Teacher/Instructor: Dr Ch Rajendra Babu

Department of Computer Science and Engineering
Professor in CSE

Lesson Plan for a Day
Term/Semester/Year: IV Sem- I - Syllabus
JNTUK R16

MICRO LESSON PLAN

(ACCORDING TO BLOOMS DIGITAL TAXONOMY)

Programme	B Tech
Semester	IV Year – ISemester
Subject Title	CRYPTOGRAPHY AND NETWORKSECURITY
Subject Code	R1641051
Class Hours	5
Total Hours	80
Credits	3
Max Marks	100
Unit & Title	Unit 2 DES
Teaching and Learning Tools	Google classrooms, Smart Board, Pedagogy ,E-material , Video clips for **Post Task**

Detailed – Lesson DES Lesson Objectives:	
Factual	• **Introduction to Data Encryption Standard**
Conceptual	• **Compare and contrast various encryption and decryption schemes.**
Procedural	• **Design various Scheduling algorithms** • **Design various encryption and decryption algorithms** • **Design triple DES.**
Applied	**DES algorithm was made mandatory for all financial transactions.**

Prerequisite Knowledge:

Fiestel structure, Block message. Initial permutation, final permutation, D Box

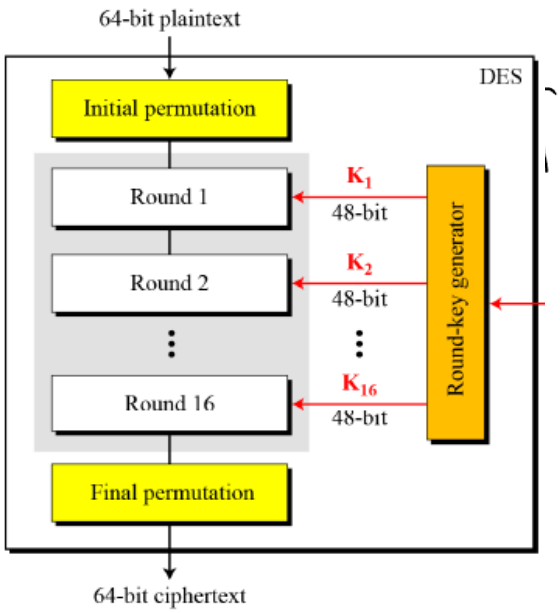
Micro Lesson Plan: Day -1.

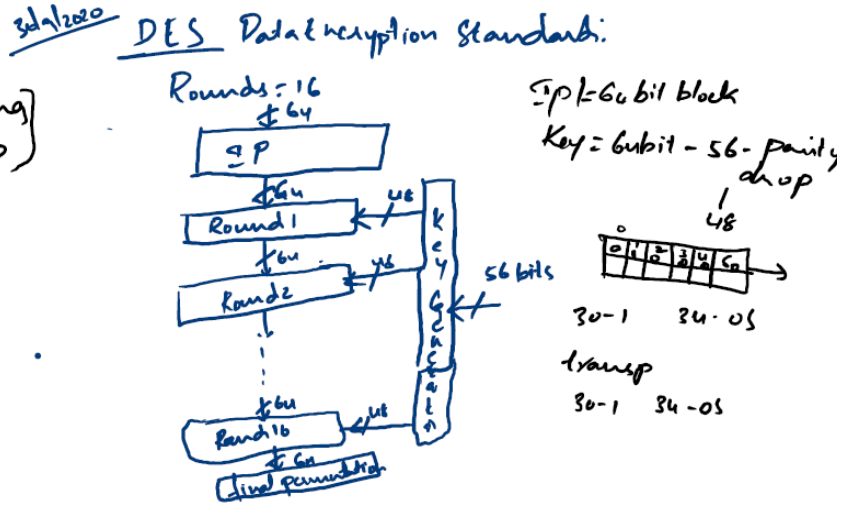
1. Pre-task Activity- Introduction to DES

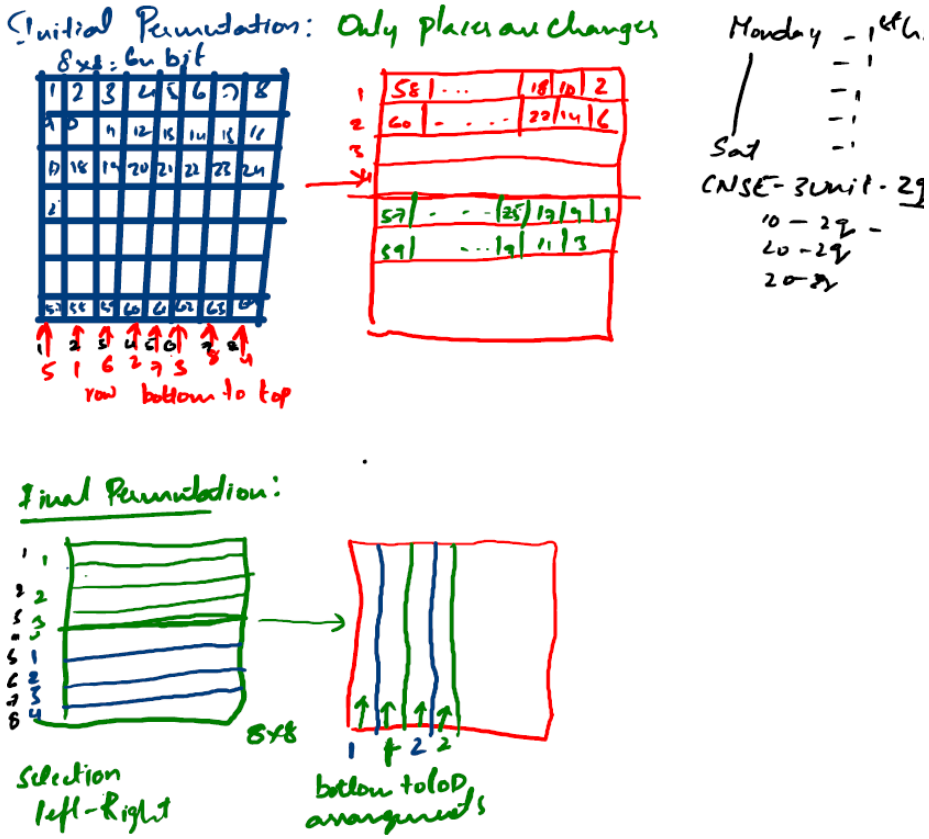
In DES structure

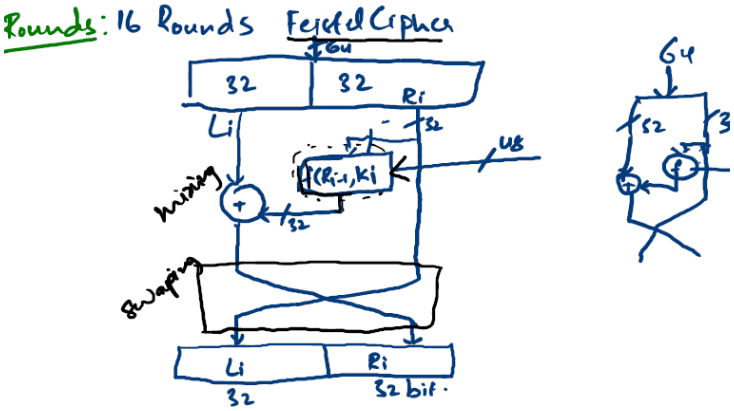
- **The entire data is divided into blocks of equal size.**
- **The block data is again divided into 2 parts.**
- **Some operation is performed on either LHS or RHS**
- **Again LHS is mixed with RHS.**
- **Key generation**
- **Round operations**
- **The same process is repeated for n times**

2. In-class Activity:









DES uses 16 rounds. Each round of DES is a Feistel cipher.

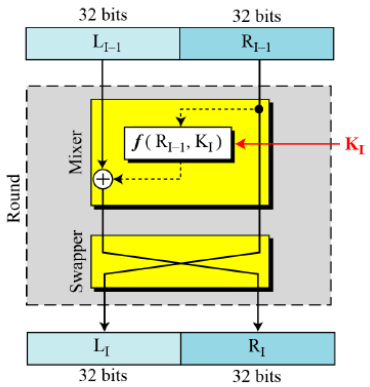
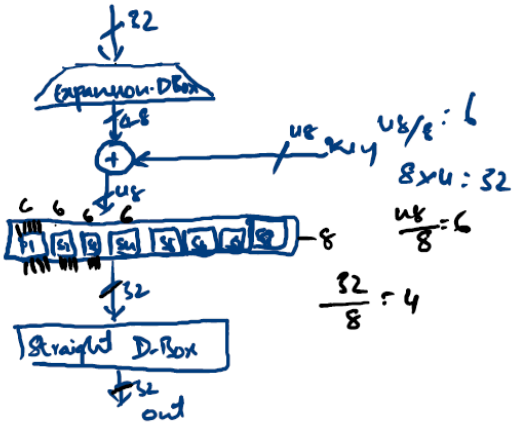
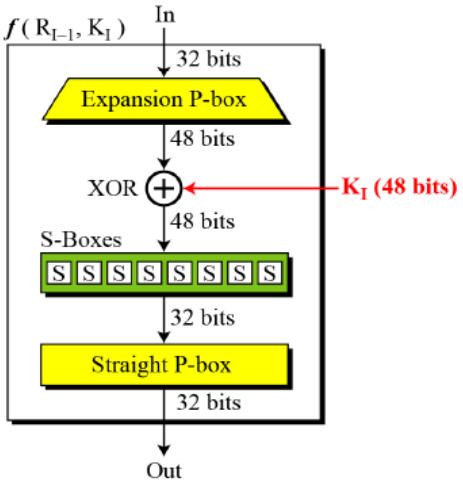
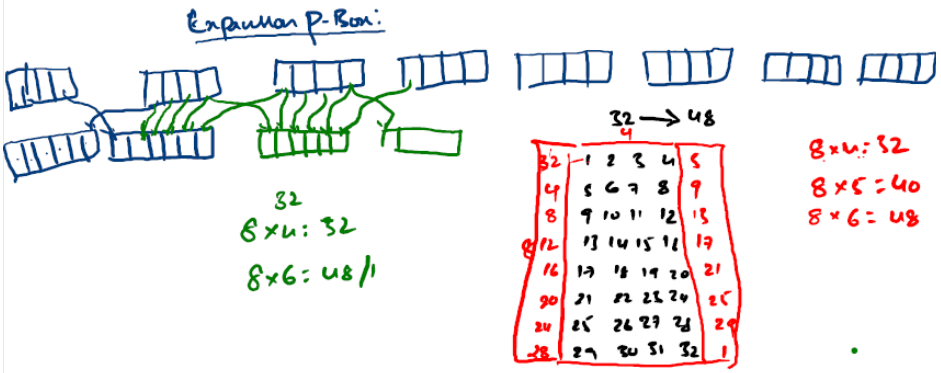


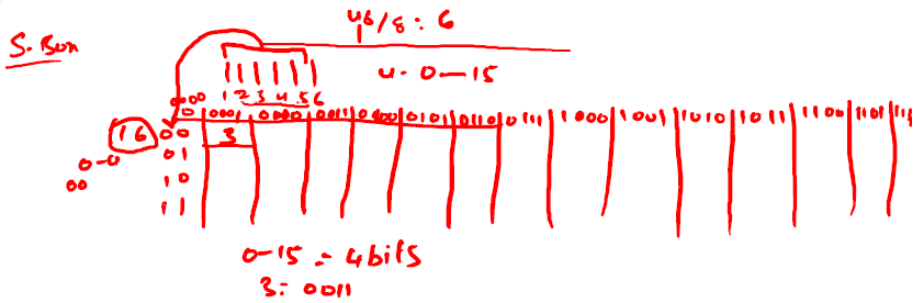
Figure 6.4
A round in DES (encryption site)

DES function:





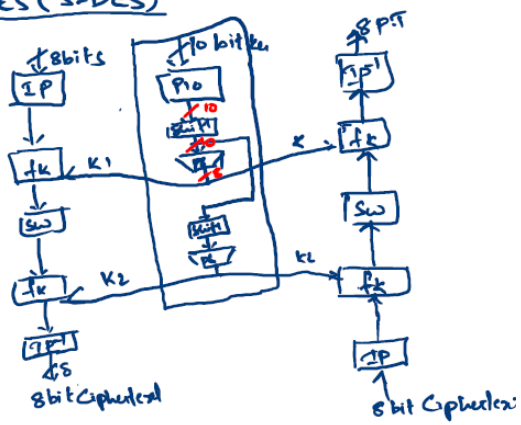




2/10/2020

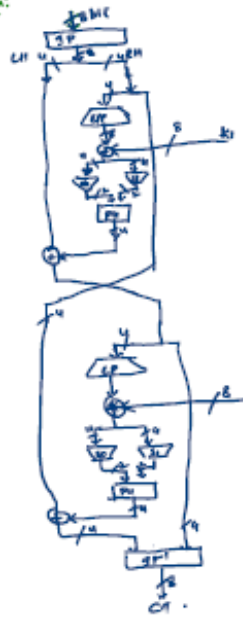
Simplified DES (S-DES)

block size : 8 bits
Key : 10 bits
Rounds : 2

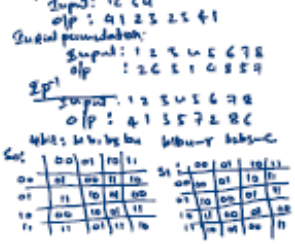


Input 10 bit key k = 1010000010
K1 & K2
P10 : permutate
i/p : 1 2 3 4 5 6 7 8 9 10
o/p : 3 5 2 7 4 10 1 9 8 6
P8 : select & permutate
i/p : 1 2 3 4 5 6 7 8 9 10
o/p : 6 3 7 4 8 5 10 9
P4 : permutate
i/p : 1 2 3 4
o/p : 2 4 3 1

Encryption:



Expand
Input : 1 2 3 4
o/p : 4 1 2 3 2 3 4 1
Initial permutation:
Input : 1 2 3 4 5 6 7 8
o/p : 2 6 3 1 4 8 5 7
IP-1
Input : 1 2 3 4 5 6 7 8
o/p : 4 1 3 5 7 2 8 6



k1 : 1010 0100
k2 : 0100 0011
PT : 0111 0010
LHS : 0111 RHS : 0010
RHS : 0010
EP : 1 2 3 4
4 1 2 3 2 3 4 1
EP : 1 1 0 0 0 0 1 0
⊕ 1 0 1 0 0 1 0 0
0 1 1 0 0 0 1 1
S0 : 0110 S1 : 0011
S0(00,11) = 10 S1(01,11) = 11
S0S1 : 1011
P4 : 1 2 3 4
2 4 3 1
0 1 1 1
Exp. P4 : 0 1 1 1
LHS : 1010
⊕ 1 0 0 1
S0 LHS : 1001 RHS : 1101
RHS : 1101
Exp : 1 2 3 4
4 1 2 3 2 3 4 1
1 1 1 0 1 0 1 1
Exp : 1 1 1 0 1 0 1 1
⊕ k2 : 0 1 0 0 0 0 1 1
1 0 1 0 1 0 0 0
S0 : 1010 S1 : 1000

S0S1 : 10 11
P4 : 1 2 3 4
2 4 3 1
P4 : 0 1 1 1
⊕ RHS : 1 0 0 1
: 1 1 1 0
RHS : 1 1 0 1
LHS RHS : 1 1 1 0 1 1 0 1
CT : 1 2 3 4 5 6 7 8
4 1 5 3 7 2 8 6
0 1 1 1 0 1 1 1 CT

Initial Permutation

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

Final Permutation

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

Expansion D-Box

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	32

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

Parity Bit Drop table

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	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

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