
PARTH IMAGING CENTER
DINESHBHAI TAK M /22Y
RT KIDNEY
LT KIDNEY
Renal
OPPO A55 · ©kartik
2025/09/13 10:36

Parth Imaging Center

Dr. Bhavin Shah (M.D.)
Consultant Radiologist

al X-rays
le Body Ultrasonography
ur Doppler Study
5. Guided Interventional Procedures
iopsy Consultation

Clinical Experience
- Nanavati Hospital (Bombay)
- Tata Memorial Hospital (Bombay)
- Kailash Cancer Hospital, Goraj

PATIENT'S NAME: DINESH TAK, M/23Y
DATE: 01.09.2025

Urinary Bladder:
It is optimally distended.
No evidence of calculus / wall thickening / floating echoes / diverticulum is seen within.

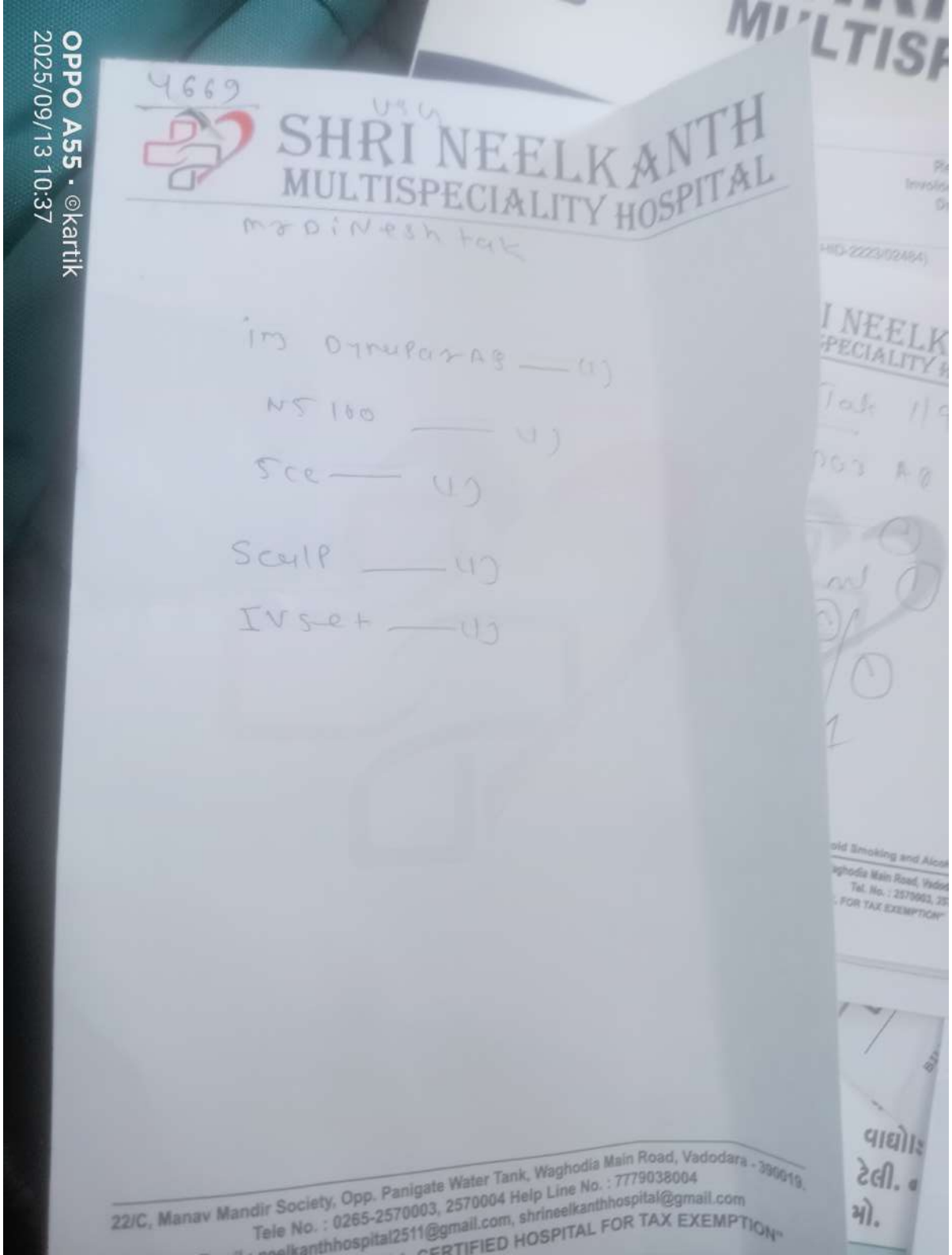
Prostate measures 27 x 25 x 31mm (CC x AP x RL) with volume 11cc.

Bilateral suprarenal regions reveal no obvious abnormality.
Bowel loops (small intestines and ascending colon, transverse colon, descending colon and sigmoid colon) reveal normal wall thickness.
RIF reveals no abnormality.
Omentum and mesentery reveal no obvious abnormality.
No evidence of mesenteric/ retroperitoneal/ periportal / peripancreatic lymphadenopathy is seen.
No evidence of free fluid is seen in peritoneal cavity.
Bilateral diaphragms reveal normal respiratory movements.
Bowel loops reveal normal peristalsis.
Retroperitoneal great vessels – naming abdominal aorta and inferior vena cava appear normal.
Anterior abdominal wall reveals no obvious abnormality.
Hermial sites (umbilical region and bilateral inguinal regions) appear normal.
Bilateral posterior paraspinous regions appear normal.

IMPRESSION:
Mild hydronephrosis on right side along with mild ipsilateral upper and mid hydro-ureter; right distal ureter – obscured by bowel gas

Dr. Bhavin Shah
(Consultant Radiologist)

Vrai-II, Uma Char Rasta, Waghodia Road, Vadodara-390 019.
drbhavinbshah@gmail.com


OPPO A55 · ©kartik
2025/09/13 10:37
4669
SHRI NEELKANTH
MULTISPECIALITY HOSPITAL
mr dinesh tak
im Oxyparas AB —— (1)
NS 100 —— (1)
Sce —— (1)
Scalp —— (1)
IV set —— (1)
22/C, Manav Mandir Society, Opp. Panigate Water Tank, Waghodia Main Road, Vadodara - 390019.
Tele No. : 0265-2570003, 2570004 Help Line No. : 7779038004
CERTIFIED HOSPITAL FOR TAX EXEMPTION

SHRI NEELKANTH MULTISPECIALITY HOSPITAL

MR. DINESH TAK

AGE:23YRS/M
DATE:1/09/2025
WEIGHT:59KGS

SPO2;99%
PULSE;65MIN%

S/ Rt ureteral

Rx

TAB Catulin 1-0-1 — (10)

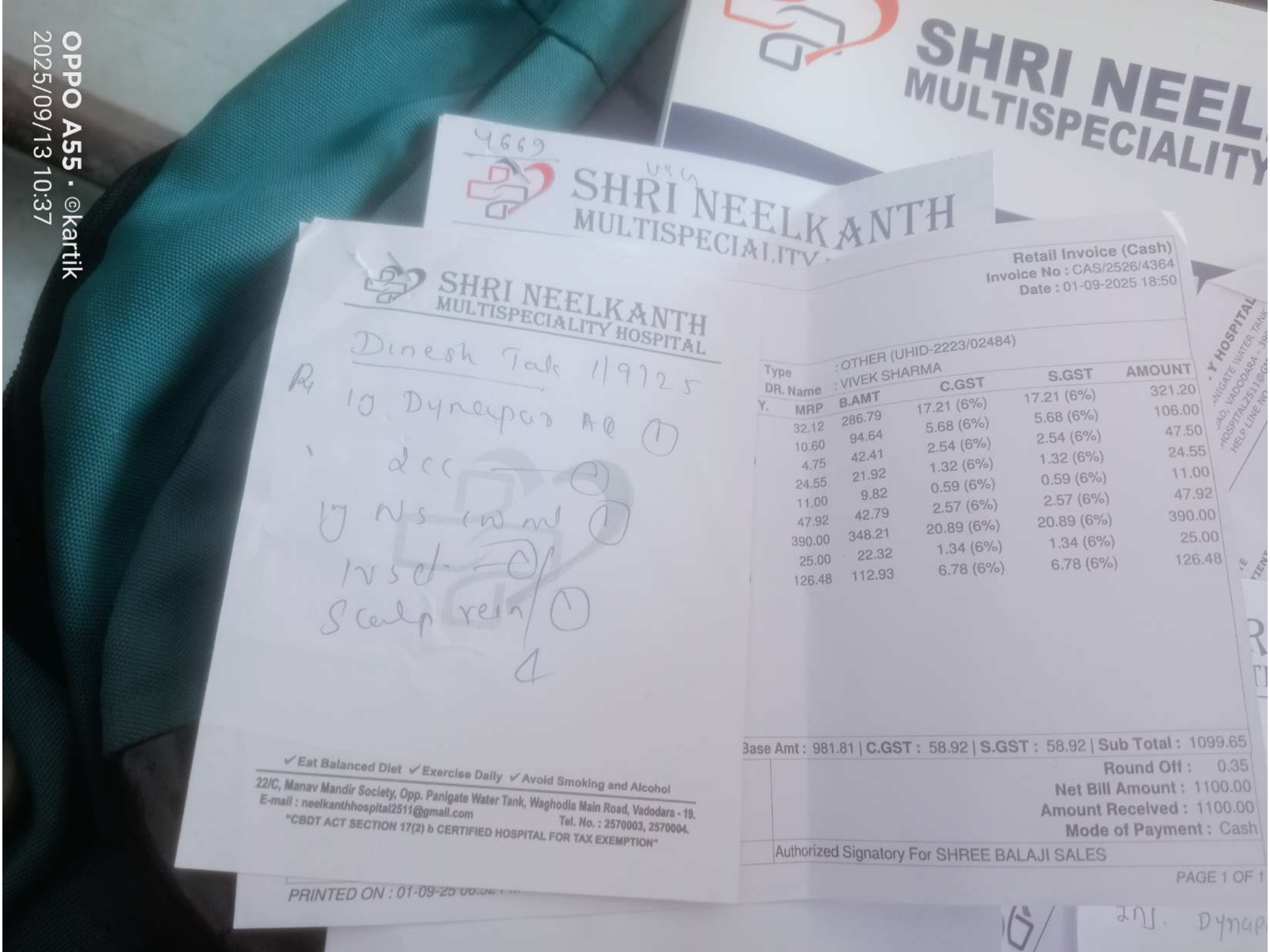
TAB Zifi LV 325 1-0-1 — (10)

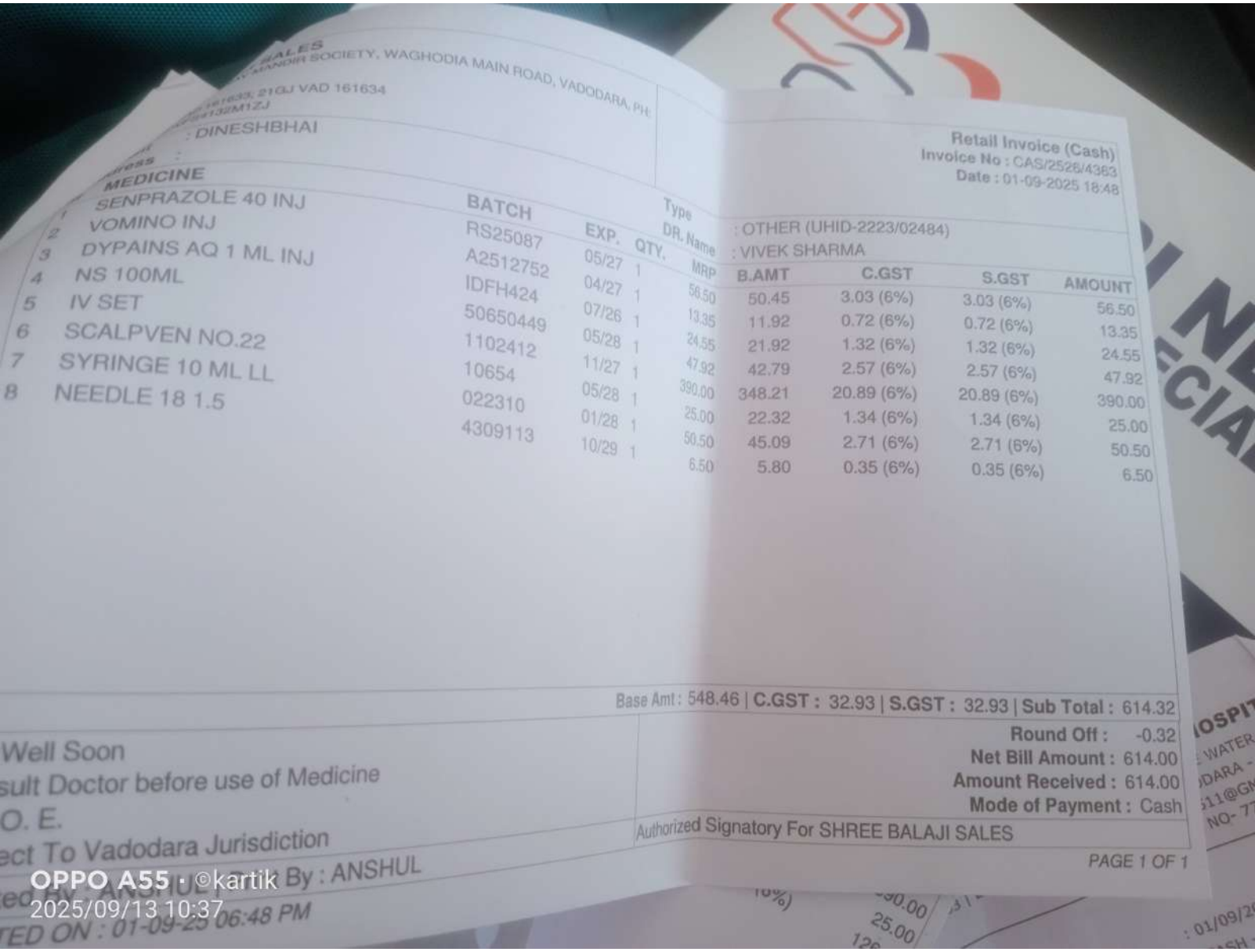
TAB Pan-D 1-0-1 — (10)

Inj Dynapar I/M Stat

Syp Clear UTI 10ml c water

2/C, Manav Mandir Society, Opp. Panigate Water Tank, Waghodia Main Road, Vadodara - 390019.
Tel. No. : 2570003, 2570004
Help Line No. : 7779038004
mail : neelkanthhospital2511@gmail.com
shrineelkanthhospital@gmail.com


OPPO A55 · ©kartik
2025/09/13 10:37
SHRI NEELKANTH
MULTISPECIALITY HOSPITAL
Dinesh Tak 11/9725
Retail Invoice (Cash)
Invoice No : CAS/2526/4364
Date : 01-09-2025 18:50
Type : OTHER (UHID-2223/02484)
DR. Name : VIVEK SHARMA
Y. MRP B.AMT C.GST S.GST AMOUNT
32.12 286.79 17.21 (6%) 17.21 (6%) 321.20
10.60 94.64 5.68 (6%) 5.68 (6%) 106.00
4.75 42.41 2.54 (6%) 2.54 (6%) 47.50
24.55 21.92 1.32 (6%) 1.32 (6%) 24.55
11.00 9.82 0.59 (6%) 0.59 (6%) 11.00
47.92 42.79 2.57 (6%) 2.57 (6%) 47.92
390.00 348.21 20.89 (6%) 20.89 (6%) 390.00
25.00 22.32 1.34 (6%) 1.34 (6%) 25.00
126.48 112.93 6.78 (6%) 6.78 (6%) 126.48
Base Amt : 981.81 | C.GST : 58.92 | S.GST : 58.92 | Sub Total : 1099.65
Round Off : 0.35
Net Bill Amount : 1100.00
Amount Received : 1100.00
Mode of Payment : Cash
Authorized Signatory For SHREE BALAJI SALES
PAGE 1 OF 1
✓Eat Balanced Diet ✓Exercise Daily ✓Avoid Smoking and Alcohol
22/C, Manav Mandir Society, Opp. Panigate Water Tank, Waghodia Main Road, Vadodara - 19.
E-mail : neelkanthhospital2511@gmail.com Tel. No. : 2570003, 2570004.
"CBDT ACT SECTION 17(2) b CERTIFIED HOSPITAL FOR TAX EXEMPTION"
PRINTED ON : 01-09-25
4669
Rx
1) Dynapar AQ (1)
2) CC
3) NS inj IM (1)
4) Inj D
5) Scalp vein (1)
4



...ALES
...MANDIR SOCIETY, WAGHODIA MAIN ROAD, VADODARA, PH:
...161633, 21GJ VAD 161634
...4132M1ZJ
: DINESHBHAI

Retail Invoice (Cash)
Invoice No : CAS/2526/4363
Date : 01-09-2025 18:48

Type : OTHER (UHID-2223/02484)
DR. Name : VIVEK SHARMA

	MEDICINE	BATCH	EXP.	QTY.	MRP	B.AMT	C.GST	S.GST	AMOUNT
1	SENPRAZOLE 40 INJ	RS25087	05/27	1	56.50	50.45	3.03 (6%)	3.03 (6%)	56.50
2	VOMINO INJ	A2512752	04/27	1	13.35	11.92	0.72 (6%)	0.72 (6%)	13.35
3	DYPAINS AQ 1 ML INJ	IDFH424	07/26	1	24.55	21.92	1.32 (6%)	1.32 (6%)	24.55
4	NS 100ML	50650449	05/28	1	47.92	42.79	2.57 (6%)	2.57 (6%)	47.92
5	IV SET	1102412	11/27	1	390.00	348.21	20.89 (6%)	20.89 (6%)	390.00
6	SCALPVEN NO.22	10654	05/28	1	25.00	22.32	1.34 (6%)	1.34 (6%)	25.00
7	SYRINGE 10 ML LL	022310	01/28	1	50.50	45.09	2.71 (6%)	2.71 (6%)	50.50
8	NEEDLE 18 1.5	4309113	10/29	1	6.50	5.80	0.35 (6%)	0.35 (6%)	6.50

Base Amt : 548.46 | C.GST : 32.93 | S.GST : 32.93 | Sub Total : 614.32

Round Off : -0.32
Net Bill Amount : 614.00
Amount Received : 614.00
Mode of Payment : Cash

Well Soon
sult Doctor before use of Medicine
O. E.
ect To Vadodara Jurisdiction
...ed By : ANSHUL
...TED ON : 01-09-25 06:48 PM

Authorized Signatory For SHREE BALAJI SALES

PAGE 1 OF 1

Parth Imaging Center

al X-rays
le Body Ultrasonography
ur Doppler Study
S. Guided Interventional Procedures
iopsy Consultation

Dr. Bhavin Shah (M.D.)
Consultant Radiologist

Clinical Experience
- Nanavati Hospital (Bombay)
- Tata Memorial Hospital (Bombay)
- Kailash Cancer Hospital, Goraj

PATIENT'S NAME: DINESH TAK, M/23Y
DATE: 01.09.2025

USG Finding	Mild hydronephrosis on right side along with mild ipsilateral upper and mid hydro-ureter; right distal ureter – obscured by bowel gas
Suggestion	CT KUB/ CTIVP to evaluate for the possibility of right distal ureteric calculus

Ultrasonography of abdomen & Pelvis

HEPATO-BILIARY SYSTEM:

Liver:
It measures 118mm in its CC dimension. Its surface is smooth. It reveals normal homogeneous echo-pattern. No evidence of focal lesion (solid/cystic) is seen. Portal vein measures 9.4mm at porta hepatis. It reveals normal hepato-petal flow. Perihepatic space appears clear.

Gall Bladder & Biliary System:
Is optimally distended. Its fundus, body, neck and cystic duct are well visualized. No evidence of calculus/wall thickening/ pericholecystic collection is seen. No evidence of dilatation of intrahepatic biliary radicals is seen. CBD is normal.

Pancreas:
It is of normal size, shape and echo-pattern. No evidence of solid/cystic lesion is seen. MPD appears normal. No evidence of Peripancreatic fluid is seen. Pancreatic tail appears normal.

Spleen:
It measures 116mm along its long axis. It reveals normal shape and echo-pattern. No evidence of solid/cystic lesion is seen within.

URINARY SYSTM;

Right Kidney:
It measures 99mm in its CC span. Cortico-medullary differentiation appears normal. No evidence of calculus is seen. **It reveals mild hydronephrosis along with mild ipsilateral upper and mid hydro-ureter. Right distal ureter is obscured by bowel gas.** No evidence of solid/ cystic lesion is seen. Perinephric space appears clear.

Left Kidney:
It measures 107mm in its CC span. Cortico-medullary differentiation appears normal. No evidence of calculus / hydronephrosis is seen. No evidence of solid/ cystic lesion is seen. Perinephric space appears clear.

No evidence of hydro-ureter is seen on left side.
Bilateral uretero-vesical junctions appear normal.

Dr. Bhavin Shah
(Consultant Radiologist)

A-101, Vraj-II, Uma Char Rasta, Waghodia Road, Vadodara-390 019.
Mobile : 9624708315 • E-mail : drbhavinbshah@gmail.com
Time : 9.00 am to 8.00 pm (Monday to Saturday)

10/09/25

c/o: Pain at right flank

Rx

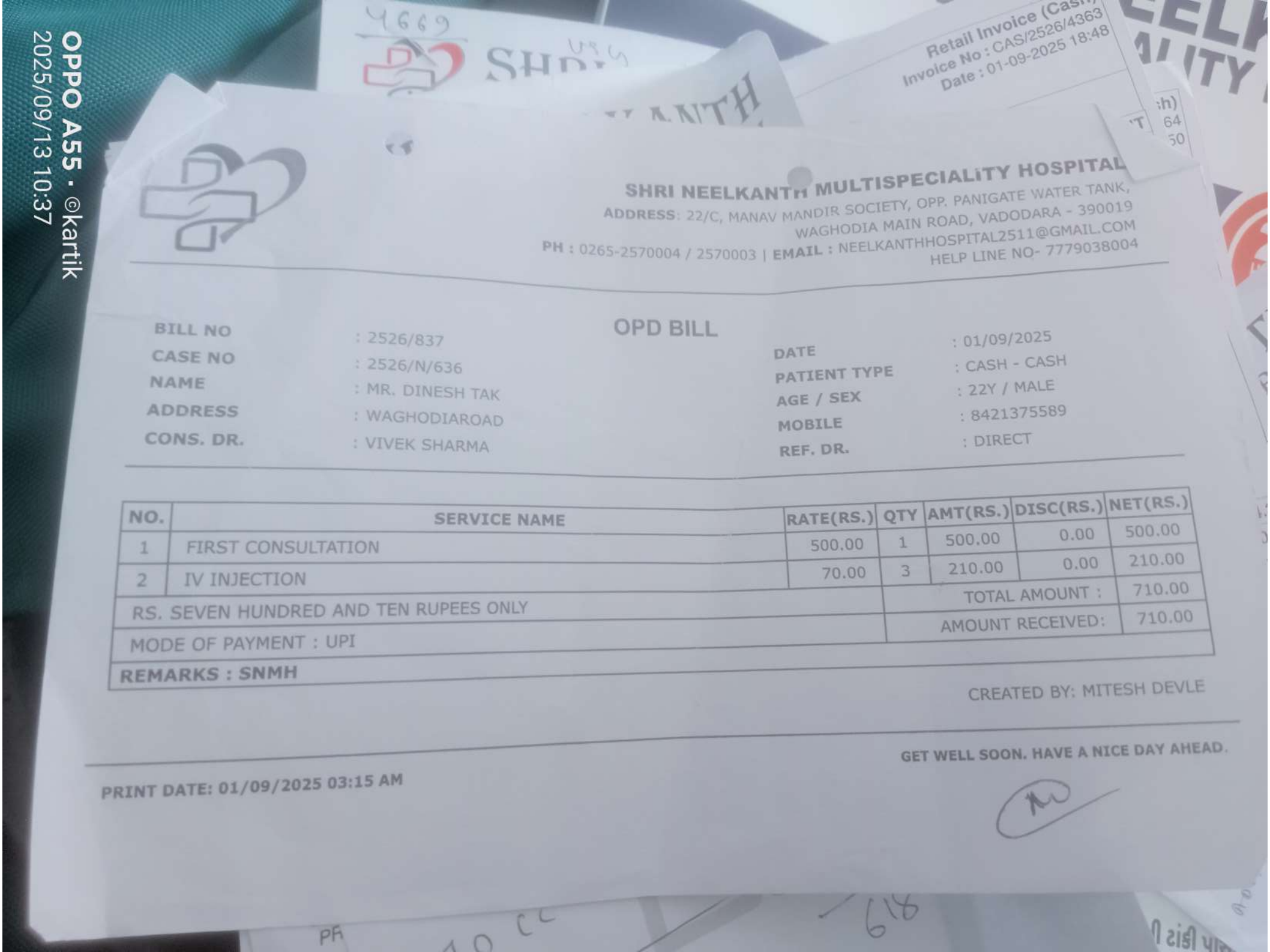
Inj. Dynapar AQ 1 Amp | 100 ml NS IV stat

Tab. Lenoflox (500) 0+0 (5)

Tab. Pan D (40) 1+0 (10)

Tab. Catcospa 1+0 (10)

Syp. Alkin 4 tsf TDS ē glass of water.



Retail Invoice (Cash)
Invoice No : CAS/2526/4363
Date : 01-09-2025 18:48

SHRI NEELKANTH MULTISPECIALITY HOSPITAL
ADDRESS: 22/C, MANAV MANDIR SOCIETY, OPP. PANIGATE WATER TANK,
WAGHODIA MAIN ROAD, VADODARA - 390019
PH : 0265-2570004 / 2570003 | EMAIL : NEELKANTHHOSPITAL2511@GMAIL.COM
HELP LINE NO- 7779038004

OPD BILL

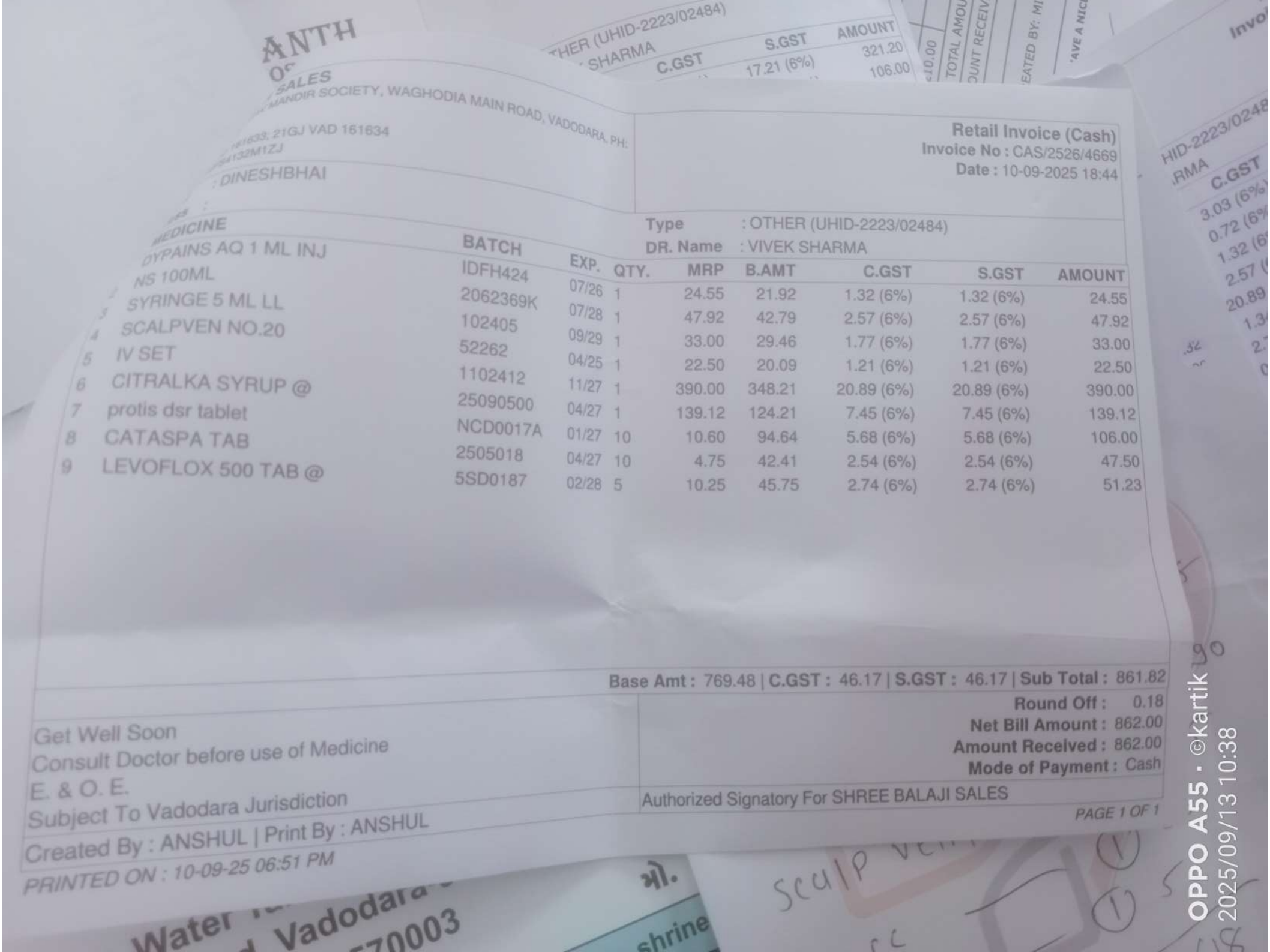
BILL NO	: 2526/837	DATE	: 01/09/2025
CASE NO	: 2526/N/636	PATIENT TYPE	: CASH - CASH
NAME	: MR. DINESH TAK	AGE / SEX	: 22Y / MALE
ADDRESS	: WAGHODIAROAD	MOBILE	: 8421375589
CONS. DR.	: VIVEK SHARMA	REF. DR.	: DIRECT

NO.	SERVICE NAME	RATE(RS.)	QTY	AMT(RS.)	DISC(RS.)	NET(RS.)
1	FIRST CONSULTATION	500.00	1	500.00	0.00	500.00
2	IV INJECTION	70.00	3	210.00	0.00	210.00
RS. SEVEN HUNDRED AND TEN RUPEES ONLY				TOTAL AMOUNT :		710.00
MODE OF PAYMENT : UPI				AMOUNT RECEIVED:		710.00
REMARKS : SNMH						

CREATED BY: MITESH DEVLE

PRINT DATE: 01/09/2025 03:15 AM

GET WELL SOON. HAVE A NICE DAY AHEAD.



ANTH
O
SALES
MANDIR SOCIETY, WAGHODIA MAIN ROAD, VADODARA. PH:
HE1633; 21GJ VAD 161634
54132M1ZJ
: DINESHBHAI

Retail Invoice (Cash)
Invoice No : CAS/2526/4669
Date : 10-09-2025 18:44

Type : OTHER (UHID-2223/02484)
DR. Name : VIVEK SHARMA

	MEDICINE	BATCH	EXP.	QTY.	MRP	B.AMT	C.GST	S.GST	AMOUNT
	DYPAINS AQ 1 ML INJ	IDFH424	07/26	1	24.55	21.92	1.32 (6%)	1.32 (6%)	24.55
	NS 100ML	2062369K	07/28	1	47.92	42.79	2.57 (6%)	2.57 (6%)	47.92
3	SYRINGE 5 ML LL	102405	09/29	1	33.00	29.46	1.77 (6%)	1.77 (6%)	33.00
4	SCALPVEN NO.20	52262	04/25	1	22.50	20.09	1.21 (6%)	1.21 (6%)	22.50
5	IV SET	1102412	11/27	1	390.00	348.21	20.89 (6%)	20.89 (6%)	390.00
6	CITRALKA SYRUP @	25090500	04/27	1	139.12	124.21	7.45 (6%)	7.45 (6%)	139.12
7	protis dsr tablet	NCD0017A	01/27	10	10.60	94.64	5.68 (6%)	5.68 (6%)	106.00
8	CATASPA TAB	2505018	04/27	10	4.75	42.41	2.54 (6%)	2.54 (6%)	47.50
9	LEVOFLOX 500 TAB @	5SD0187	02/28	5	10.25	45.75	2.74 (6%)	2.74 (6%)	51.23

Base Amt : 769.48 | **C.GST :** 46.17 | **S.GST :** 46.17 | **Sub Total :** 861.82
Round Off : 0.18
Net Bill Amount : 862.00
Amount Received : 862.00
Mode of Payment : Cash

Get Well Soon
Consult Doctor before use of Medicine
E. & O. E.
Subject To Vadodara Jurisdiction
Created By : ANSHUL | Print By : ANSHUL
PRINTED ON : 10-09-25 06:51 PM

Authorized Signatory For SHREE BALAJI SALES

PAGE 1 OF 1

SHRI NEELKANTH
MULTISPECIALITY HOSPITAL

Dinesh

Inj. Panto 40 mg — (1) 56

Inj. ~~Inj~~ Imeset — (1) 14

Inj. Dynapar — (1) 30

Inj.

NS 100 — (1) 48

IV set — (1) 390

Scalp vein — (1) 25

10 cc — (1) 50

18 ½ — (1) 5

618

22/C, Manav Mandir Society, Opp. Panigate Water Tank, Waghodia Main Road, Vadodara - 390019.
Tele No.: 0265-2570003, 2570004 Help Line No.: 7779038004
Email : neelkanthhospital2511@gmail.com, shrineelkanthhospital@gmail.com
"CBDT ACT SECTION 17(2) b CERTIFIED HOSPITAL FOR TAX EXEMPTION"
1. Eat Balance diet 2. Exercise Daily 3. Avoid Smoking and Alcohol

4669

SHRI NEELKANTH
MULTISPECIALITY HOSPITAL

Dinesh. 11/9/25.

c/o: Pain at right flank & radiation to hypogastric region.

ADV:

Inj. Diclofenac Aq 1 amp/100 ml NS IV stat

1. Cataflam tab (10)
1. Pan D (40) tab (10)
1. Augmentin 625 tab (10)

22/C, Manav Mandir Society, Opp. Panigate Water Tank, Waghodia Main Road, Vadodara - 390019.
Tele No.: 0265-2570003, 2570004 Help Line No.: 7779038004
hospital2511@gmail.com, shrineelkanthhospital@gmail.com

Parul® University

NAAC A++

Stream cipher and Block Cipher

Chapter-3: Block Ciphers and the Data Encryption Standard

Mohammad Asif
Assistant Professor
Department of Computer Science and Engineering

Content

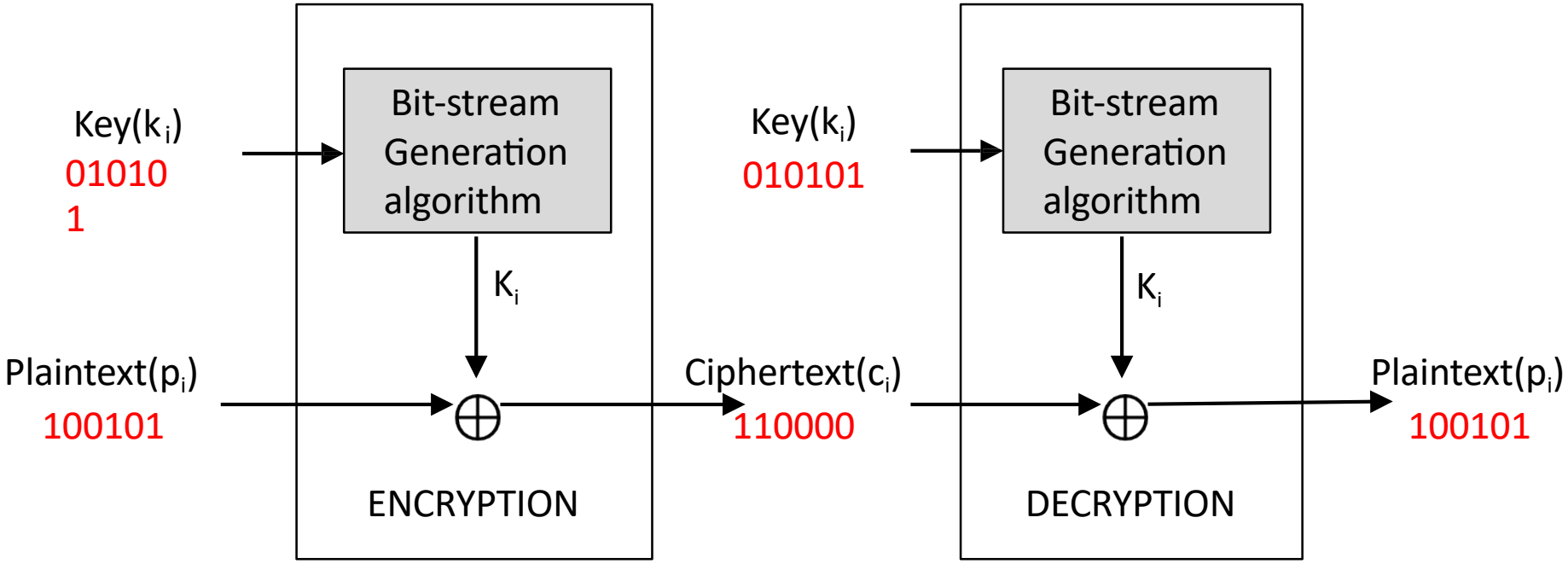
Stream cipher and Block Cipher:

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

Examples:

Autokeyed Vigenère cipher
A5/1
RC4
Vern
am
ciph
er.

Stream cipher and Block Cipher:



Stream cipher and Block Cipher:

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used.

Examples:

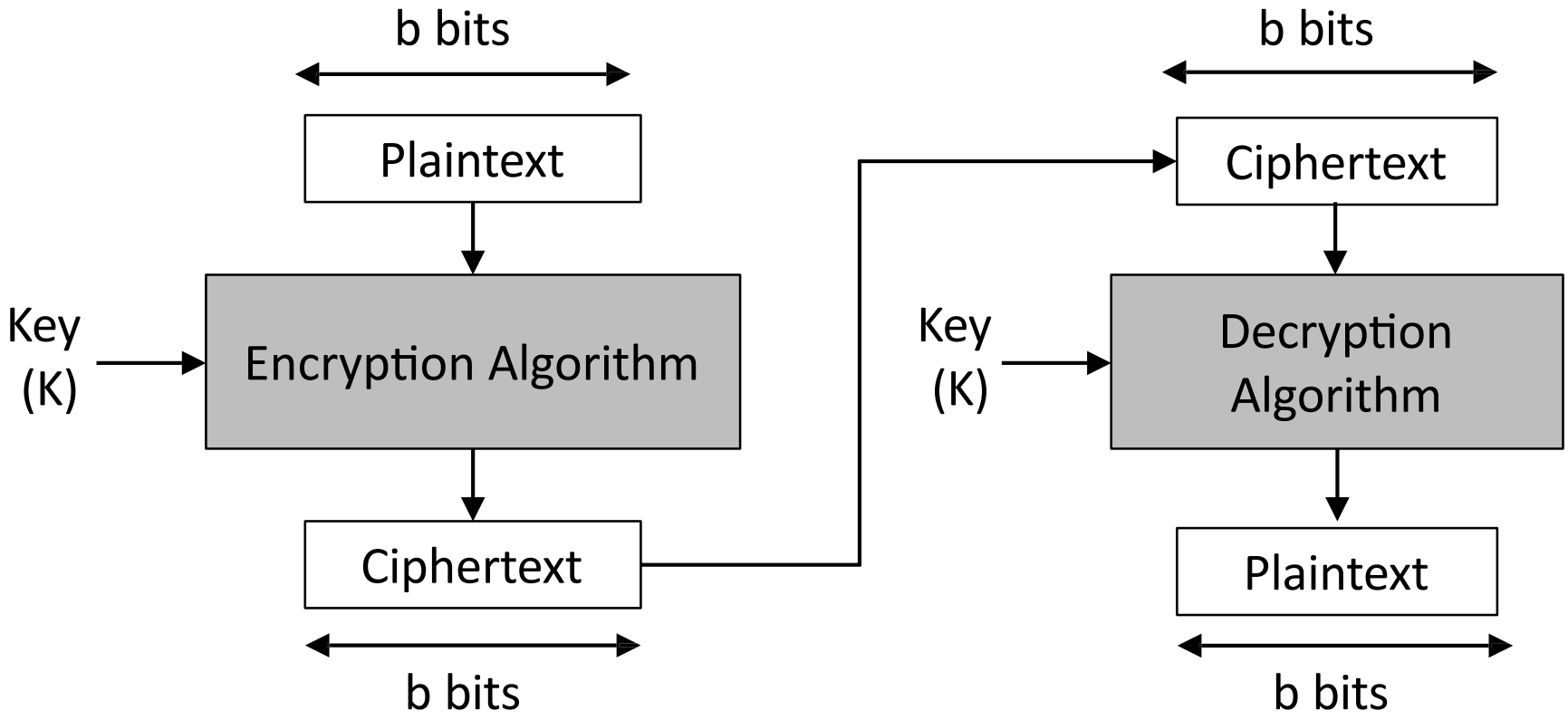
Feistel cipher

DES

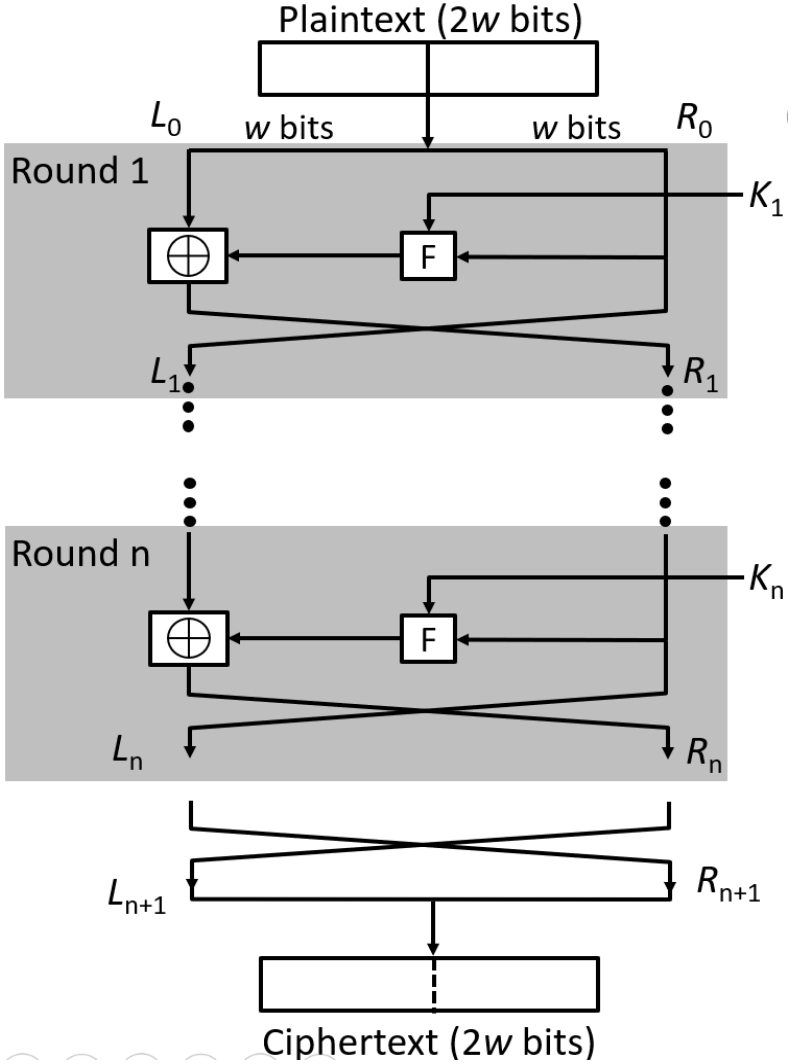
Triple DES

AES

Stream cipher and Block Cipher:



Block Cipher Principle – Fiestel Structure



1. Plaintext is split into 32-bit halves L_i and R_i
2. R_i is fed into the function F.
3. The output of function F is then XORed with L_i
4. Left and right half are swapped.

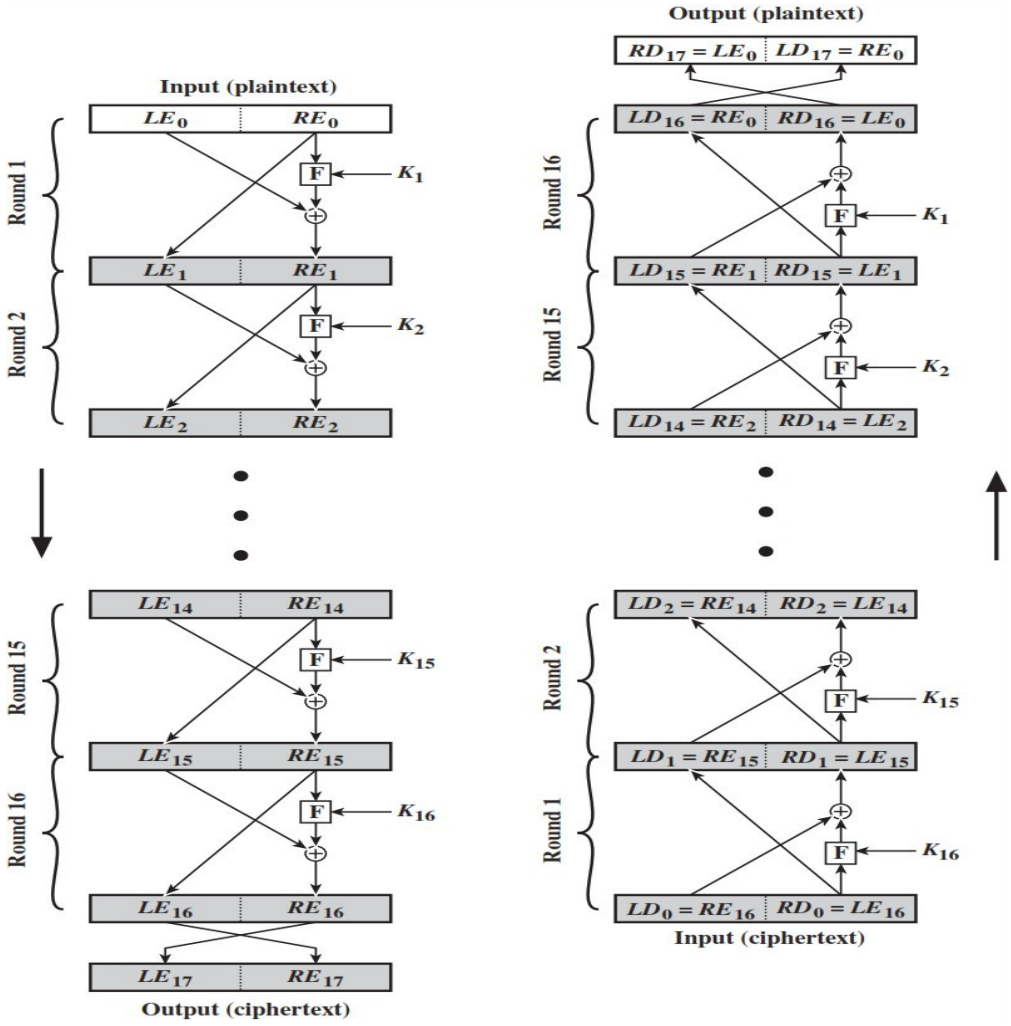
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

$$L_i = R_{i-1}$$

Block Cipher Principle – Fiestel Structure

1. **Block size:** Common block size of 64-bit. However, the new algorithms uses a 128-bit, 256-bit block size.
2. **Key size:** Key sizes of 64 bits or less are now widely considered to be insufficient, and 128 bits has become a common size.
3. **Number of rounds**: A typical size is 16 rounds.
4. **Round function F:** This phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions. Again, greater complexity generally means greater resistance to cryptanalysis.
5. **Subkey generation algorithm:** For each of the sixteen rounds, a different subkey (Ki) derived from main key by the combination of a left circular shift and a permutation. Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

Block Cipher Principle – Fiestel Structure



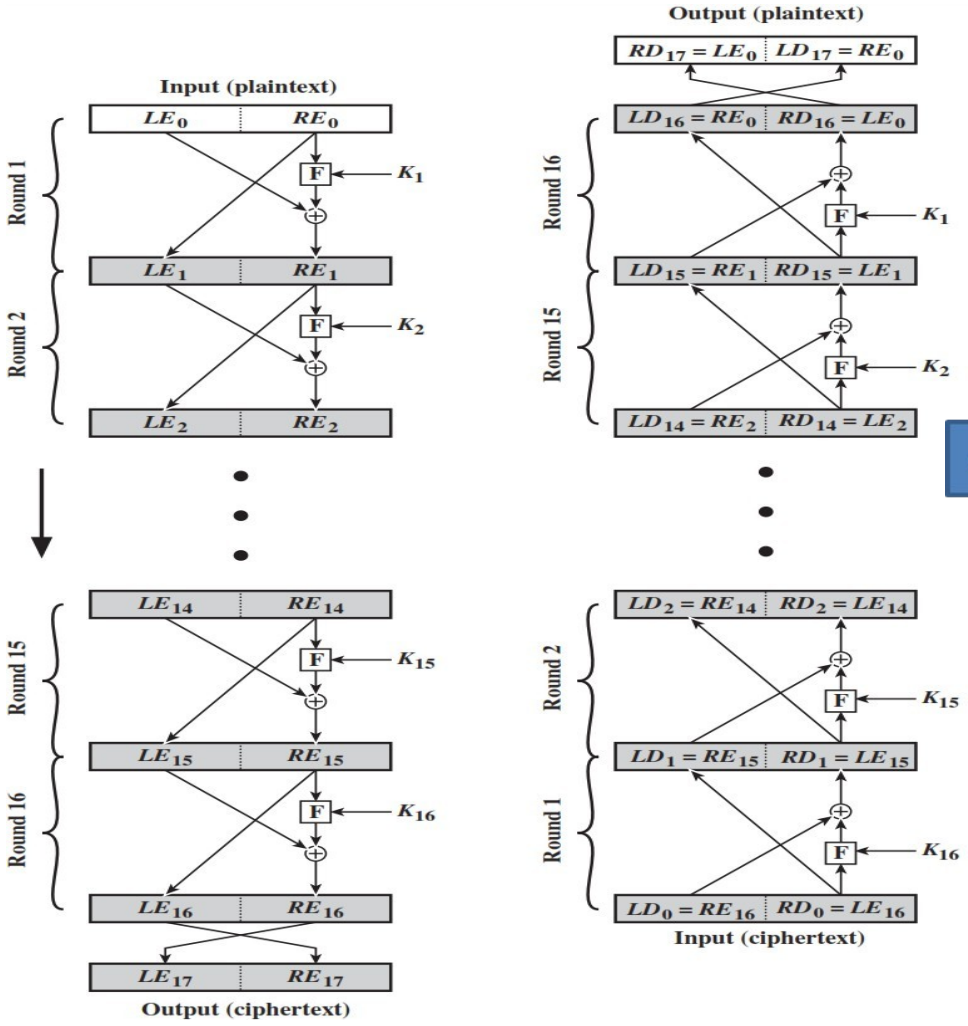
Prove that o/p of first round of Decryption is equal to 32-bit swap o i/p of 16th round of Encryption LD1=RE15 & RD1=LE15

On Encryption Side:

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

Block Cipher Principle – Fiestel Structure



On Decryption Side:

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$

$$RD_1 = LD_0 \oplus F(RD_0, K_{16})$$

$$= RE_{16} \oplus F(RE_{15}, K_{16})$$

$$= [LE_{15} \oplus F(RE_{15}, K_{16})] \oplus F(RE_{15}, K_{16})$$

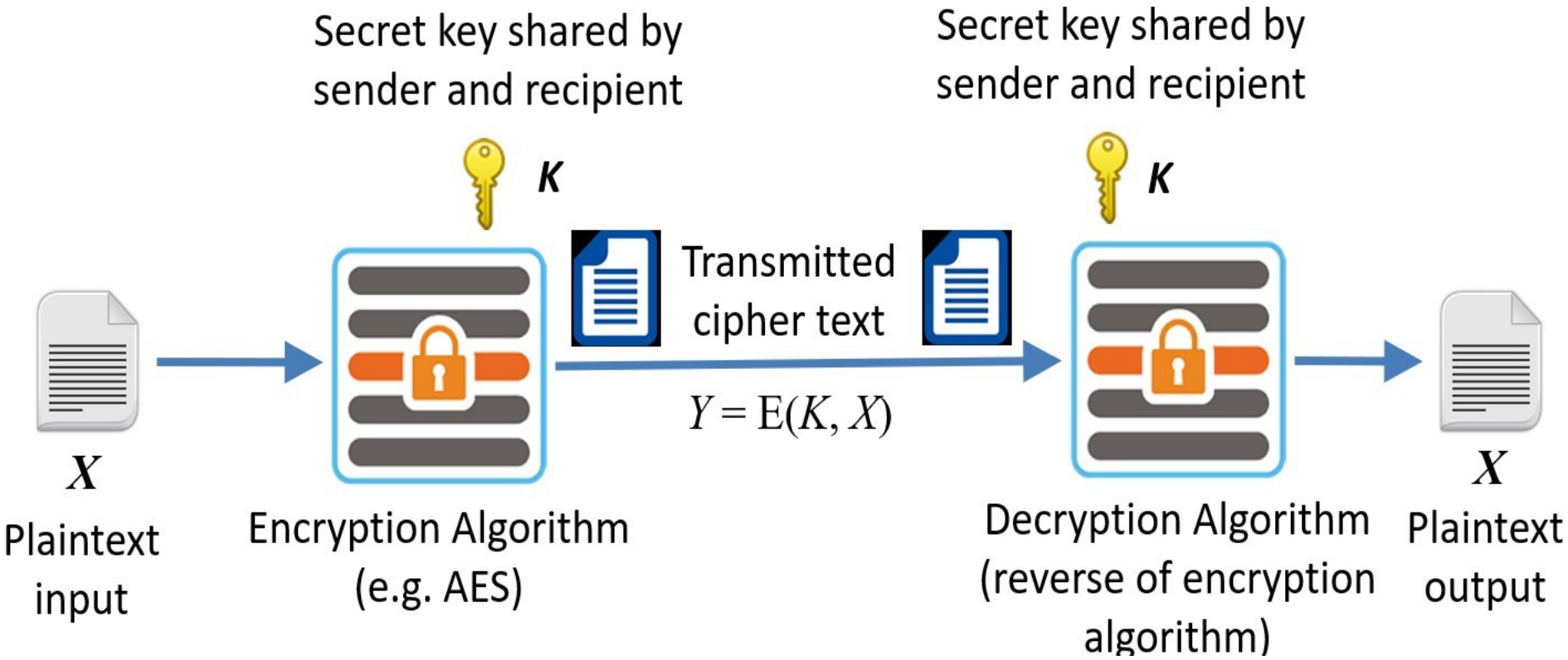
Thus,

$$LD_1 = RE_{15} \;\&\; RD_1 = LE_{15}$$

XOR Associativity Property

$$\because [A \oplus B] \oplus C = A \oplus [B \oplus C]$$

Symmetric Cipher Model



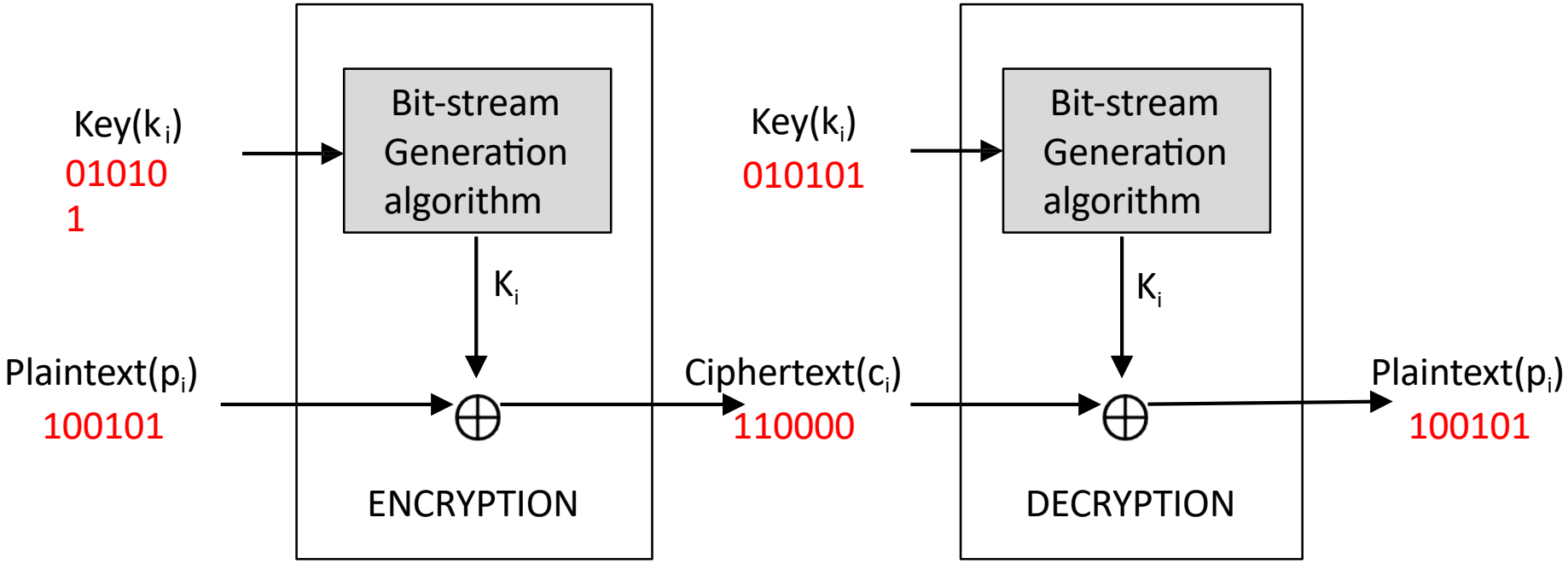
Stream cipher and Block Cipher:

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

Examples:

Autokeyed Vigenère cipher
A5/1
RC4
Vern
am
ciph
er.

Stream cipher and Block Cipher:



Stream cipher and Block Cipher:

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used.

Examples:

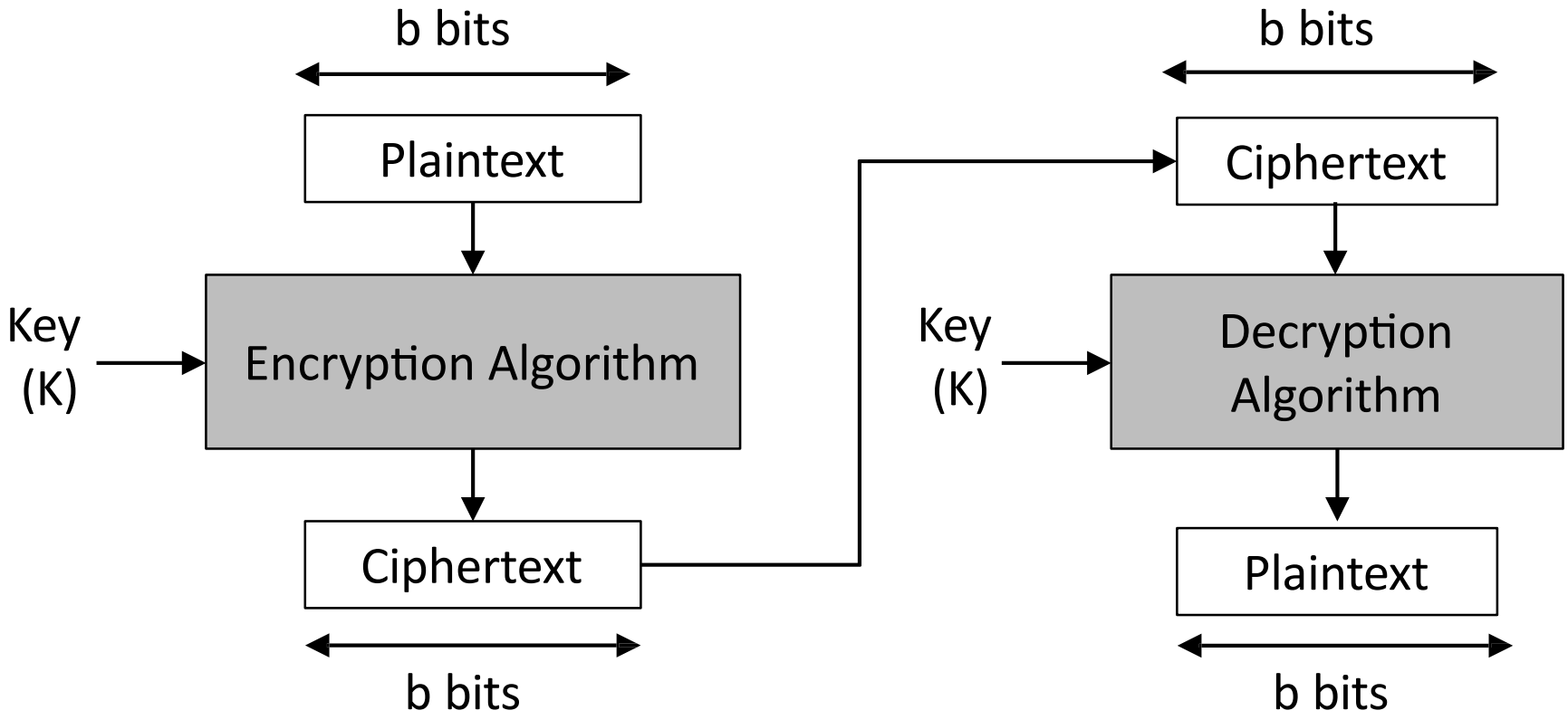
Feistel cipher

DES

Triple DES

AES

Stream cipher and Block Cipher:



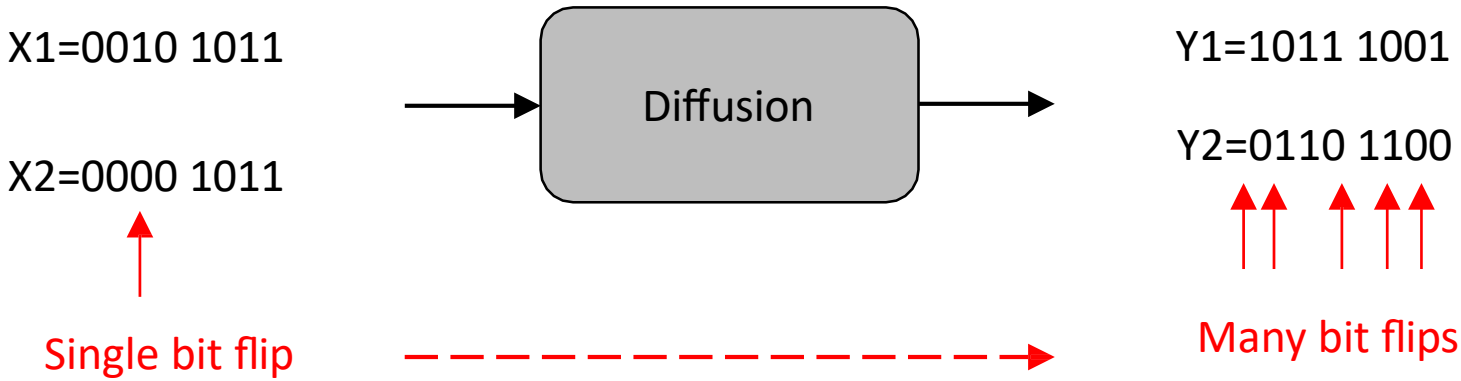
Confusion & Diffusion:

Confusion

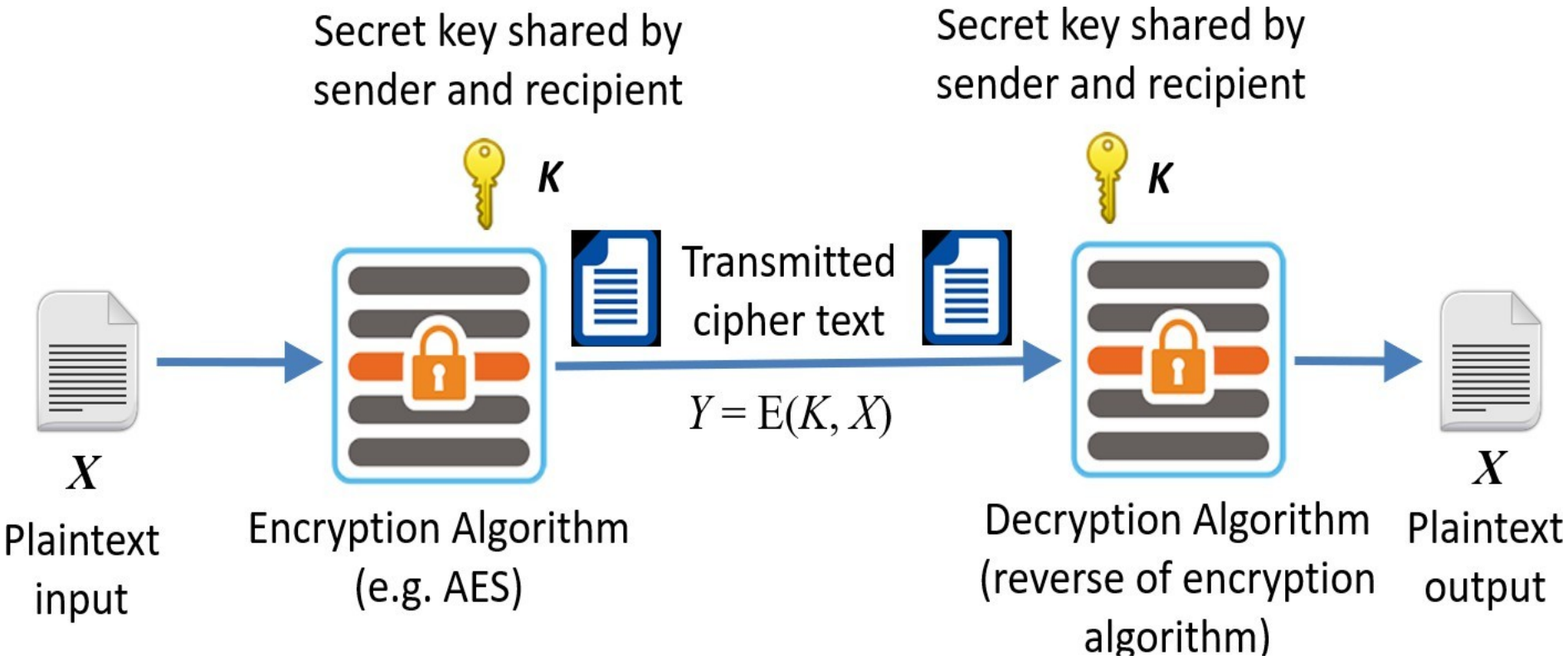
- Confusion hides the relationship between the cipher text and the key.
- This is achieved by the use of a complex substitution algorithm.

Diffusion

- Diffusion hides the relationship between the cipher text and the plaintext.
- This is achieved by changing one plaintext digit which affect the value of many cipher text digits.

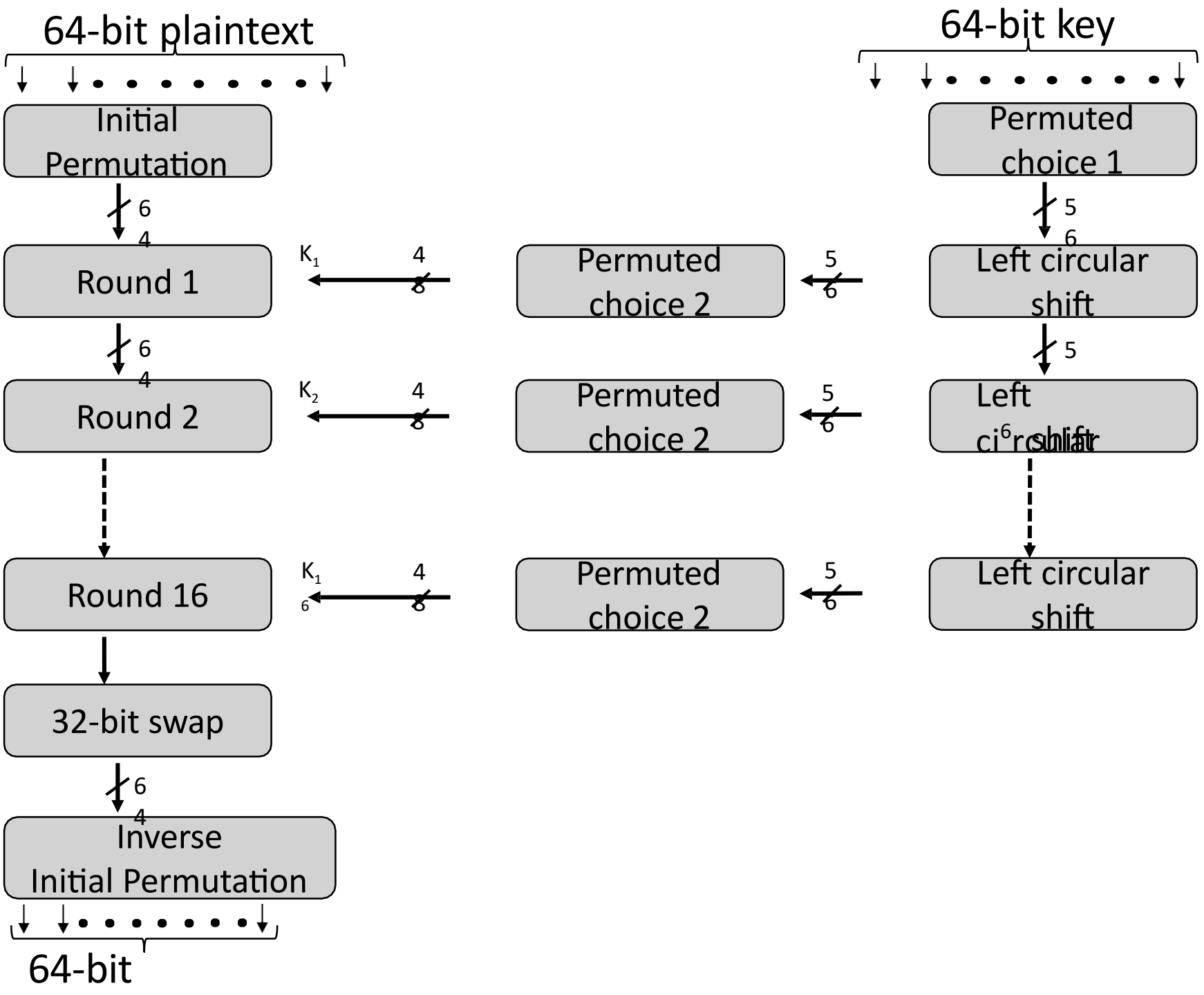


Symmetric Cipher Model

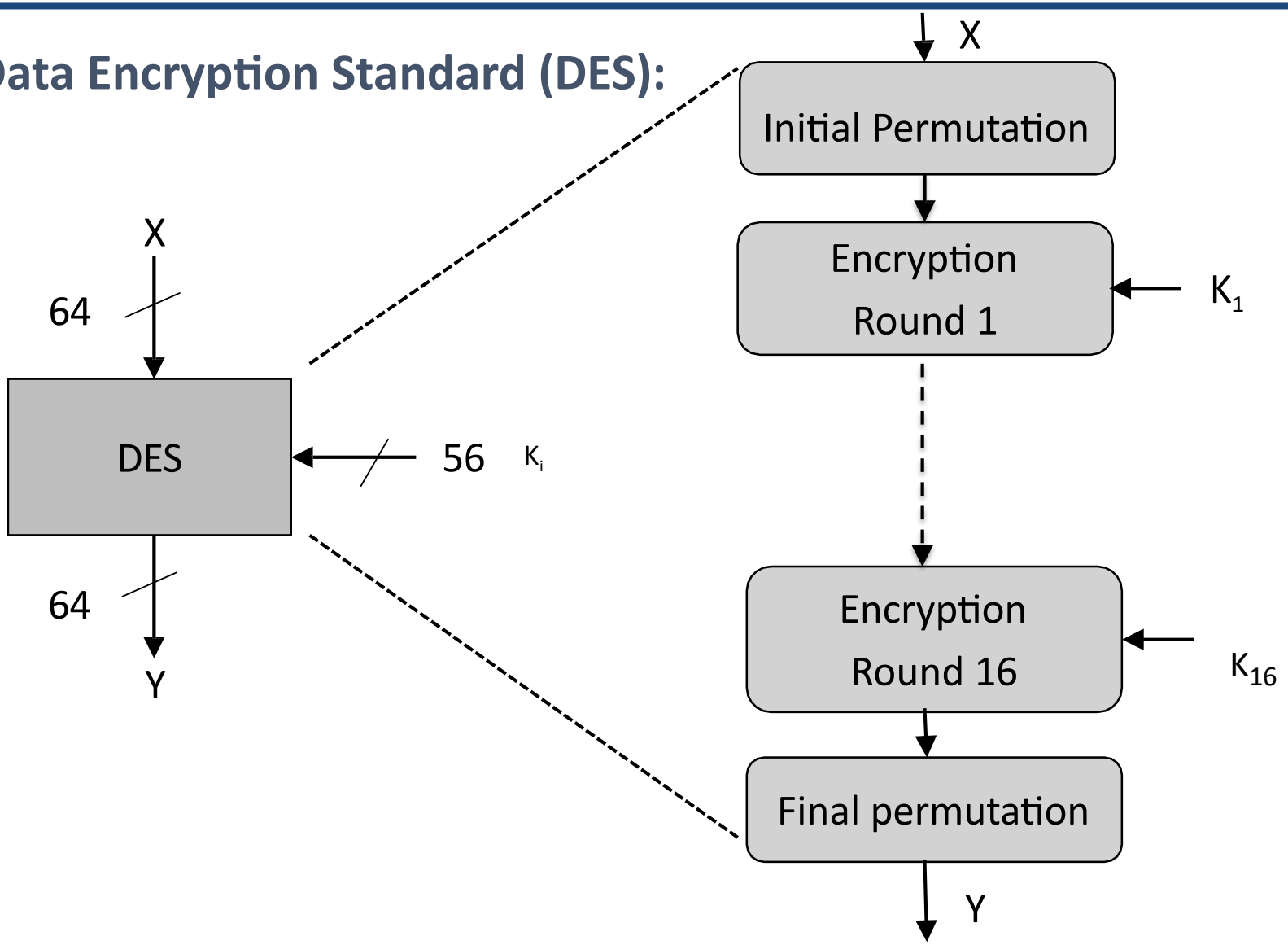


Data Encryption Standard (DES):

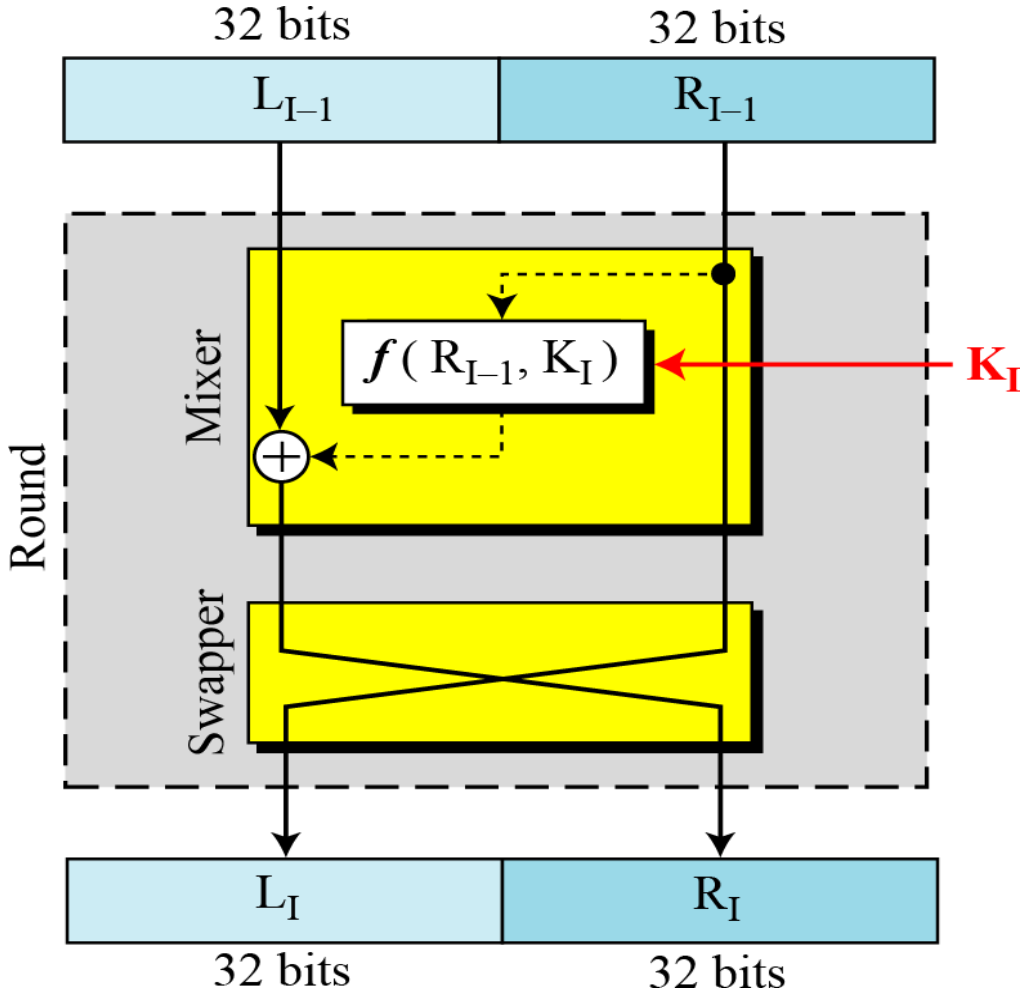
Type: Block Cipher
Block Size : 64-bit
Key Size: 64-bit,
with only 56-bit
effective
Number of
Rounds: 16

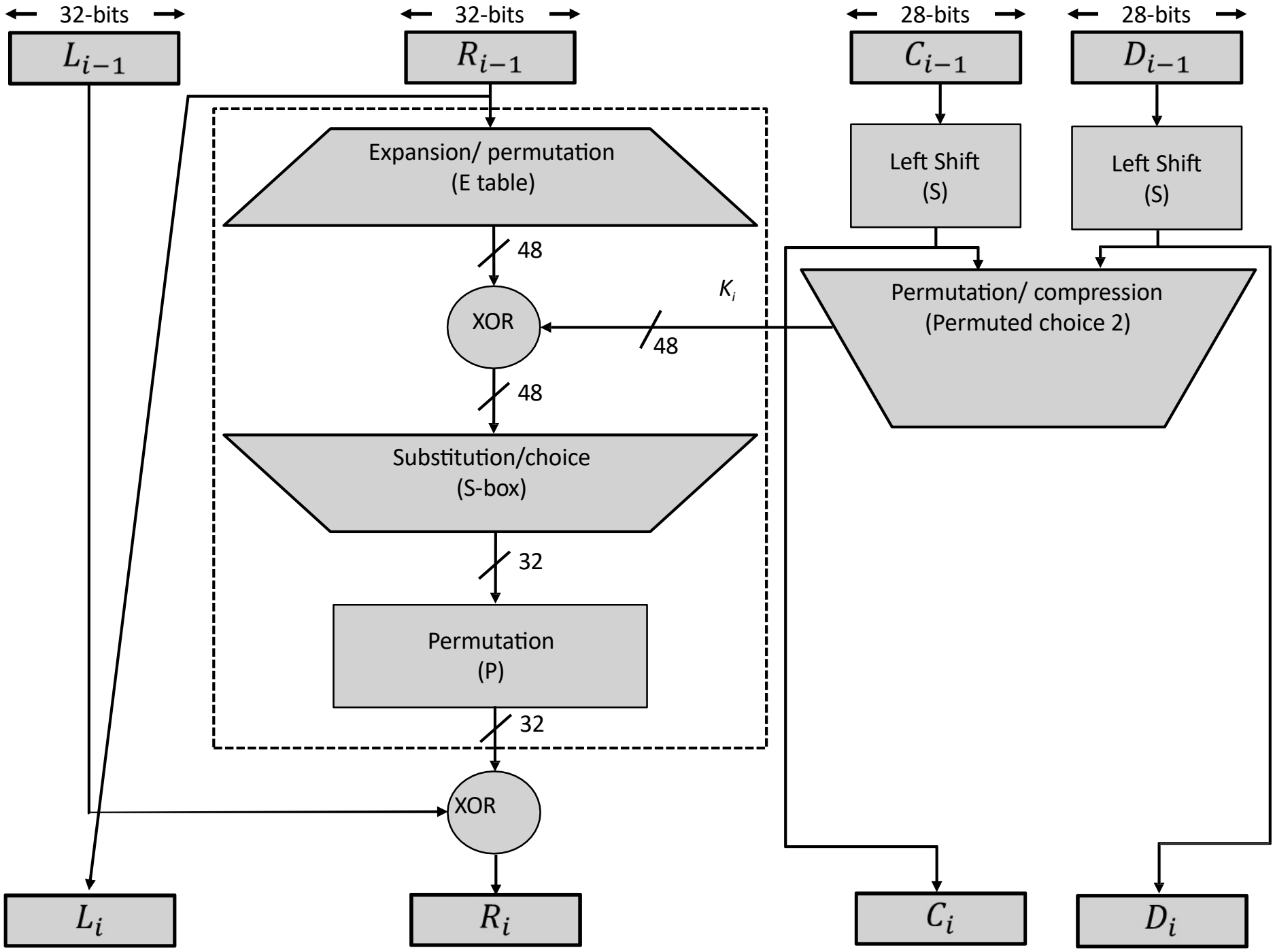

64-bit plaintext
64-bit key
Initial Permutation
Permuted choice 1
64
56
Round 1
Permuted choice 2
Left circular shift
48
56
K1
Round 2
Permuted choice 2
Left circular shift
48
56
K2
Round 16
Permuted choice 2
Left circular shift
48
56
K16
32-bit swap
64
Inverse Initial Permutation
64-bit

Data Encryption Standard (DES):



Data Encryption Standard (DES) – Single round of DES:



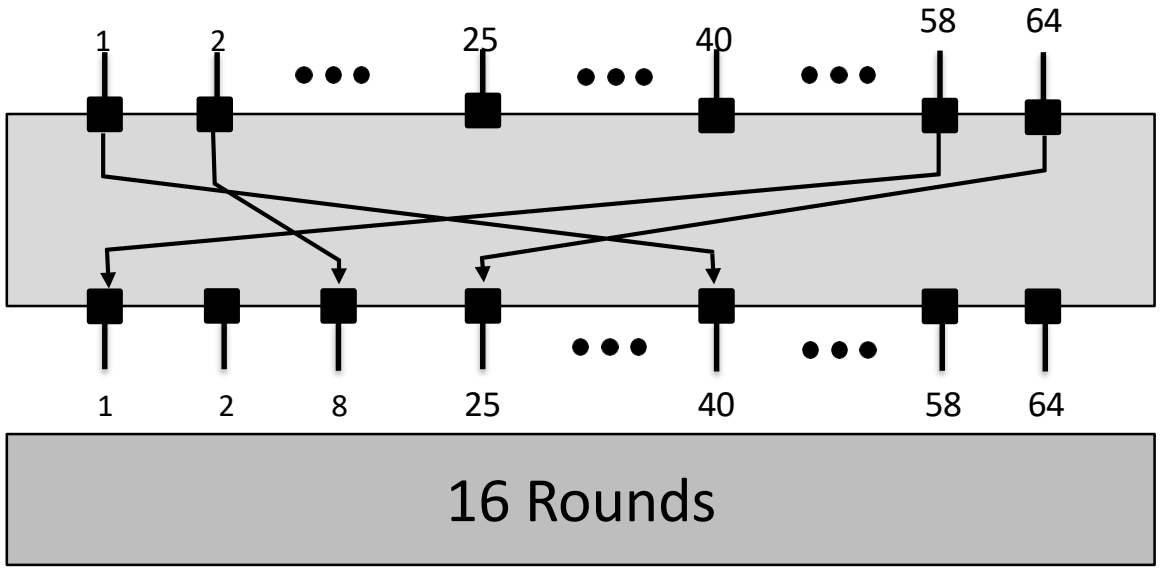

32-bits
32-bits
28-bits
28-bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion/ permutation
(E table)
Left Shift
(S)
Left Shift
(S)
48
K_i
XOR
48
Permutation/ compression
(Permuted choice 2)
48
Substitution/choice
(S-box)
32
Permutation
(P)
32
XOR
L_i
R_i
C_i
D_i

Data Encryption Standard (DES):

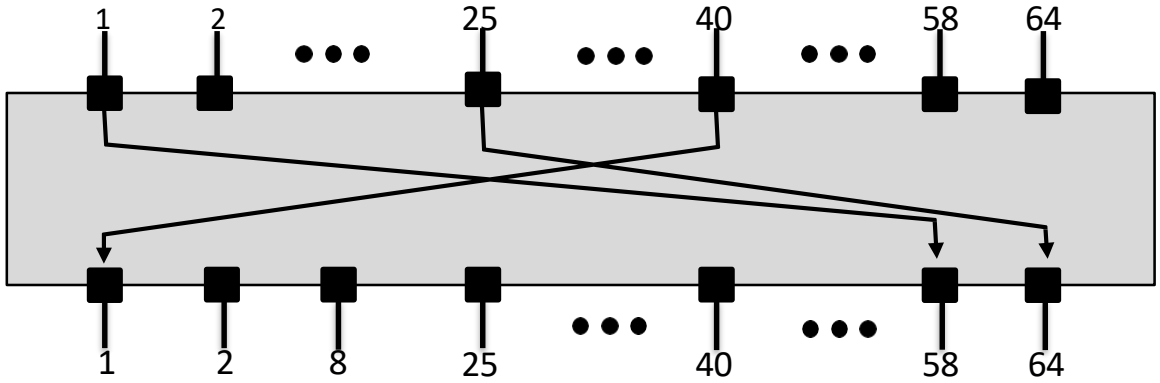
1. Initial permutation: First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
2. The F function: This phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.
3. Swap: L and R swapped again at the end of the cipher, i.e., after round 16 followed by a final permutation.
4. Inverse (Final) permutation: It is the inverse of the initial permutation.
5. Subkey generation: For each of the sixteen rounds, a different subkey (Ki) derived from main key by the combination of a left circular shift and a permutation.

Data Encryption Standard (DES): - Initial Permutation

The initial permutation of the DES algorithm changes the order of the plaintext prior to the first round of encryption



The final permutation occurs after the sixteen rounds of DES are completed. It is the inverse of the initial permutation.



Data Encryption Standard (DES): Initial and Final 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

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

Data Encryption Standard (DES): The f Function

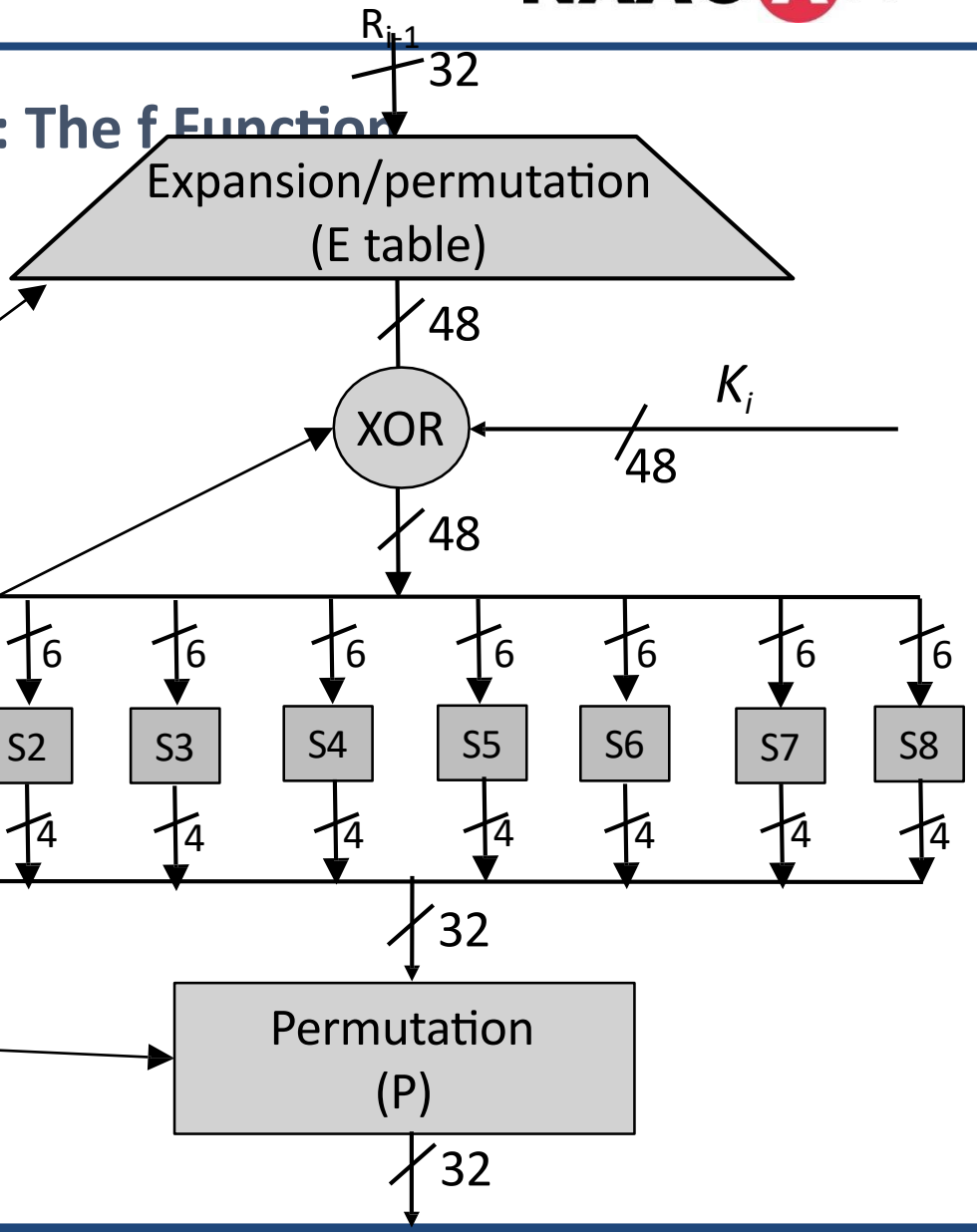
1. Main operation of DES
- f-function inputs:
  Ri-1 and round key *ki*
- **4 Steps**:

1. Expansion E

2. XOR with round key

3. S-box substitution

4. Permutation



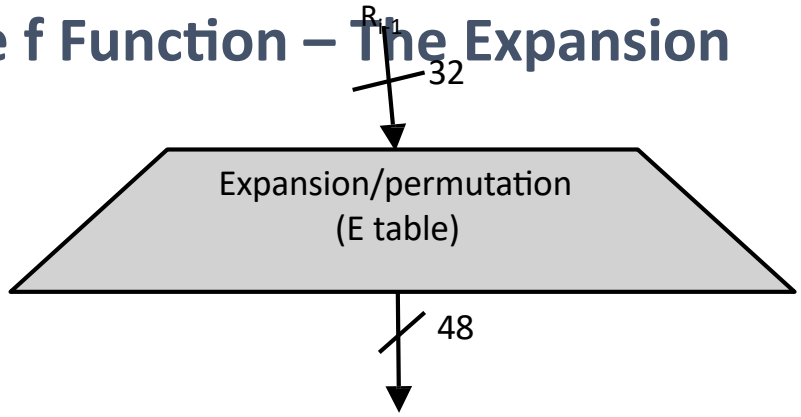
Data Encryption Standard (DES): The f Function – The Expansion Function

Main purpose: **Increases diffusion**

Since Ri-1 is a 32-bit input and Ki is a 48-bit key, we first need to expand Ri-1 to 48 bits.

Input: (8 blocks, each of them consisting 4 bits) - 32 bits

Output: (8 blocks, each of them consisting 6 bits) – 48 bits



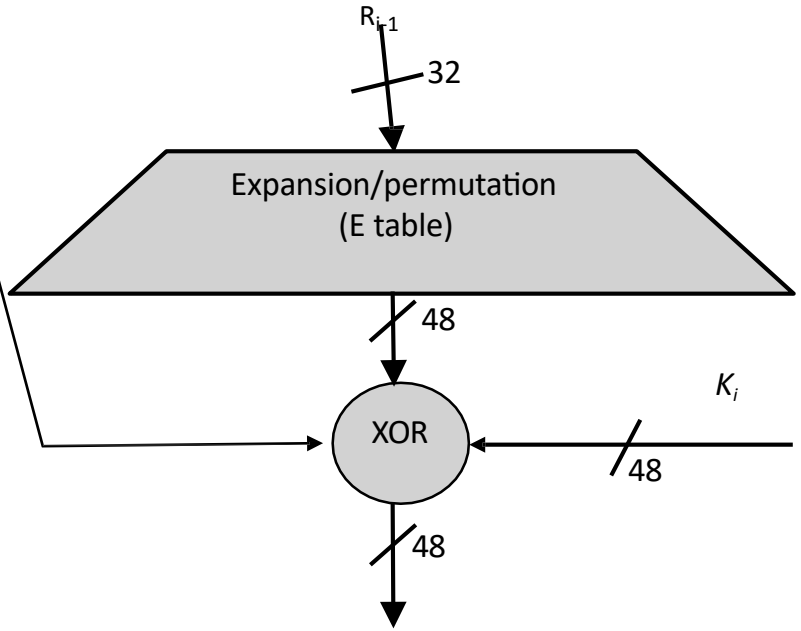
Expansion Table E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Data Encryption Standard (DES): XOR round Key

XOR Round Key

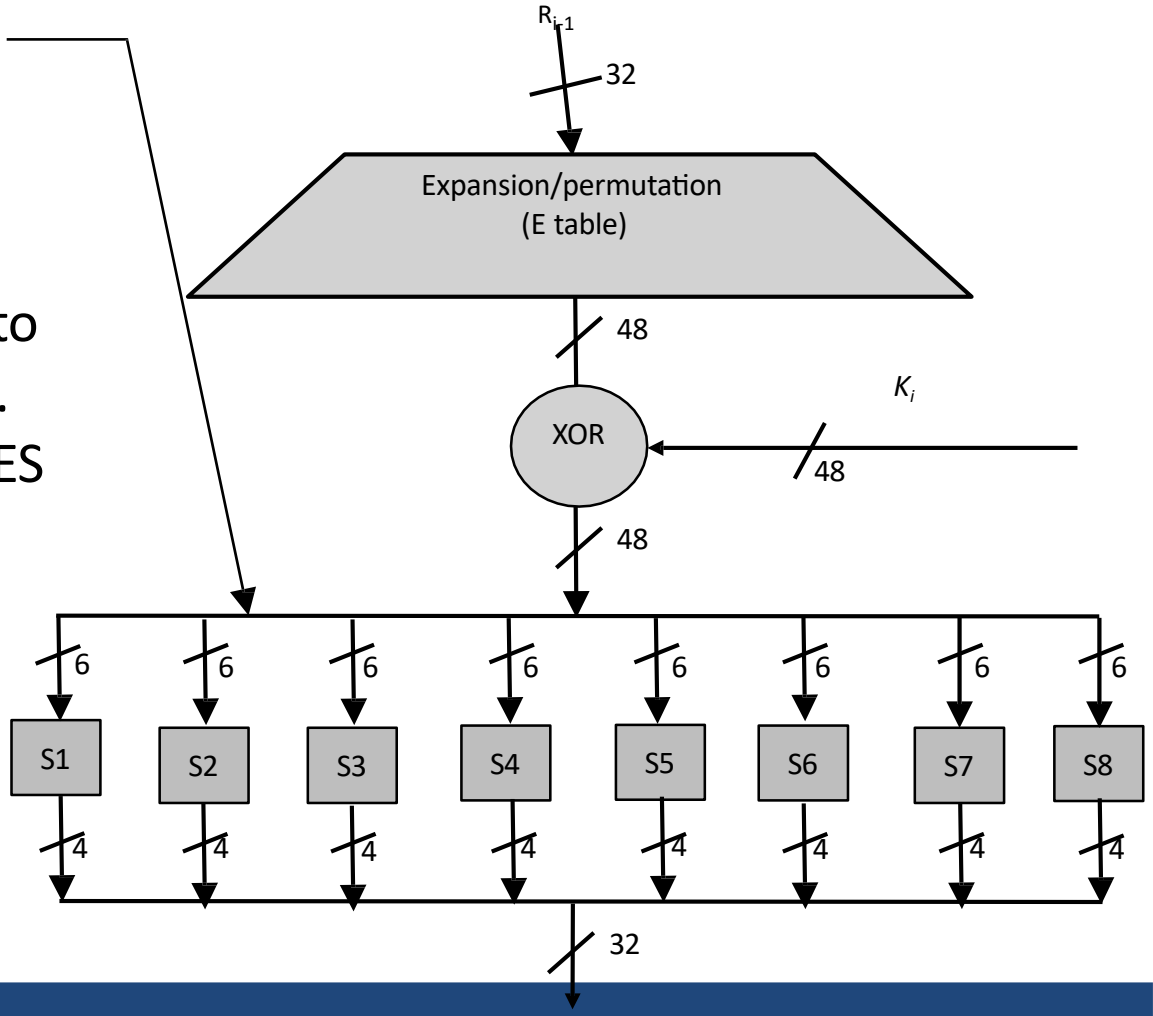
After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key.

Note that both the right section and the key are 48-bits in length now.



Data Encryption Standard (DES): S-Box substitution

- Eight substitution tables.
- 6 bits of input
- 4 bits of output.
- Convert 48 bits to 32 bits
- Non-linear and resistant to differential cryptanalysis.
- Crucial element for DES security!
- Introduces confusion.



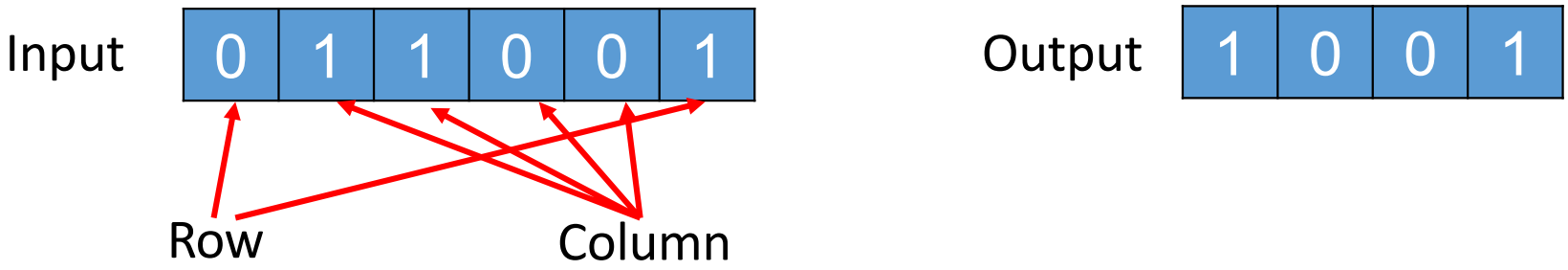
Data Encryption Standard (DES): S-Box substitution

The outer two bits of each group select one row of an S-box.
Inner four bits selects one column of an S-box.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-box 1

- Example:

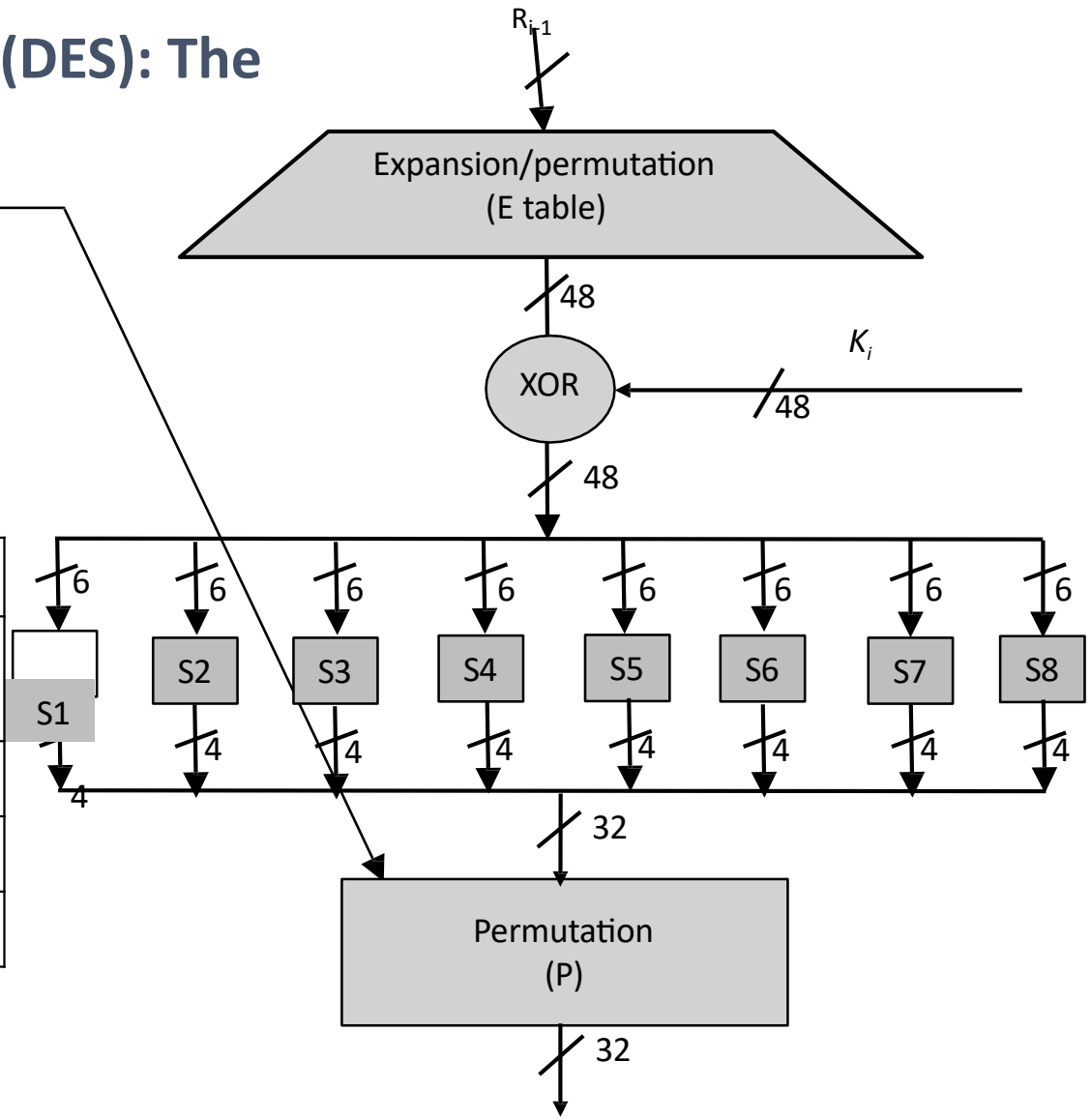


Data Encryption Standard (DES): The Permutation

Permutation P

- Bitwise permutation.
- **Introduces diffusion.**

Permutation Table P							
16	7	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25



Avalanche Effect

Desirable property of any encryption algorithm is that a change in one bit of the plaintext or of the key should produce a change in many bits of cipher text.
DES performs strong avalanche effect.

Plaintext: 0000000000000000	Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1	
Plaintext: 0000000000000001	Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3	

Although the two plaintext blocks differ only in the rightmost bit, the cipher text blocks differ in 29 bits.
This means that changing approximately 1.5 % of the plaintext creates a change of approximately 45 % in the ciphertext.

Strength of DES

The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.

The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

Design Principle of Block Cipher :

1. ConfusionPurpose: Make the relationship between the ciphertex and the encryption key as complex as possible.Achieved by: Using substitution operations (like S-boxes).
   Effect: Even a small change in the key or plaintext causes major,
   unpredictable changes in ciphertext.

2. DiffusionPurpose: Spread the influence of a single plaintext bit across many ciphertext bits. Achieved by: Using permutation and mixing operations.
   Effect: Changing one bit of the plaintext affects many bits of the ciphertext.

Design Principle of Block Cipher :

3.Kerckhoffs's Principle : A cipher should remain secure even if everything about the system (except the key) is public knowledge. Focuses security entirely on the secrecy of the key, not the algorithm.

4.Iterative Structure (Rounds)Instead of a single operation, block ciphers apply multiple rounds of transformations. Each round improves confusion and diffusion.
Example: AES uses 10, 12, or 14 rounds depending on key size.

5.Key Expansion The key schedule algorithm generates a different subkey for each round from the original key. Strong key expansion ensures better security.

Parul® University | NAAC GRADE A++

https://paruluniversity.ac.in/