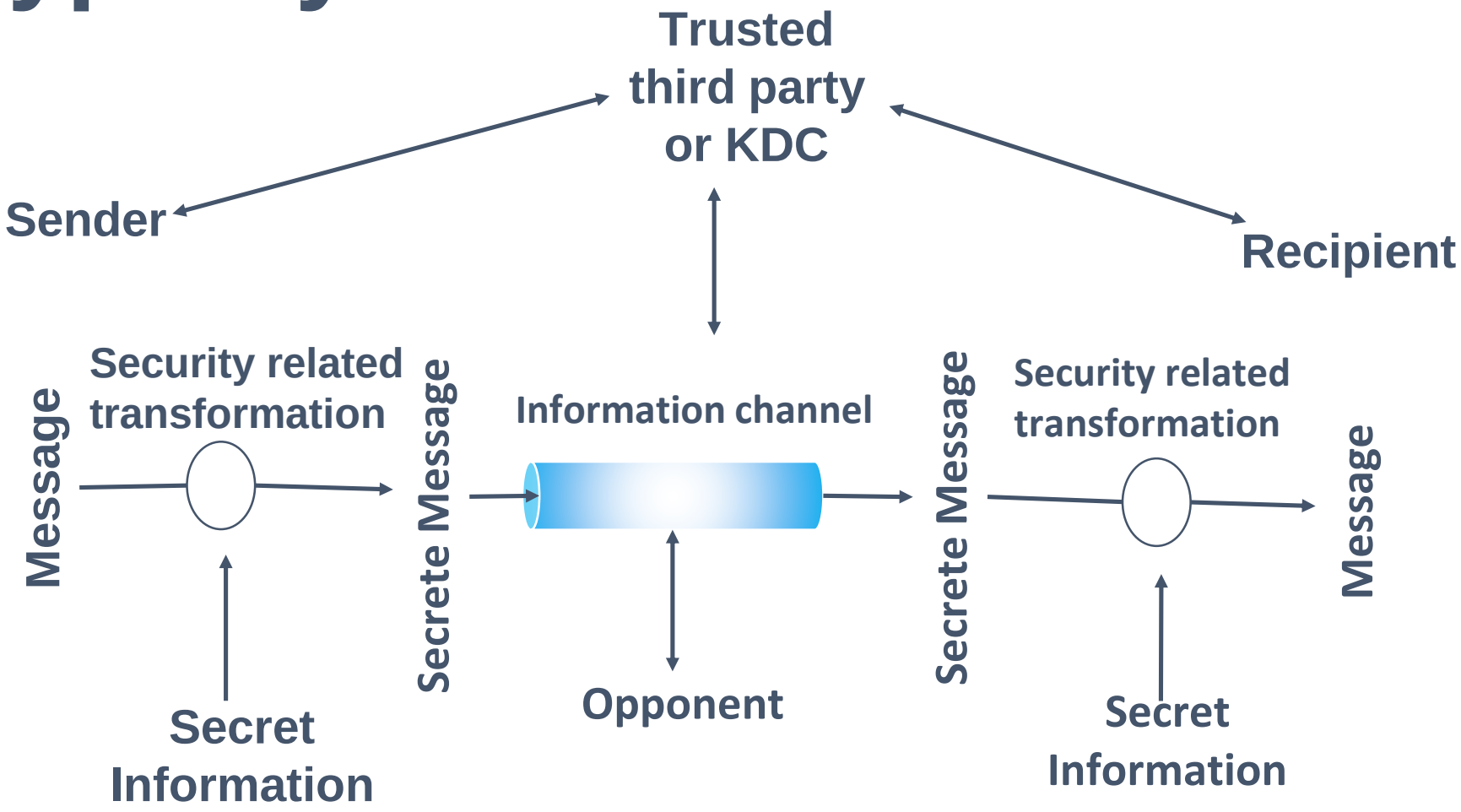
- **Crypto**

  All or any of the above

- **Crypto**systems

  Systems that use secrets.

Cryptosystem



Kerckhoffs's Principle

- Basic Assumptions
  - The system is completely known to the attacker
  - Only the key is secret

- Why do we make such an assumption?
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

KLE Technological University
Creating Value
Leveraging Knowledge

Substitution Ciphers

Shift-by-n Cipher

- Earliest known substitution cipher
- Shift letter by n letters ahead of it
- Key (n=3)

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	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

Product Ciphers

- Combination of substitution and transposition ciphers in succession
- Improves the security
- Used in modern cryptosystems

KLE Technological University
Creating Value
Leveraging Knowledge

Taxonomy of Cryptography

Taxonomy of Cryptography

Three categories of cryptography.

Symmetric Key

- Same key for encryption and decryption
- Two types: Stream ciphers, Block ciphers

Public Key

- Two keys, one for encryption (public), and one for decryption (private)
- Digital signatures.

Taxonomy of Cryptography

Hash algorithms:

Takes input of any size and produce an output of a fixed size that satisfies some very special properties.

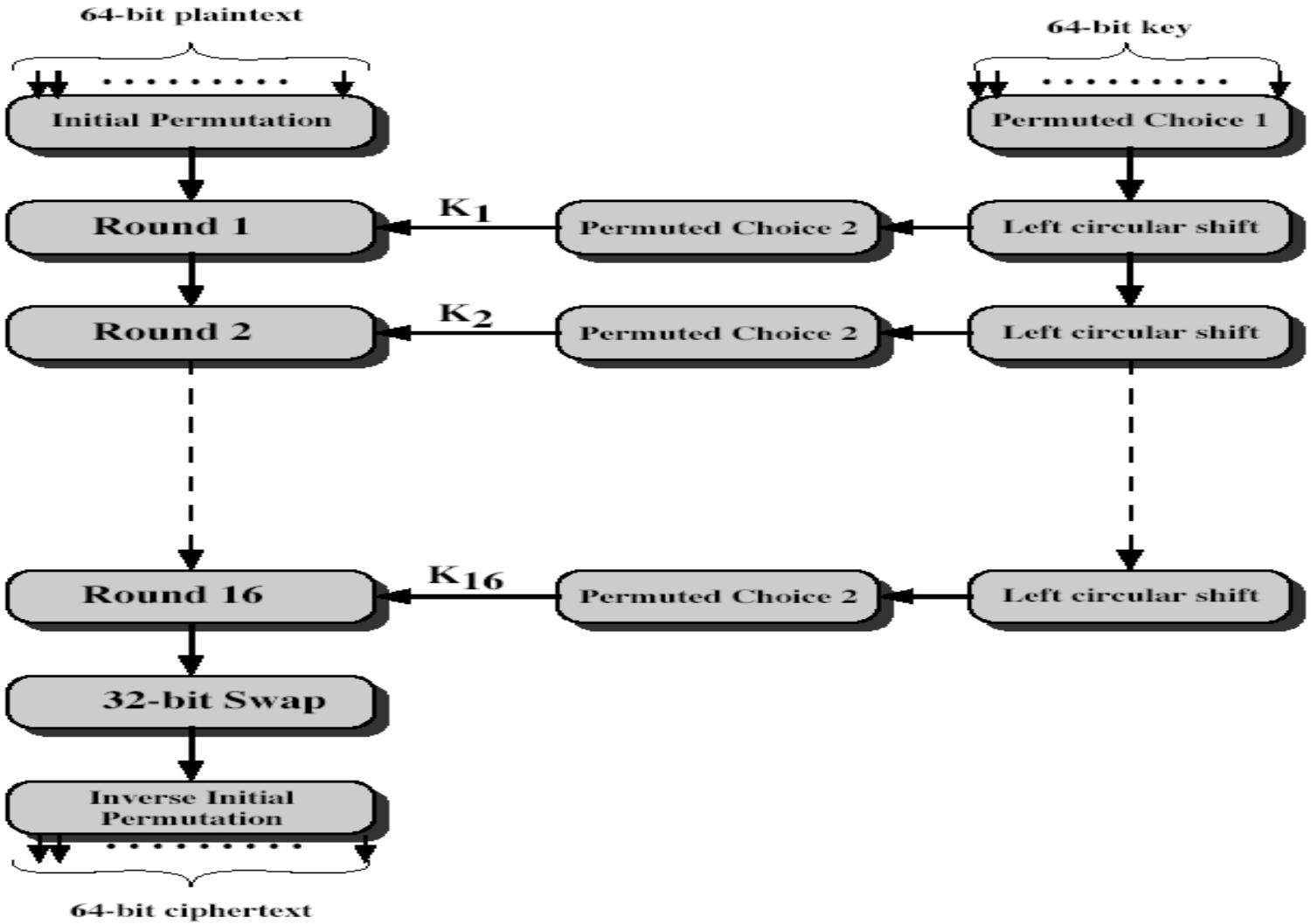
- Hash functions are one-way
- Must be infeasible to find two inputs that produce the same output.

Symmetric Key Cryptography

Data Encryption Standard

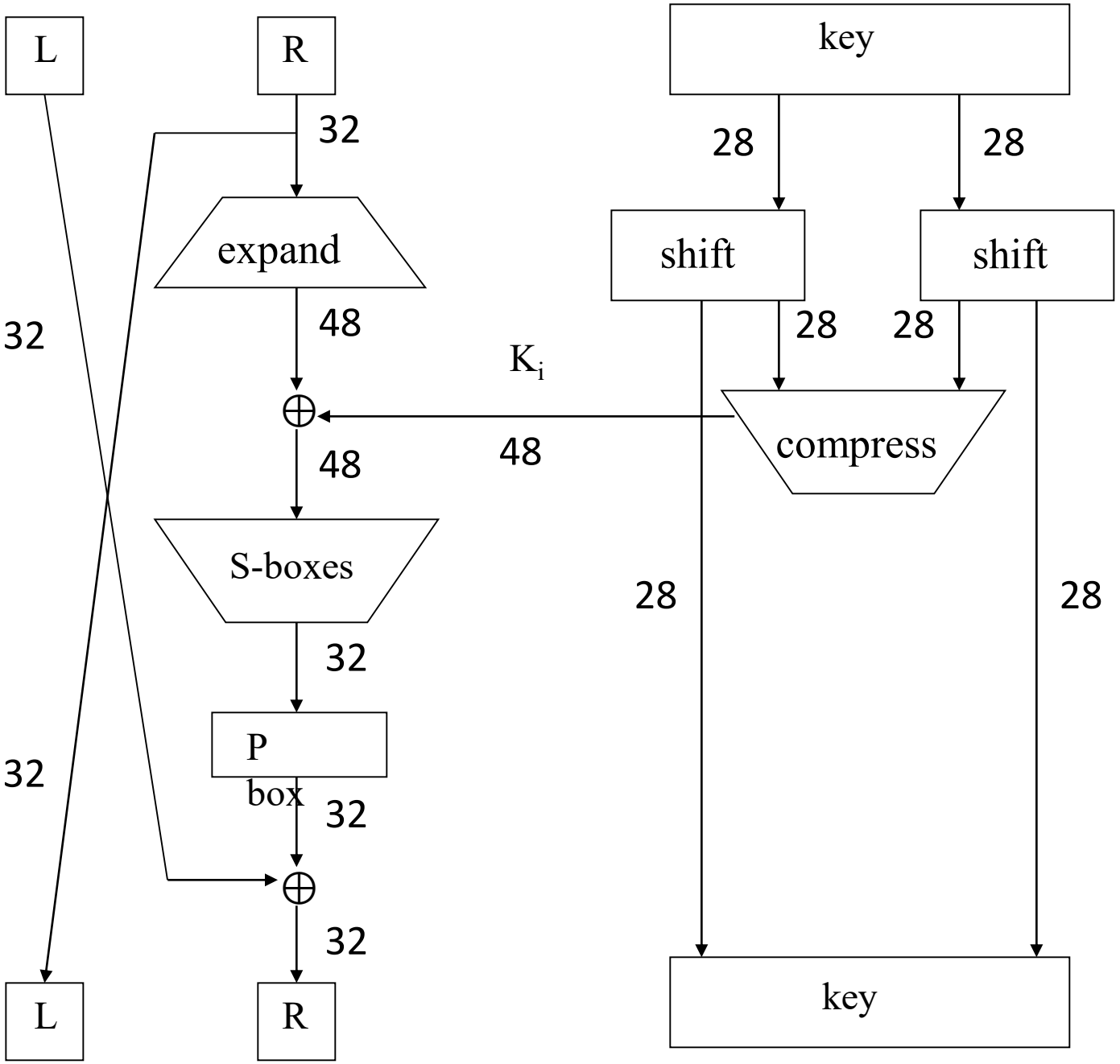
- **DES** developed in 1970's
- Based on IBM Lucifer cipher
- U.S. government standard
- DES development was controversial
  - NSA secretly involved
  - Design process was secret
  - Key length reduced
  - Subtle changes to Lucifer algorithm

DES Encryption



DES Numerology

- DES is a Feistel cipher
  - 64 bit block length
  - 56 bit key length
  - 16 rounds
  - 48 bits of key used each round (subkey)
- Each round is simple (for a block cipher)
- Security depends primarily on “S-boxes”
  - Each S-boxes maps 6 bits to 4 bits



One Round of DES

DES Expansion Permutation

- Input 32 bits

  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

  16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

- Output 48 bits

  31 0 1 2 3 4 3 4 5 6 7 8

  7 8 9 10 11 12 11 12 13 14 15 16

  15 16 17 18 19 20 19 20 21 22 23 24

  23 24 25 26 27 28 27 28 29 30 31 0

DES S-box

- 8 “substitution boxes” or S-boxes
- Each S-box maps 6 bits to 4 bits
- S-box number 1

input bits (0,5)

↓ input bits (1,2,3,4)

| 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

----

00 | 1110 0100 1101 0001 0010 1111 1011 1000 0011 1010 0110 1100 0101 1001 0000 0111

01 | 0000 1111 0111 0100 1110 0010 1101 0001 1010 0110 1100 1011 1001 0101 0011 1000

10 | 0100 0001 1110 1000 1101 0110 0010 1011 1111 1100 1001 0111 0011 1010 0101 0000

11 | 1111 1100 1000 0010 0100 1001 0001 0111 0101 1011 0011 1110 1010 0000 0110 1101

Ex 1: Input bits are 011110 output is 0111

Ex 2: Input bits are 000010 Output is 0100

8 S-boxes

i	S_i															
1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES P-box

- Input 32 bits

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

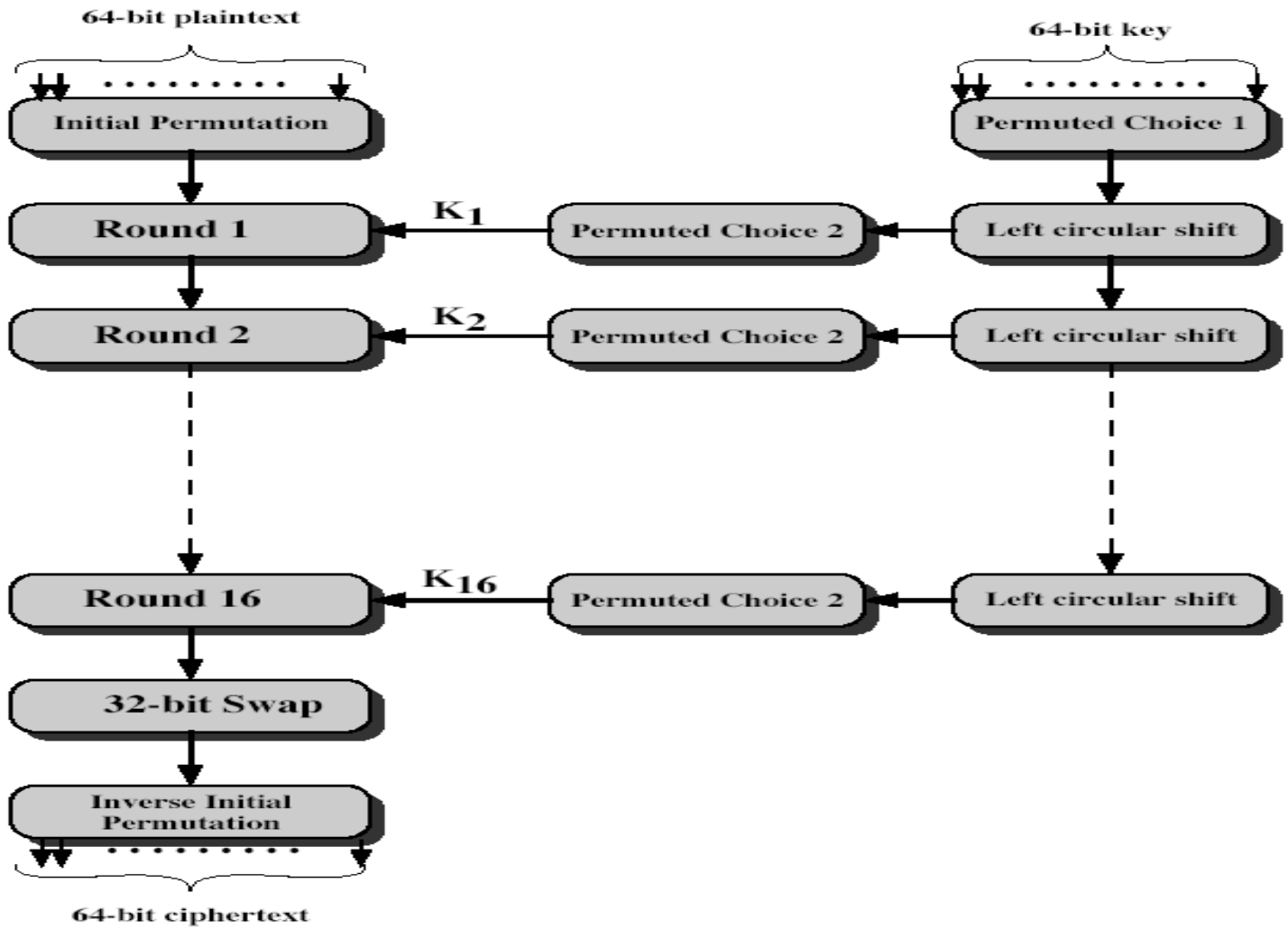
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

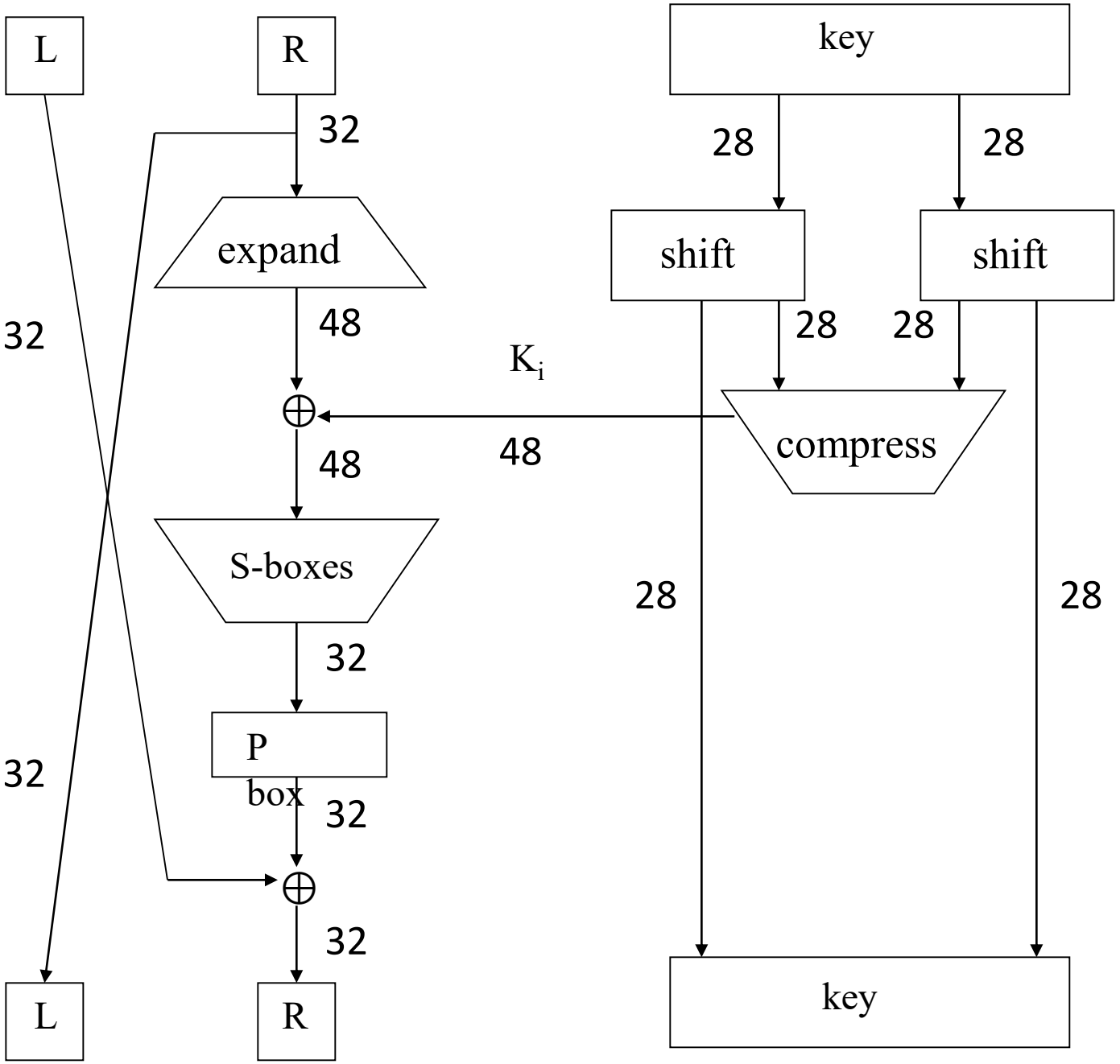
- Output 32 bits

15 6 19 20 28 11 27 16 0 14 22 25 4 17 30 9

1 7 23 13 31 26 2 8 18 12 29 5 21 10 3 24

DES Encryption





One Round of DES

DES Subkey

Step1:

- 56 bit DES key, numbered 0,1,2,…,55 is obtained using **PC-1** using 64-bit key. Every 8th bit the ignored.
- Left half key bits, LK

  49 42 35 28 21 14 7
  0 50 43 36 29 22 15
  8 1 51 44 37 30 23
  16 9 2 52 45 38 31

- Right half key bits, RK

  55 48 41 34 27 20 13
  6 54 47 40 33 26 19
  12 5 53 46 39 32 25
  18 11 4 24 17 10 3

DES Subkey

Step2:

- For rounds i=1,2,...,16
  - Let $LK = (LK$ circular shift left by $r_i)$
  - Let $RK = (RK$ circular shift left by $r_i)$

  - Apply PC-2 (compression permutation on LK and RK)

```
13 16 10 23  0  4  2 27 14  5 20  9
22 18 11  3 25  7 15  6 26 19 12  1

12 23  2  8 18 26  1 11 22 16  4 19
15 20 10 27  5 24 17 13 21  7  0  3
```

DES Subkey

- For rounds 1, 2, 9 and 16 the shift r_i is 1, and in all other rounds r_i is 2
- Bits 8,17,21,24 of LK omitted each round
- Bits 6,9,14,25 of RK omitted each round
- **Compression permutation** yields 48 bit subkey K_i from 56 bits of LK and RK
- **Key schedule** generates subkey

Security of DES

- Security of DES depends on S-boxes
  - Everything else in DES is linear
- Thirty++ years of intense analysis has revealed no “back door”
- Attacks use exhaustive key search
- 3DES with 112 bit key is used..