جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (07)
Block Ciphers and Feistel cipher

Dr. Ahmed M. ElShafee

introduction

- Modern block ciphers are widely used to provide encryption of quantities of information, and/or a cryptographic checksum to ensure the contents have not been altered.
- Block ciphers work a on block / word at a time, which is some number of bits.
- All of these bits have to be available before the block can be processed.
- Stream ciphers work on a bit or byte of the message at a time, hence process it as a "stream".
- Block ciphers are currently better analysed, and seem to have a broader range of applications, hence focus on them.

Block cipher principles

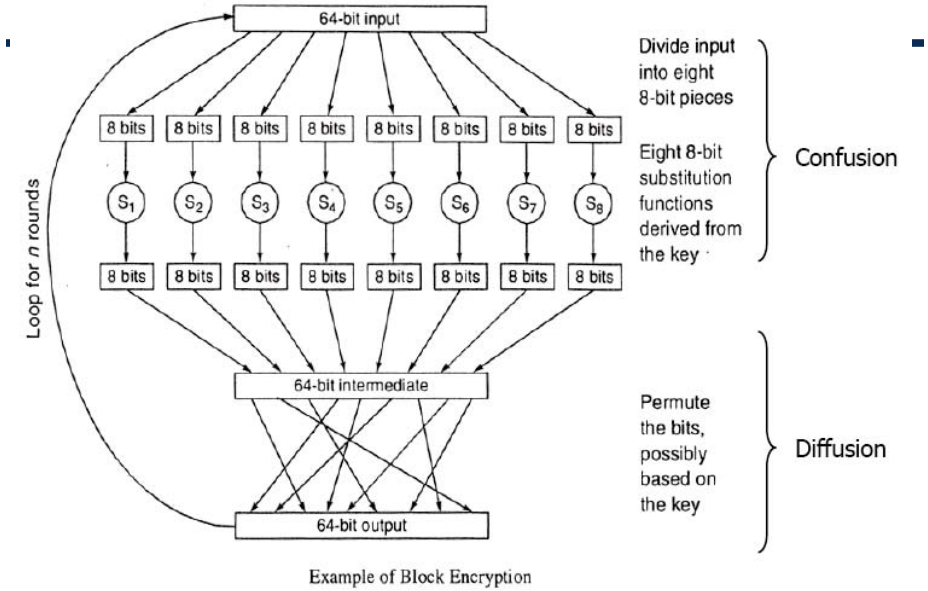
- An arbitrary reversible **substitution** cipher for a **large block size** is not practical, however, from an **implementation** and **performance** point of view.
- In general, for an *n*-bit general substitution block cipher, need a substitution box of 2^n entities
- For a 64-bit block (8 bytes block), a pure block substation cipher is a huge table contains 2^{64} entities, each entity has a 64 bits length.
- So the size of sbox is 64 x 2^{64} = 2^{70} = 1.18 E21 bits = 1.34 E8 tera bytes
- In general, for an *n*-bit general substitution block cipher, the size of the key is $n \times 2^n$.

Block length	Sbox length
8 bits	8 x 2^8 = 2048 bits = 256 bytes
16 bits	16 x 2^{16} = 1.05 E6 bits = 128 kBytes
32 bits	32 x 2^{32} = 1.37 E 11 bits = 16 G bytes
64 bits	64 x 2^{64} = 2^{70} = 1.18 E21 bits = 1.34 E8 tera bytes

Claude Shannon and Substitution-Permutation Ciphers

- Claude Shannon's 1949 paper has the key ideas that led to the development of modern block ciphers.
- Critically, it was the technique of layering groups of S-boxes separated by a larger P-box to form the S-P network, a complex form of a product cipher.
- He also introduced the ideas of ***confusion*** and ***diffusion***, notionally provided by **S-boxes** and **P-boxes** (in conjunction with S-boxes).
- Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key.

Block Ciphers

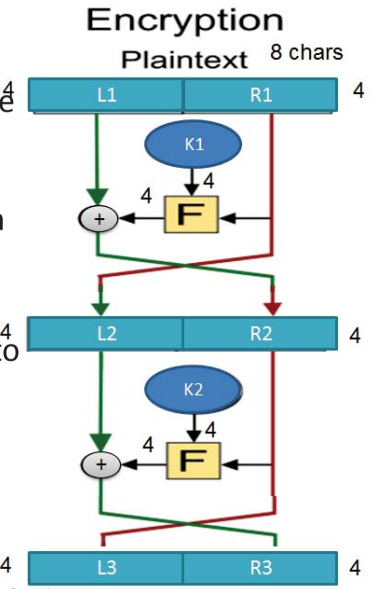


Example of Block Encryption

- The mechanism of **diffusion** seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.
- **Confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key.
- So successful are diffusion and confusion in capturing the essence of the desired attributes of a block cipher that they have become the cornerstone of modern block cipher design.

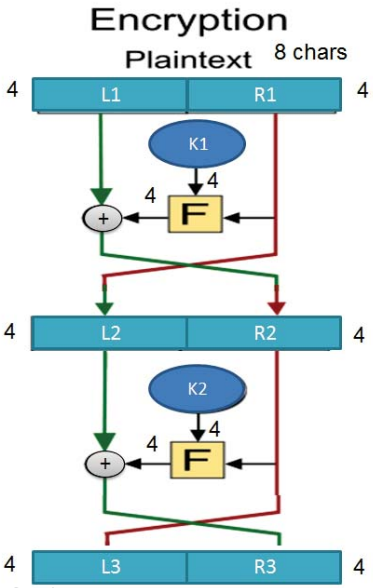
Block cipher designing rules

- Applying what shannon said cryptosystem designer should follow the following rules
  - instead of building a huge blocks a smaller blocks is used to create from smaller building blocks
  - using idea of a product cipher (SPN)
  - Block cipher transforms plain block to text block based on user key
  - Block cipher is invertible and based one 1:1 functions

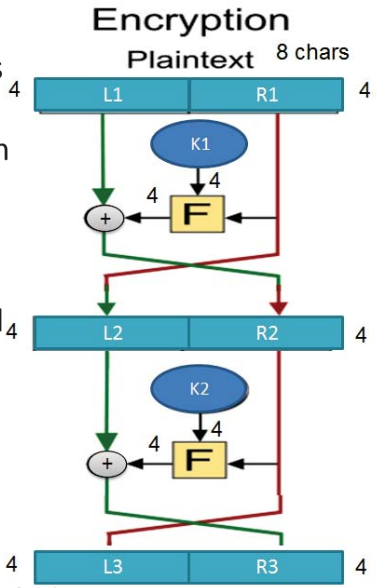


Feistel Cipher

- Horst Feistel, working at IBM Thomas J Watson Research Labs devised a suitable invertible cipher structure in early 70's.
- One of Feistel's main contributions was the invention of a suitable structure which adapted Shannon's S-P network in an easily inverted structure.

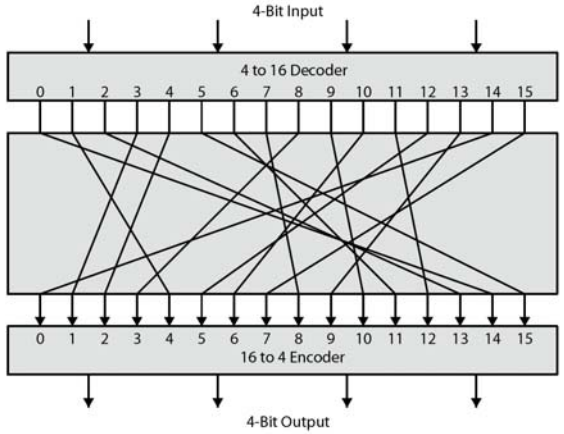


- It partitions input block into two halves which are processed through multiple rounds which perform a substitution on left data half, based on round function of right half & subkey, and then have permutation swapping halves.
- Essentially the same h/w or s/w is used for both encryption and decryption, with just a slight change in how the keys are used.
- One layer of S-boxes and the following P-box are used to form the round function.

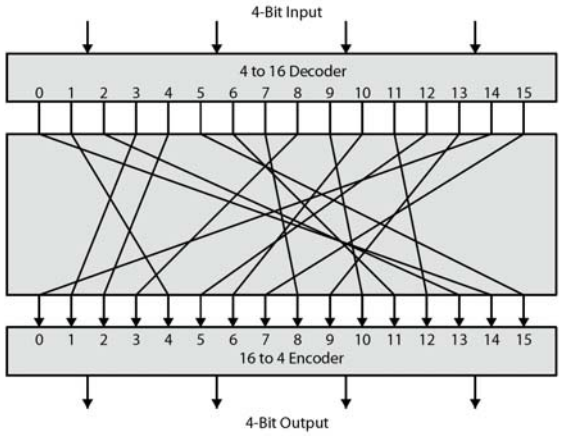


Feistel cipher as black substitution box

- Feistel refers to an *n*-bit general substitution as an ideal block cipher
- it allows for the maximum number of possible encryption mappings from the plaintext to ciphertext block.



- Ex: A 4-bit input produces one of 16 possible input states, which is mapped by the substitution cipher into a unique one of 16 possible output states, each of which is represented by 4 ciphertext bits.
- The encryption and decryption mappings can be defined by a tabulation



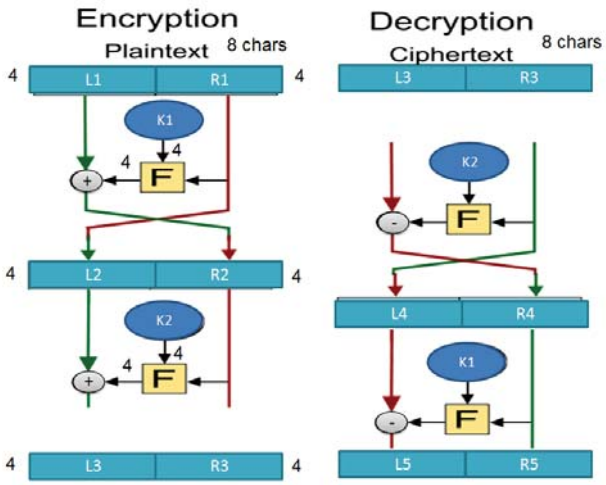
0000	
0001	
0010	
0011	
0100	
.	
.	
1111	

Feistel Cipher Design Elements

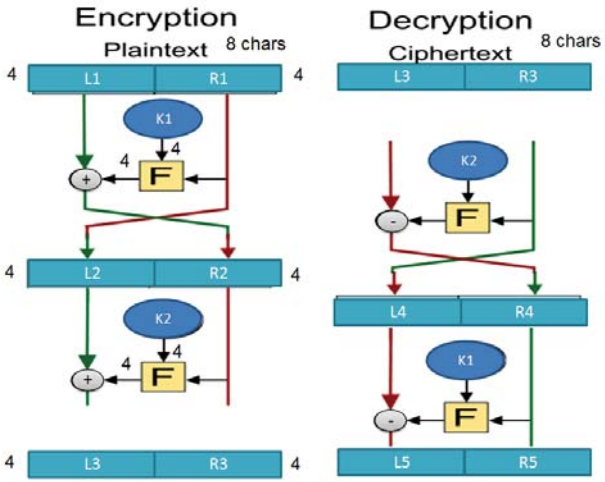
- The exact realization of a Feistel network depends on the choice of the following parameters and design features:
- **block size** - increasing size improves security, but slows cipher
- **key size** - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds** - increasing number improves security, but slows cipher
- **subkey generation algorithm** - greater complexity can make analysis harder, but slows cipher
- **round function** - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption** - more recent concern for practical use ease of analysis - for easier validation & testing of strength

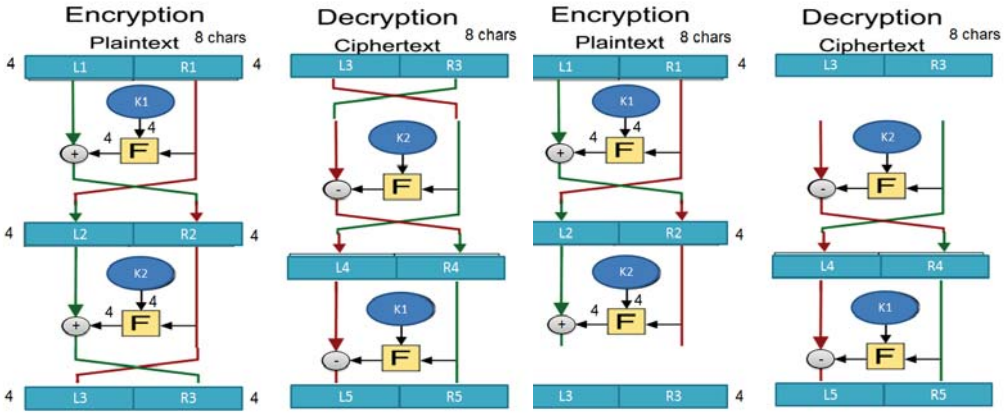
Feistel cipher decryption

- The process of decryption with a Feistel cipher, is essentially the same as the encryption process.
- The rule is as follows:
  - Use the ciphertext as input to the algorithm, but use the subkeys *Ki* in reverse order.



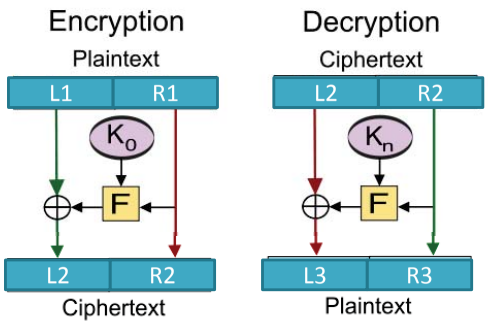
  - That is, use *Kn* in the first round, *Kn*–1 in the second round, and so on until *K*1 is used in the last round.
- This is a nice feature because it means we need not implement two different algorithms, one for encryption and one for decryption.





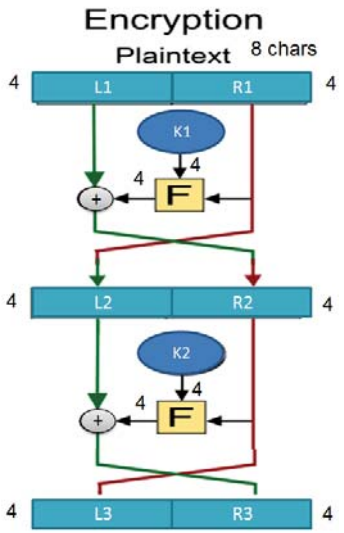
Proof; Feistel encryption is the same as Feistel decryption

- Enc:
  R2 = R1 → 1
  L2 = L1 xor F(R1, K) →2
- Dec:
  R3 = R2 →3
  L3 = L2 xor F(R2, k) →4
- From 3 & 1
  R1= R3
- From 2 & 4
  L 3 = L1 xor F(R1, k) xor F(R2, k)
- But R1 = R2
  L3 = L1 xor F(R1, k) xor F(R1, k)
  L3 = L1

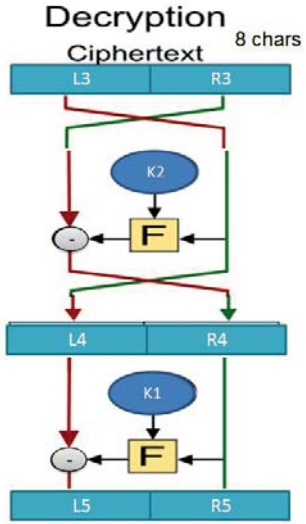


Proof; Feistel encryption is the same as Feistel decryption

- encryption
- R3 = L2 xor F(R2,K2) →1
- L3 = R2 →2
- R2 = L1 xor F(R1,k1) →3
- L2 = R1 →4



- Decryption
- R5 = R4 →5
- L5 = L4 xor F(R4,K1) →6
- R4 = R3 xor F(L3,k2) →7
- L4 = L3 →8



R3 = L2 xor F(R2,K2) →1
L3 = R2 →2
R2 = L1 xor F(R1,k1) →3
L2 = R1 →4

R5 = R4 →5
L5 = L4 xor F(R4,K1) →6
R4 = R3 xor F(L3,k2) →7
L4 = L3 →8

- From 1,2,4: R3 = R1 xor F(L3,K2) → 8
- From 2,3: L3 = L1 xor F(R1,K1) →9
- From 7,5,8: R5 = R3 xor F(L3,K2)→10
- From 8,5,6: L5 = L3 xor F(R5,K1) →11
- Sub 10 in 8
- R5 = R1 xor F(L3,K2) xor F(L3,k2) = R1 →#

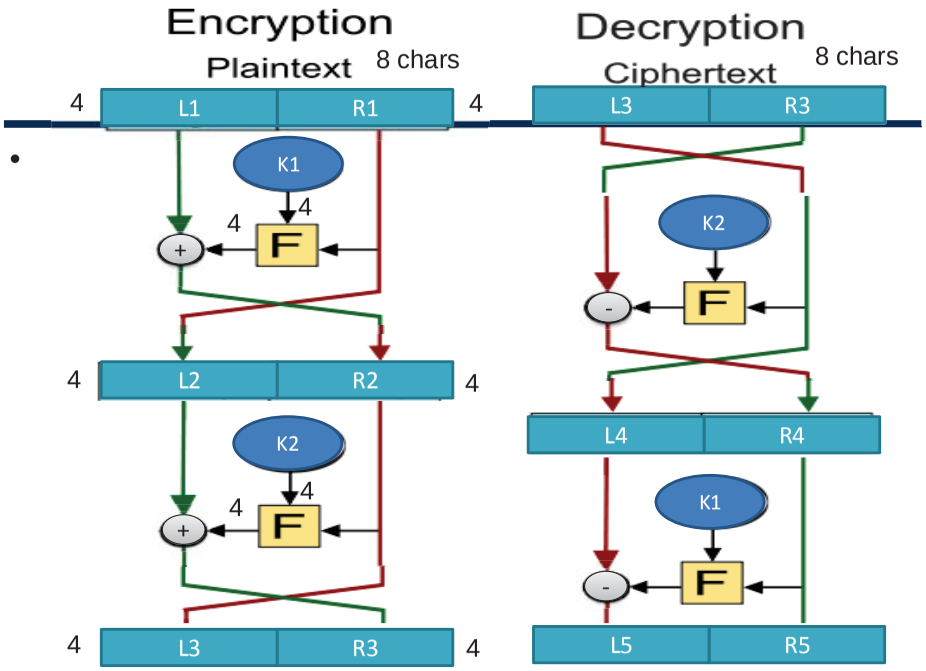
- Sub 11 in 9
- L5 = L1 xor F(R1,K1) xor F(R5,K1)
- But R1 == R5 so F(R1,K1) = F(R5,K1)
- So L5 = L1 →#

Thanks,..

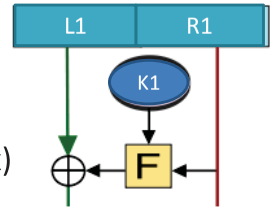
See you next week (ISA),…

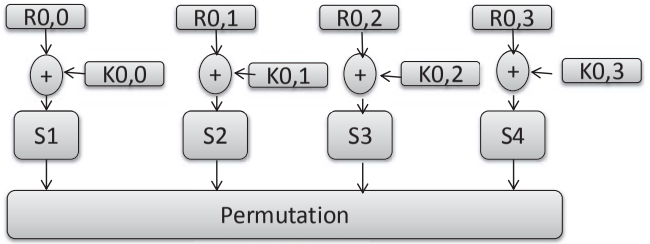
Feistel Cipher Example Simplified 2 rounds operated on 26 characters English plaintext characters space

Dr. Ahmed M. ElShafee

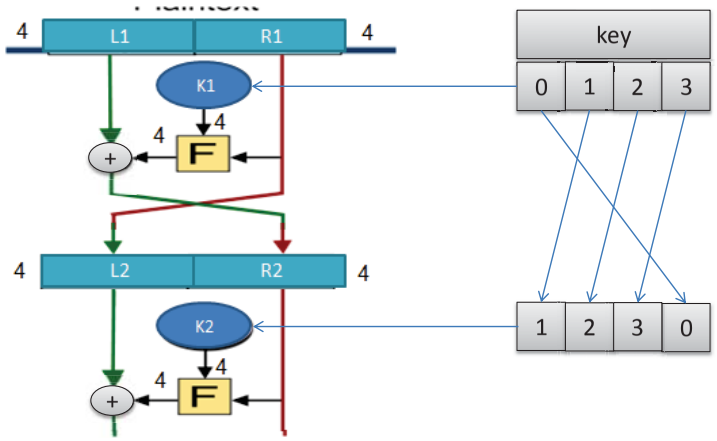


- Feistel Function is SP network
  - Plain characters xored with Key
  - a simple substitution (4 x sbox)
  - Followed by simple permutation (1 x pbox)



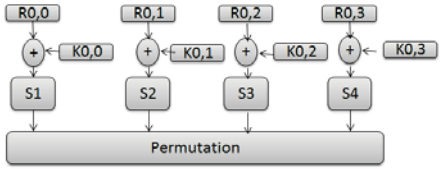


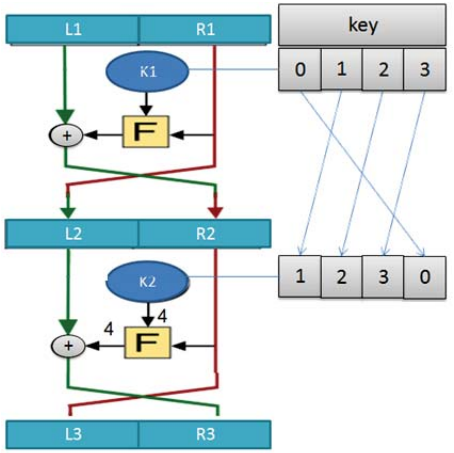
- Key schedule



Example 1

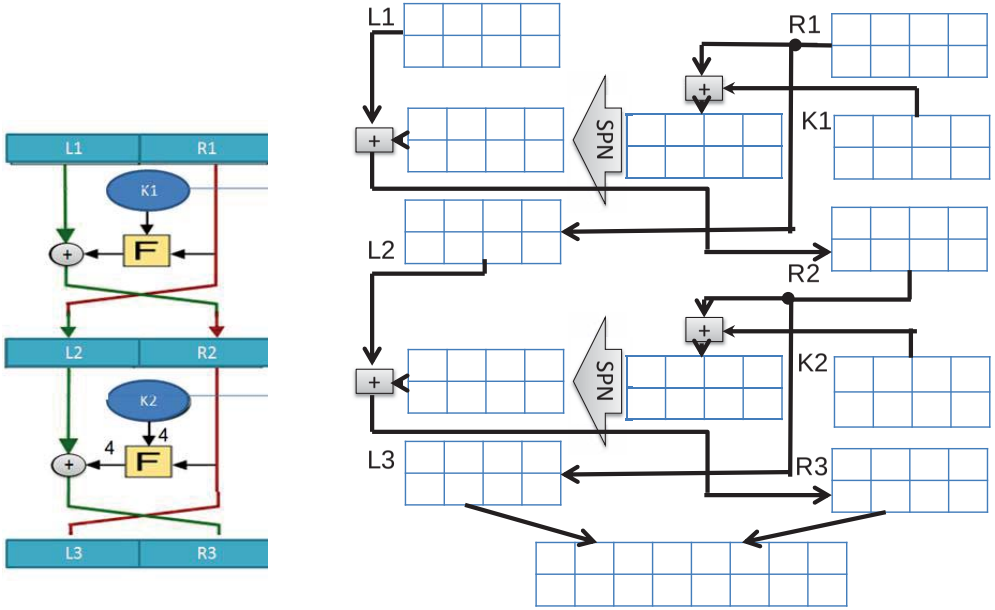
- Use the following feistel cipher to encrypt the following message "**supplies**"
- Using the following key "**scrt**"



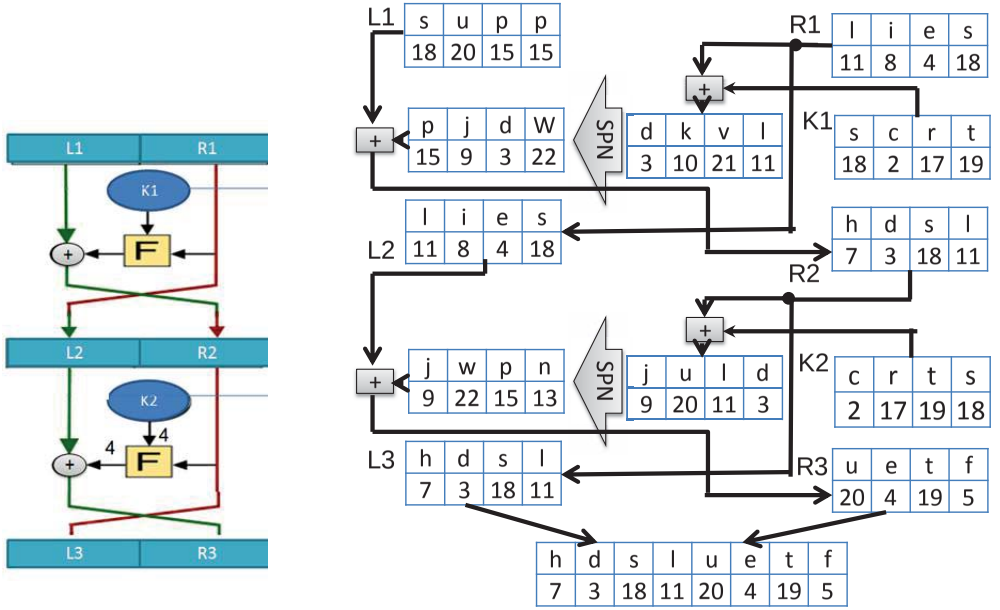


- s1= pdqjkfvobwselcmtirhgnyxazu
- S2=gcobidpjmywurtzqefkxnlhsav
- S3=musxelogkrqpzbatifjycdnvhw
- S4=ycsjndegatipzwhrokfqvxlubm
- P=dacb

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
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



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
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



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
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

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b

pbox

Sboxes output

Feistel output

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
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

d	k	v	l

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b

pbox

j	w	d	p

Sboxes output

p	j	d	w

Feistel output

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
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

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b

pbox

Sboxes output

Feistel output

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
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

j	u	l	d

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b

pbox

w	n	p	j

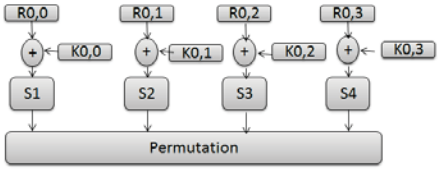
Sboxes output

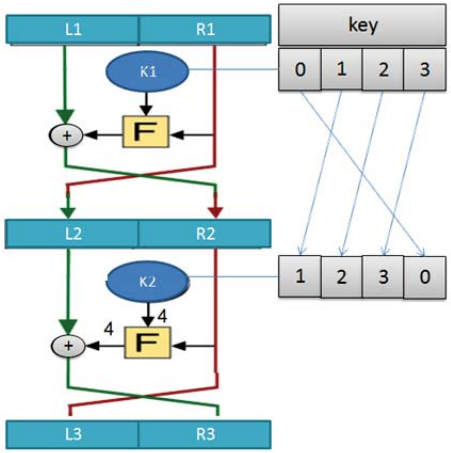
j	w	p	n

Feistel output

Example 2

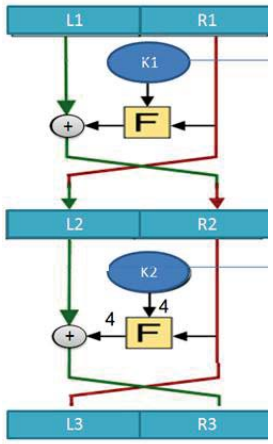
- Use the following feistel cipher to encrypt the following message "**ten fifty**"
- Using the following key "**scrt**"

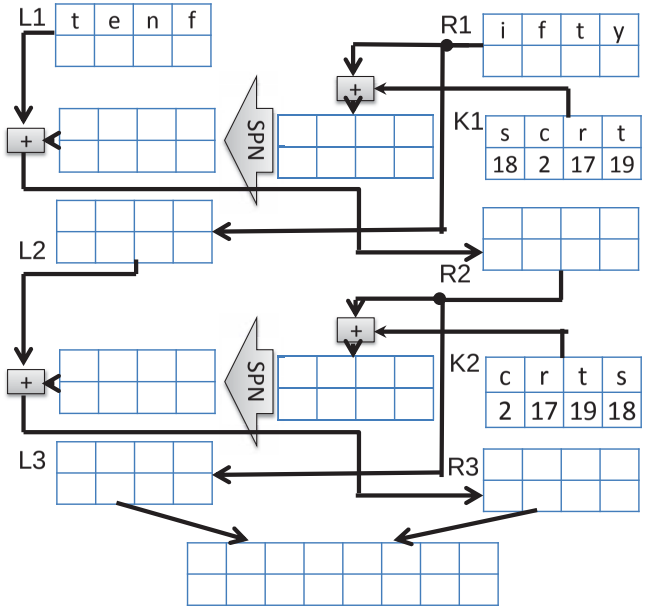




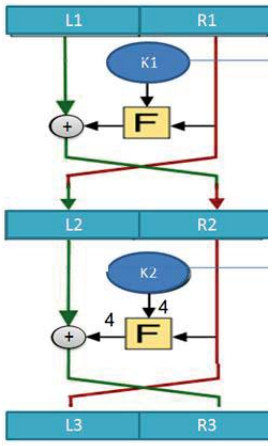
- s1= pdqjkfvobwselcmtirhgnyxazu
- S2=gcobidpjmywurtzqefkxnlhsav
- S3=musxelogkrqpzbatifjycdnvhw
- S4=ycsjndegatipzwhrokfqvxlubm
- P=dacb

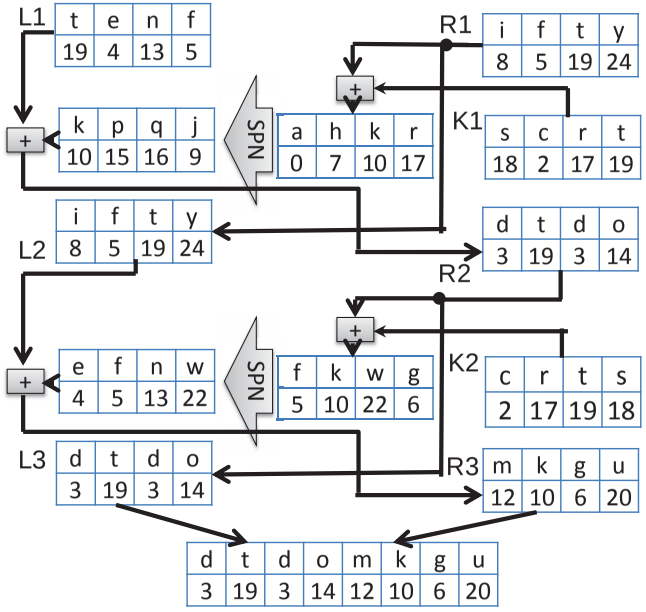
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z





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
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





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
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

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b

pbox

Sboxes output

Feistel output

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
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

SPN

a	h	k	r	Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b	pbox	p	j	q	k	Sboxes output

k	p	q	j	Feistel output

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
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

SPN

				Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b	pbox					Sboxes output

				Feistel output

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
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

SPN

f	k	w	g	Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

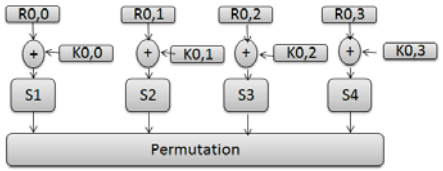
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

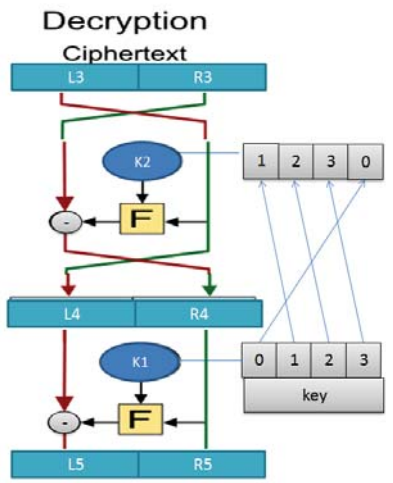
d	a	c	b	pbox	f	w	n	e	Sboxes output

e	f	n	w	Feistel output

Example 3

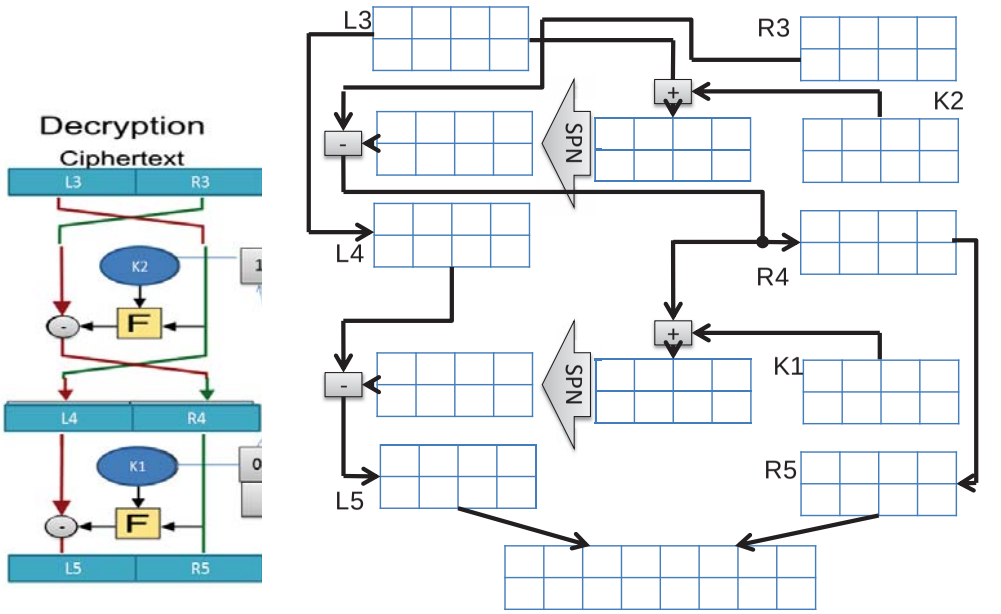
- Use the following feistel cipher to decrypt the following message "**qdkcdyjk**"
- Using the following key "**scrt**"



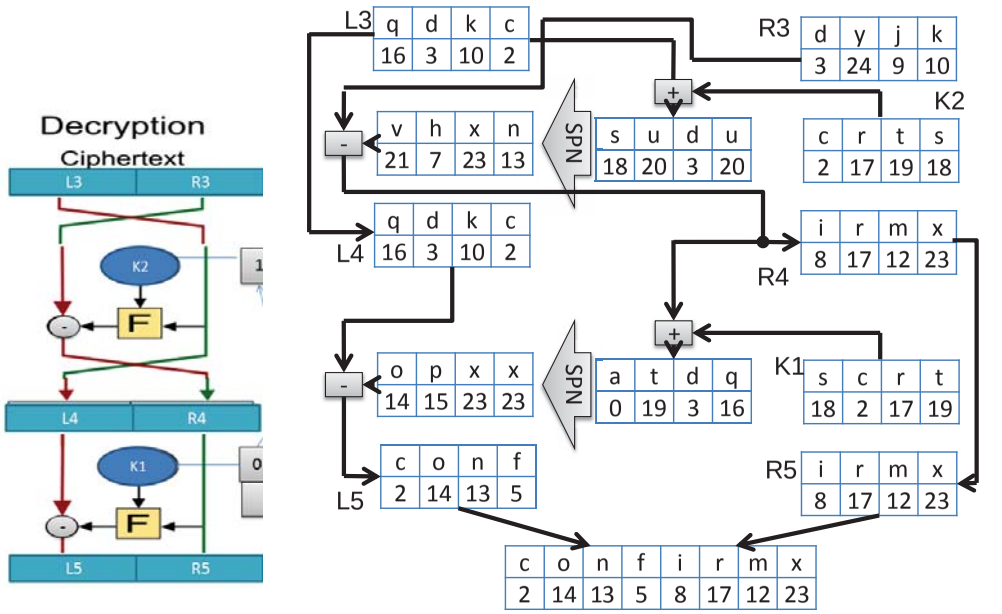


- s1= pdqjkfvobwselcmtirhgnyxazu
- S2=gcobidpjmywurtzqefkxnlhsav
- S3=musxelogkrqpzbatifjycdnvhw
- S4=ycsjndegatipzwhrokfqvxlubm
- P=dacb

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
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



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
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



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
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

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d a c b pbox

Sboxes output

Feistel output

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
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

s u d u Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d a c b pbox

h n x v Sboxes output

v h x n Feistel output

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
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

SPN

Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d a c b pbox

Sboxes output

Feistel output

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
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

SPN

a t d q Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

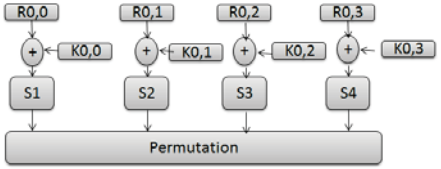
d a c b pbox

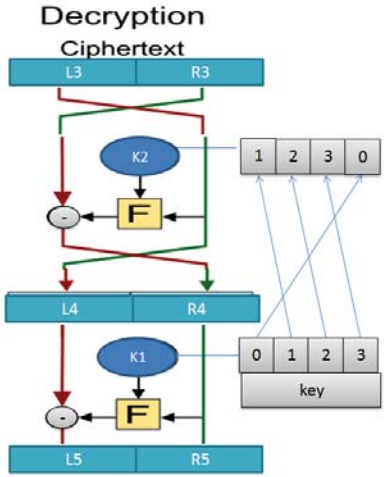
p x x o Sboxes output

o p x x Feistel output

Example 4

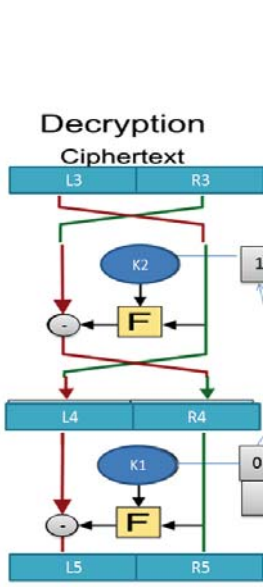
- Use the following feistel cipher to decrypt the following message "**hvxswxwk**"
- Using the following key "**scrt**"

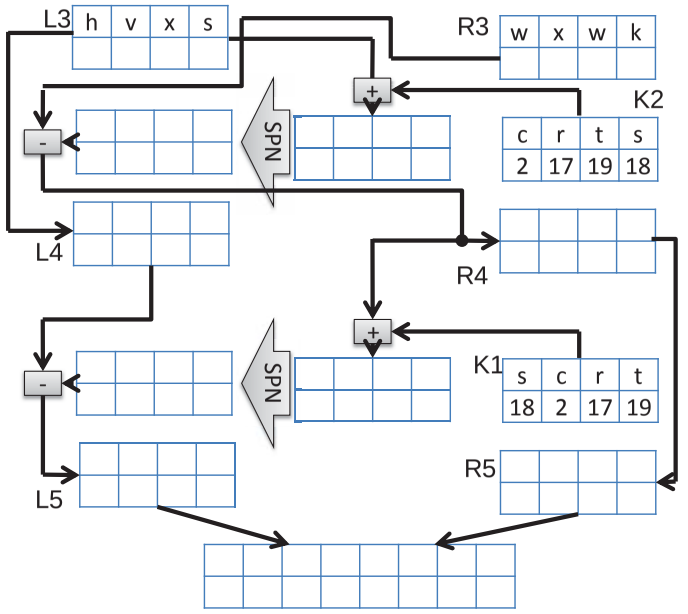




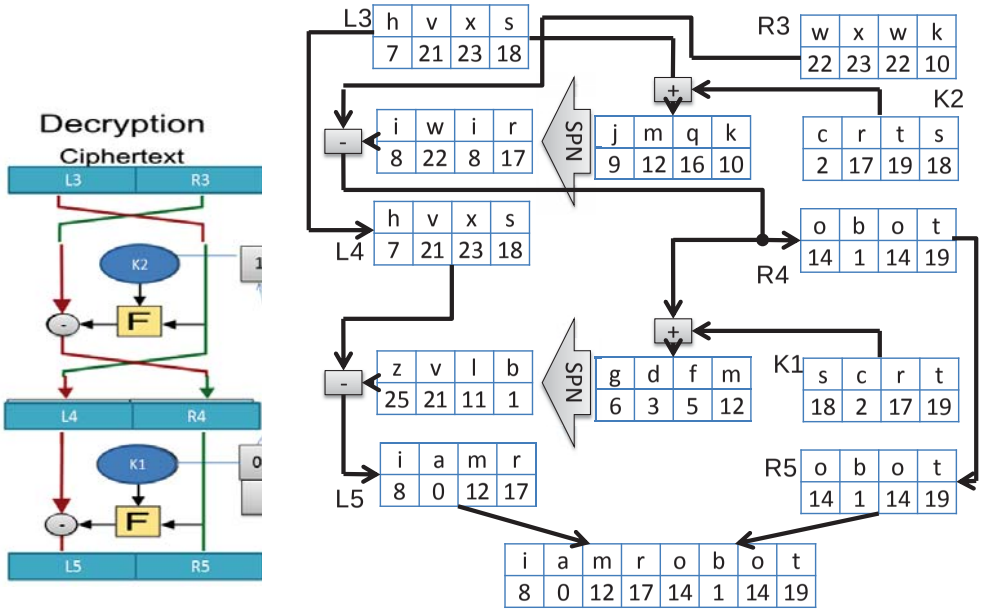
- s1= pdqjkfvobwselcmtirhgnyxazu
- S2=gcobidpjmywurtzqefkxnlhsav
- S3=musxelogkrqpzbatifjycdnvhw
- S4=ycsjndegatipzwhrokfqvxlubm
- P=dacb

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
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

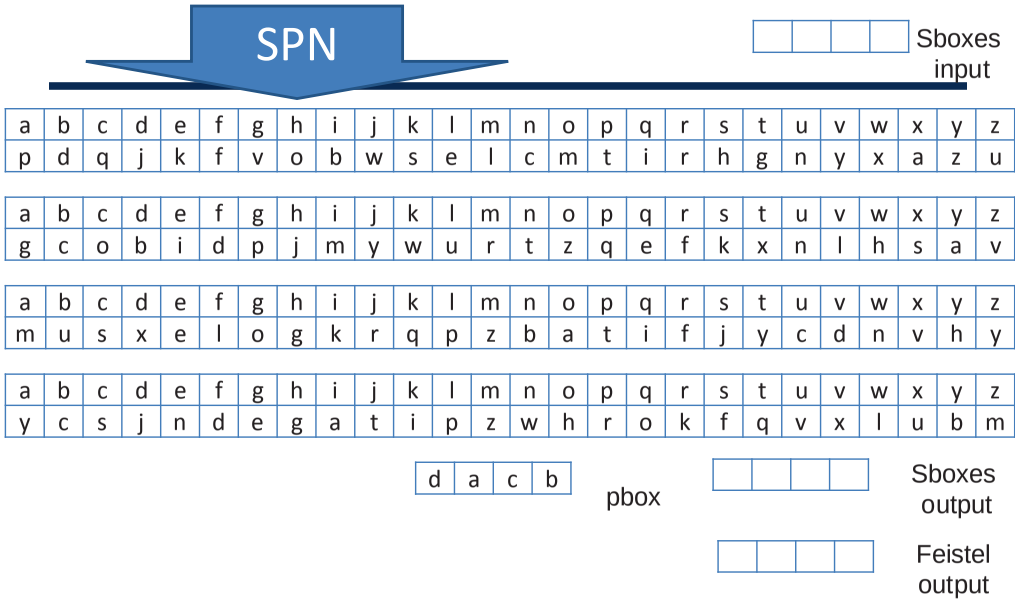




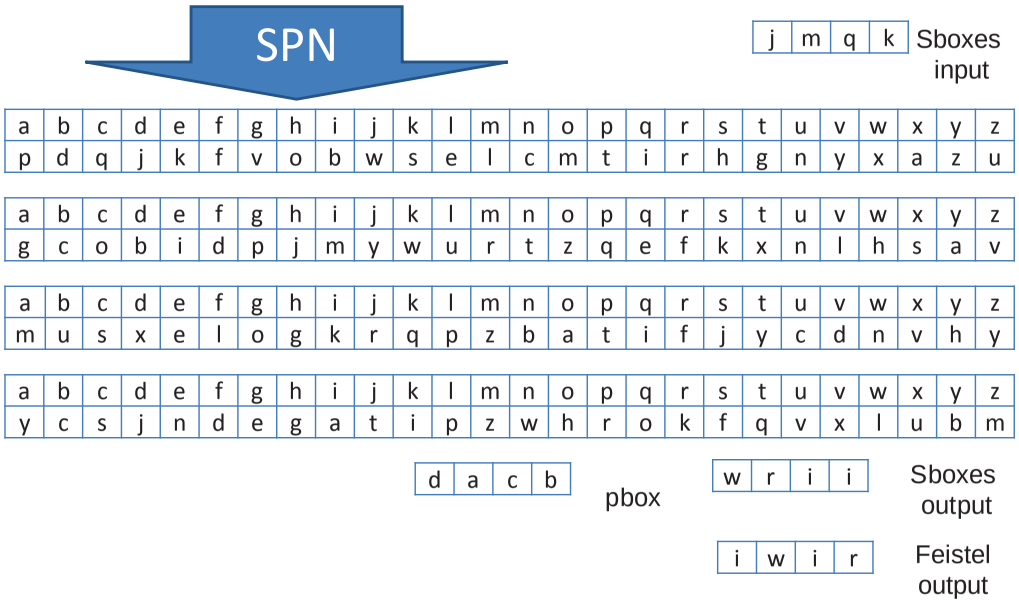
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z



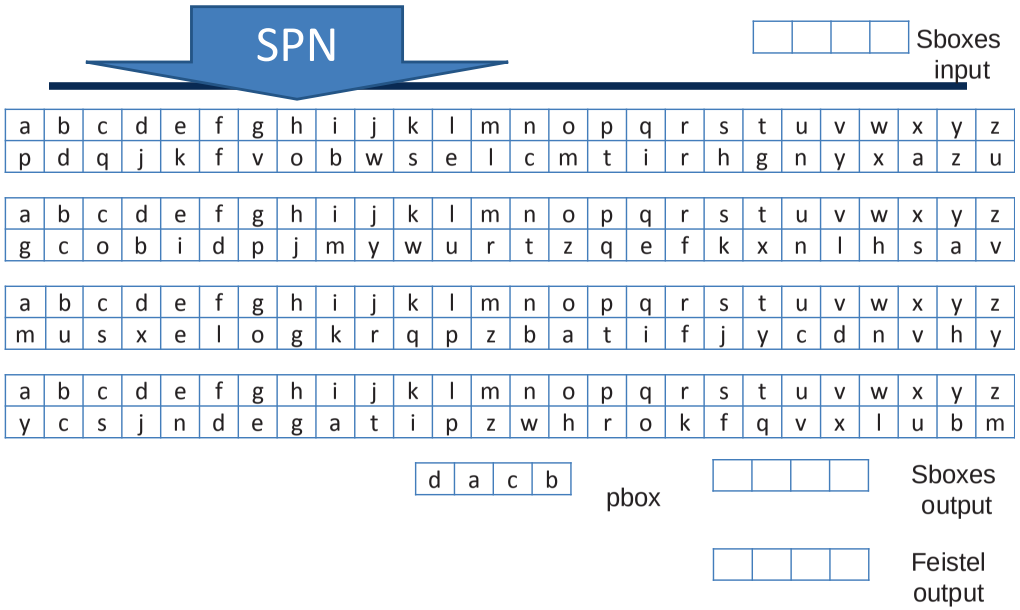
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z



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
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



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
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



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
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

SPN

g	d	f	m	Sboxes input

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
p	d	q	j	k	f	v	o	b	w	s	e	l	c	m	t	i	r	h	g	n	y	x	a	z	u

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
g	c	o	b	i	d	p	j	m	y	w	u	r	t	z	q	e	f	k	x	n	l	h	s	a	v

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
m	u	s	x	e	l	o	g	k	r	q	p	z	b	a	t	i	f	j	y	c	d	n	v	h	y

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
y	c	s	j	n	d	e	g	a	t	i	p	z	w	h	r	o	k	f	q	v	x	l	u	b	m

d	a	c	b

pbox

v	b	l	z	Sboxes output

z	v	l	b	Feistel output

Thanks,..

See you next week (ISA),...