

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

Data Science



Semester: Subject: 035 Academic Year: 2028 - 2024
DES (Data Encryption Standard):
* DES is a block cipher.
* It encrypte date in blocks of size of 64bile
* 64 bits of plaintent goes as an input to DES, was
* DES is a block cipher. * It encrypti date in blocks of size of 64bili * 64 bits of plaintent goes as an input to DES, which produces 64bits of Cipher text. The same also other and key are used for encryption
* The same algorithm and key are used for energy
* The same algorithm and key are used for encryption and decryption with minor difference.
* The key length is ST bill
and decryption with minor aliferate. * The key length is \$6 bilt Broad level steps in DES (or) Block diagram of DES.
Step 1: Plain Text (64 bits)
Step 4.1: Key Transformation
Step 2: Initial Permutation Step 4-2: Expansion Permutation
Step 3: (32 Bits) (32 bits) Step 4.3: S-Box Substitution
OL GUILLE III. D III. V
Step4: PBox Permentation
- W
Steps: Final Permutation Steps: XOR and Swap
Step 6: Cipher Text
The state of the s
Slepa: Initial Permutation. *There are pre-defined permutation gules for initial *There are pre-defined permutation Table) Refer PPT.
votere are pre-defined to the PRIL PPT.
then, the planted
for example, the S8" bit position in hew plain text, the so position in takes 1st position in hew plain text, the so position in
Subject Incharge: Prof. Sarala Mary Page No. 1. Department of CSE-Data Science APSIT



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

Data Science



Semester: VI Subject: CSS	Academic Year: 20 23- 20 24
Semester: VI Subject: <u>CSS</u> The plain-text <u>becomes</u> takes and bit	position in the new
generated plain text. *After initial permutation, a new 6.	4 bit plain text is
delived	
* The resulting 64-bit permuted to	od-block is divided
I THE TWO MALL WILLIAM I	1
* Fach half block consists of 32 bi * LPT (Left Plain Text) - 32 bits) ar	al RPT (Right Plain
* LPT (Left Plain lex) -> 32010)	U
1674 / 340.	
The key transformation undergoes of	ne following steps:
64 bit Key Discarding Shifting 16 keys of leach 56 bills	Permutation le keys of Permutation
*DES uses 16 rouners	used.
* For each round a unique	keys are generated
* For each round a unique of \$16	0
for each sound.	
key Discarding:	ted.
* Initially a 64bits key is see	is discarded.
Key Discarding: *Initially a 64bits key is select *Every 8th bit of original key *Every After discarding one key generaled	101= 200
* From After discarding one key	of \$66118 are
generaled.	



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Department of CSE-Data Science | APSIT

Semester:	V				Su	biect	::	CS	3.0				Acade	emic Ye	ar: 200	3-2024
Generale	16	Kei	13	of	56	bili										
To gen	uali	~	t - b k	out.	~	2-1	haill	£	110	ω -	the i	belo	ω:	nule	. J-1	will
perform	leff	ci.	rcul	as	shi	FI	acc	202	ling	15	-this	A	able	2.		
Round							7	8	9	10	41	12		14	15	16
# Key bili shifted.		1	2	2	2	2	2	2	1	2	- 2	2	. 2	2	I	1
Example 1111000 0101010 Accordi bit lef L1:11100 R1:1010 L16 R16. L2R2 is L3R3 is The sa keys of Compress permutat permutat k2, K4	tenol der me each	lo second sived por Per com	for for abl	10 your som	lal shi, 100 Lily re airon co	Re is per inti	by by ger	per per uta	the ool for ed too Ra ar	min fo	9 1 2 3 16 Li Ri	10 10 010 010 010 010 010 010 010 010 0	st. wi	of cir	reula: iscula 16d	ifferent

Page No._3

Subject Incharge: Prof. Sarala Mary



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

Data Science



Academic Year: 2093-2024 Semester: 5 Subject: CSC lumutation: The expansion permutation is applied on the original Step 4.2: - Expansion RPT of 22 bils. Original RPT of 32 bils Block8 Block 7 Blockb Block& Blocks 29 632 Block3 25 628 Block 1 21624 17/020 13/016 bili 5 to 8 bile 9612 of 32 bits is expanded 1 10 4 bile bile bile permutation, the RPT bils In expansion Blocks 25 26 27 28 29 20313 Blocks lo 486°ls 21 22 23 24 Block 4 Blocks. F 18 1920 13 141516 Tololo 9 1011 12 olilile ololia Using Expansion permutation expand 32 bit RPT to 48 bils 1000 1100 0110 1110 →3261 13 Example: 011000 001110 100100 001111 110001 011000 001101 011101 48 bils RPT Way to S-Box Substitution: * The first key (Ki) of 4869 ls is XDRed with the 486it RPT generated in Expansion permutation * A new 486ils RPT is generated which will undergo Department of CSE-Data Science | APSIT Subject Incharge: Prof. Sarala Mary Page No. 4



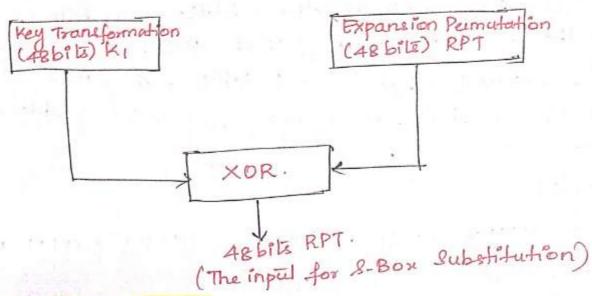
A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Academic Year: 20 23- 202 4 Semester: Subject : C.S.S

S-Box substitution.



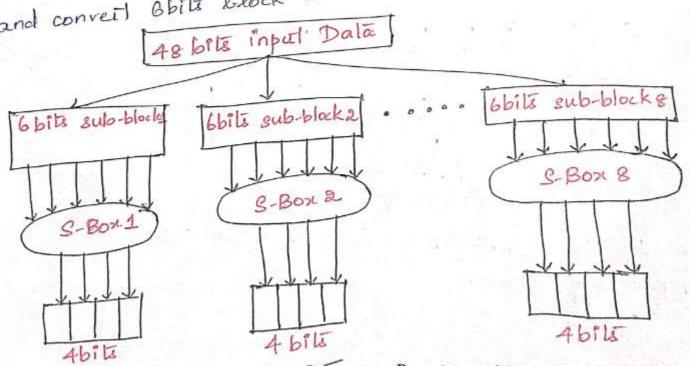
S-Box Substitution:

* The 48bits RPT is divided into 8 sub-blocks

with obite in each block.

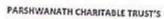
* Each sub-block will stefer to S-Box 1 to S-Box 8.

and conveil Bbita block to Abile block.



Subject Incharge: Prof. Sarala Mary Page No. 85

Department of CSE-Data Science | APSIT





Subject Incharge: Prof. Sarala Mary

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Department of CSE-Data Science | APSIT

Semester: Subject: C g C
The 1st and the lout bit will refer the now value of
despective SBox, whereas the middle four bils will
refer the coloumn value of that S-Box.
*For S-Box 1 sefer S-Box 1 lable, for S-Box-2
siefer S. Box 2 table, for S-Box 3 siefer S. Box 3-table and
80 00.
Example:
8-Box 8 0111
8-Box 4: (0 D B2 (1) B2 (1) B3 (1) B4 (0) B5 (1) B6 (0)
B1(1) B2(1) B3(1) B4(0) B5(1) B6(0) Abit coloumn
abit row. (1010) (1010) Fraglly the 48bit RPT is converted into 32 bits
Frally the 48 bit RPT is converted into 32 bits RPT using S-Box.

Page No. 46



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Department of CSE-Data Science | APSIT

Academic Year: 2023-2024 Semester: VI Subject : CSS Step 4.4 - P-Box Permutation: P-Box Permutation and new 32 bili RPT is generaled. 8 Ep 4.5 : XOR and swap Original 64 bit. Round 1 32 bit RPT Key 1 (32 bits LPT 1. Key Transformation 2. Expansion Permutation 3. S-Box Substitution 4. P-Box Permutation XORK 32-bit LPT 1. Expansion, Permutation a. G-Box XDR 32 bit RPT 32-61+LPT Alle output generated from Round 1 becomes new RPT. and the previous 32 bits RPT is new 32 bits LPT. the process is suspected to times with 16 different keys and 64bit output is generated Subject Incharge: Prof. Sarala Mary Page No. 97



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



			ALC: A
Semester:VI	Subject :	CSS	Academic Year: 2023 2021

Step 5: Final Permutation:

*The 64 bils output generaled in the previous step undergoes final permutation and new 64 bils is generated.

* The output generalied after final permutation is the

64 bit Cipher Text

DES Decryption:

* The same algorithm used for encyption in DES also works for deciption.

* The only difference between encyption and decyption

is severse of key position.

*For encyption key (K) is used allvided into Ki, Ka, Ka... Kis for decryption key should be used as Kib, Kis, Kig... Ki. for all lo siounds.

DES Analysis:

DES has proved to be a very well-designed block cipher DES satisfies both the desired properties of block cipher. Avalanche effects- A small change in plaintent (or) key results in significant change in the ciphes text-Each bit of cipher test depends on many bits of plainteset.