BEACH

CECS 378: Intro to Computer Security Principles

Lecture 3

Louis Uuh

Week 4

Cryptography Classification

BEACH

- By the type of encryption operations used
  - Substitution
  - Transportation
  - Product
- By number of keys used
  - Single-key or private key
  - Two-Key or public
- By the way in which plaintext is processed
  - Block
  - Stream

Substitution

BEACH

- Ceasar Cipher: Classic example of ancient cryptography, used by Julius Caesar
- It is based on transposition involving shifting each letter by a number, typically 3
- Ciphertext can be decrypted by applying the same number of shifts in the opposite direction
- A more recent variation of Caesar cipher is ROT13

Ceasar Cipher Example

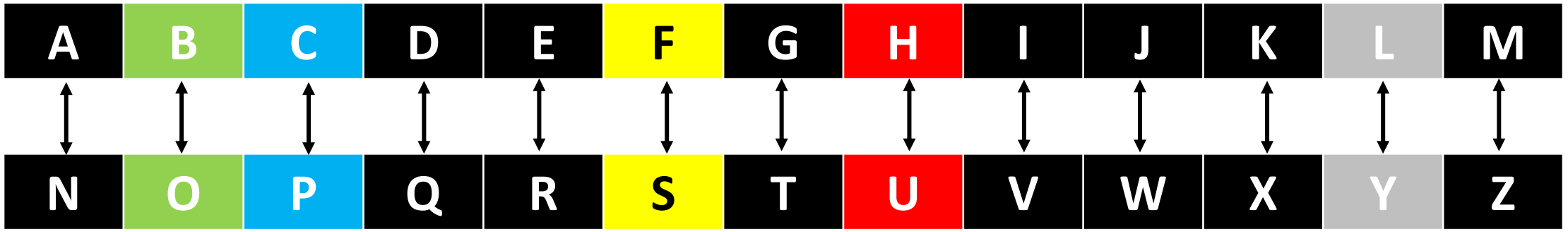
BEACH

- Define transformation as:
  - 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 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
- Example:
  - friday classes suck
  - CULGDB FODVVHV VXFN

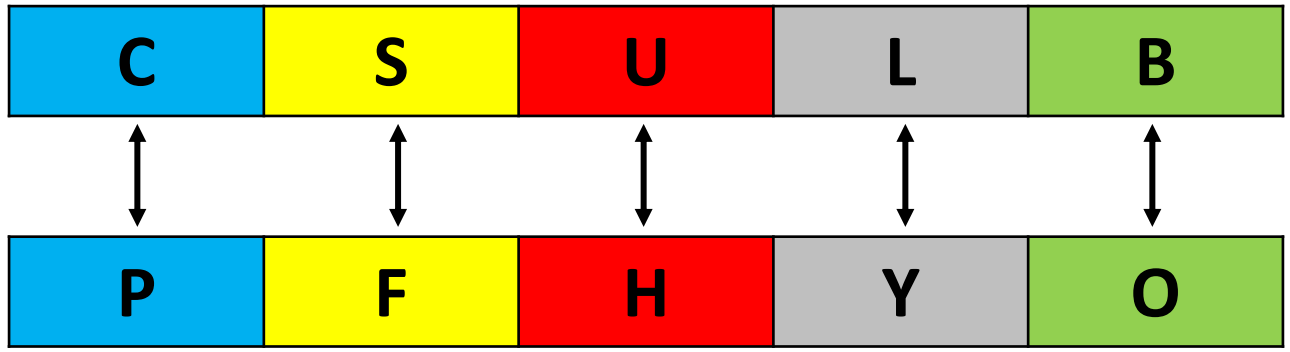
ROT13 – *Example*

BEACH

13



ROT13

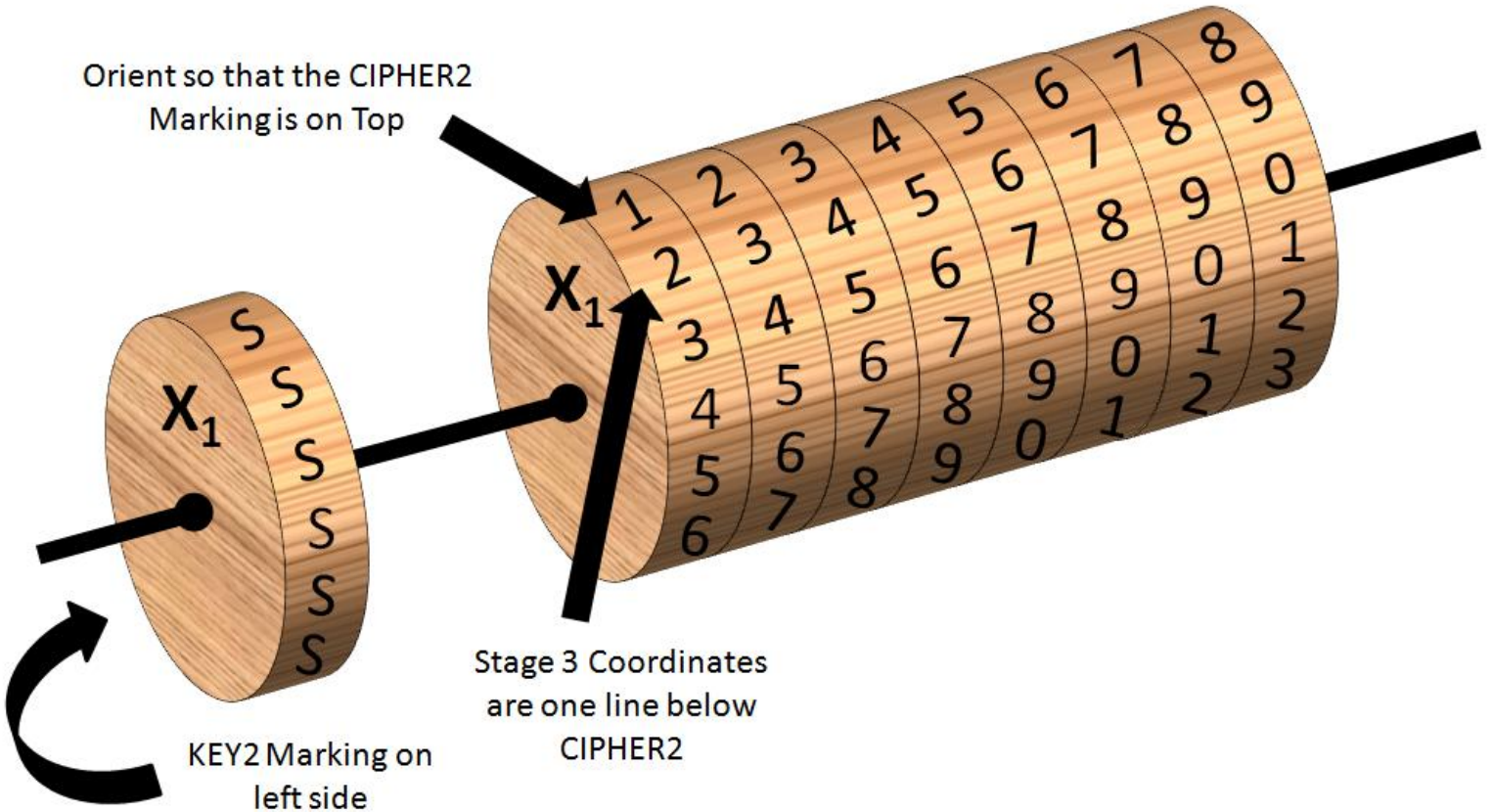


Cryptographic Machines

BEACH

- The Jefferson Disk, invented by Thomas Jefferson in 1795
- Used by US Army in early 1920's to early 1940's
- Alice and Bob would agree on the order of the disks
- Alice
  - Rotates wheels to spell out message
  - Sends any other row of text to Bob
- Bob
  - Spells out ciphertext on the wheel
  - Spins around the rows until he sees the plaintext message

Jefferson's Disk



Kerckhoff's Principle

BEACH

1. System must be substantially, if not mathematically, undecipherable
2. System must not require secrecy and can be stolen by the enemy without causing trouble
3. It must be easy to communicate and remember the keys without requiring written notes, and it must be easy to change or modify the keys with different participants
4. System must ought to be compatible with telegraph communication
5. System must be portable, and its use must not require more than one person
6. It must be easy to use and must require neither the stress of mind nor the knowledge of a long series of rules

One-Time Pad

BEACH

- If a truly random key as long as the message is used, the cipher will be secure
- Called a One-Time pad
- Is unbreakable since ciphertext bears no statistical relationship to the plaintext
- Since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- Can only use the key **once** though
- Problem in generation & safe distribution of key

Transposition (Permutation) Ciphers

BEACH

- Rearrange the letter order without altering the actual letters
  - Rail Fence Cipher: Write message out diagonally as:

    m e m o t r h o g p r y

    i t i f i t e o a a t
  - Giving ciphertext: MEMOTRHOGPRYITIFITEOAAT
- Row Transposition Ciphers: Write letters in rows, reorder the columns according to the given key before reading off .
  - Key: 3245716
  - Column Out 3 2 4 5 7 1 6
  - Plaintext:

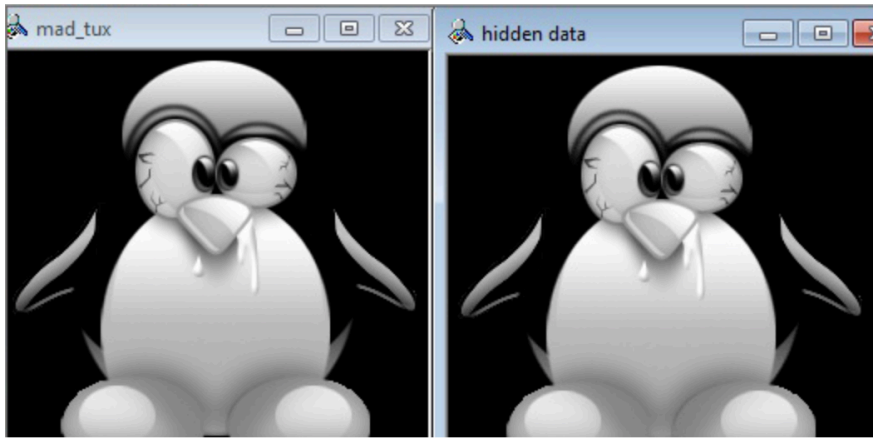
a	t	t	a	c	k	1
b	e	e	r	o	n	e
d	o	n	e	t	i	l
w	o	r	m	x	y	z

- Ciphertext:KNIYTEOOABDWTENRAREM1ELZKNIY

Steganography

BEACH

- The idea is to hide characters in a text, hide bits in a photo(e.g. .jpeg, .bit, .png, etc)
- Least significant bit (LSB) of the picture may be the message
- Pros: Can obscure encryption used
- Cons: High overhead to hide relative few info bits



Block vs Stream Ciphers

BEACH

- **Block ciphers** process messages into blocks, each of which is then encrypted\decrypted
- It is a substitution on very big characters
  - 64-bits, 512-bits, etc
- **Stream ciphers** process messages a bit or byte at a time when encrypting\decrypting
- Many current ciphers are block ciphers
- Hence why we are focusing on them

Block Cipher Principles

BEACH

- Block ciphers look like an extremely large substitution
- Would need table of 2^{64} entries for a 64-bit block
- Arbitrary reversible substitution cipher for a large block size is not practical
  - 64-bit general substitution block cipher, key size 2^{64}!
- Most symmetric block ciphers are based on a **Feistel Cipher Structure**
- Needed since must be able to **decrypt** ciphertext to recover messages efficiently

Data Encryption Standard (DES)

BEACH

- Is a block cipher algorithm
  - It follows the Feistel structure
  - Plain text should be split into halves
  - R_i should be run through the function, along with the key & the output from it should go to the left
  - The Left and the Right output from the function would then be XOR with one another
  - Then you would do a swap
  - Right → Left and Left → Right to store the bits

Data Encryption Standard (DES)

BEACH

- Plain text is process to Cipher text in a # of blocks
- Block size → 64 bits
- # of rounds → 16 rounds (P.T is process in # of rounds)
- Key size → 64 bits
- # of subkeys → 16 subkeys (because we have 16 rounds)
- Subkey size → 48 bit subkey
- Cipher text → 64 bit cipher text

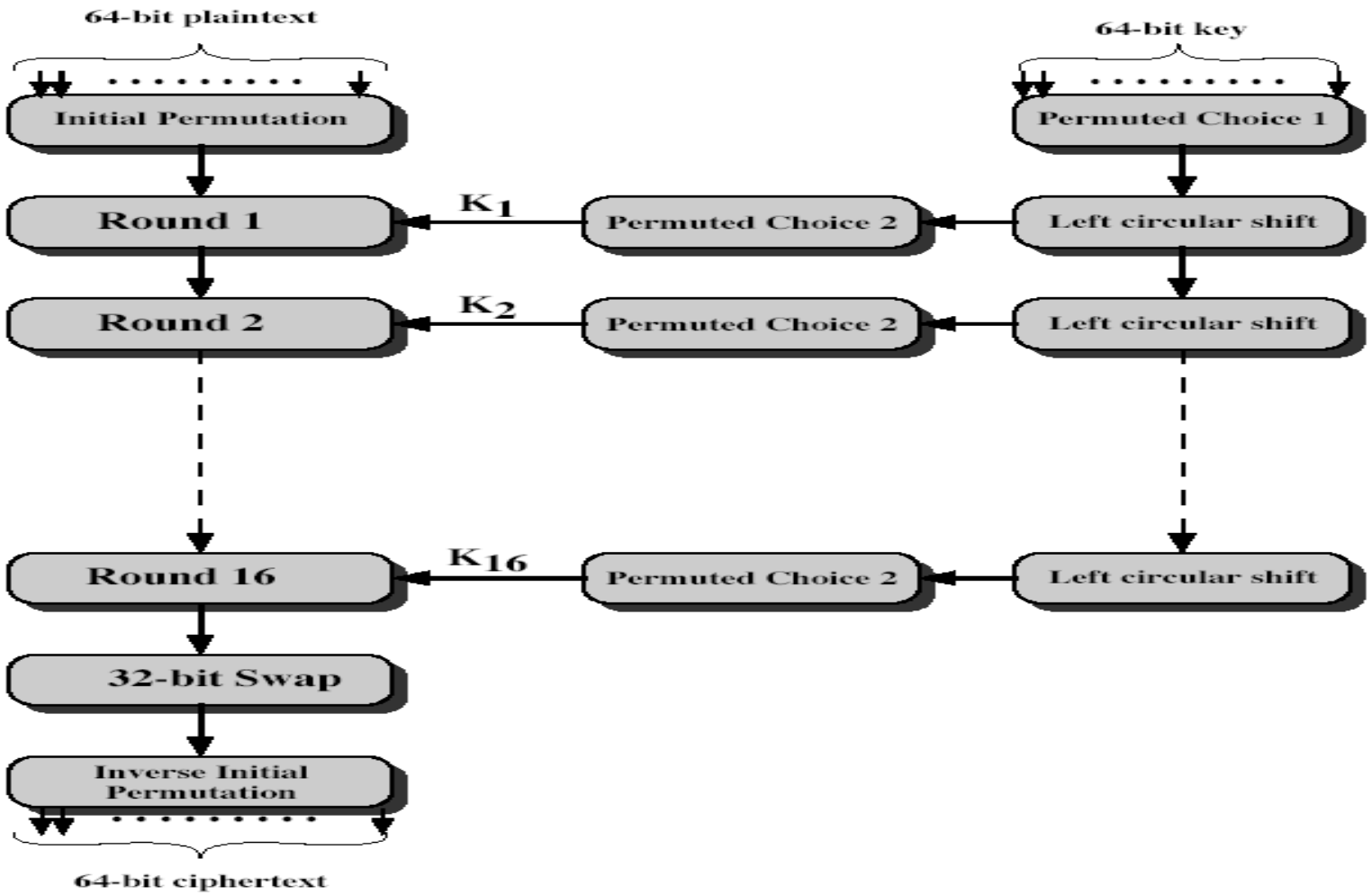
Defining the Block Cipher Algorithm

BEACH

- First point, it uses some transposition orders which are already pre-defined.
- Hence we need to arrange the bits in the given order
- Since it is fixed we have to follow the transposition order
- Transposition order means rearranging the bit position

Data Encryption Standard (DES)

BEACH

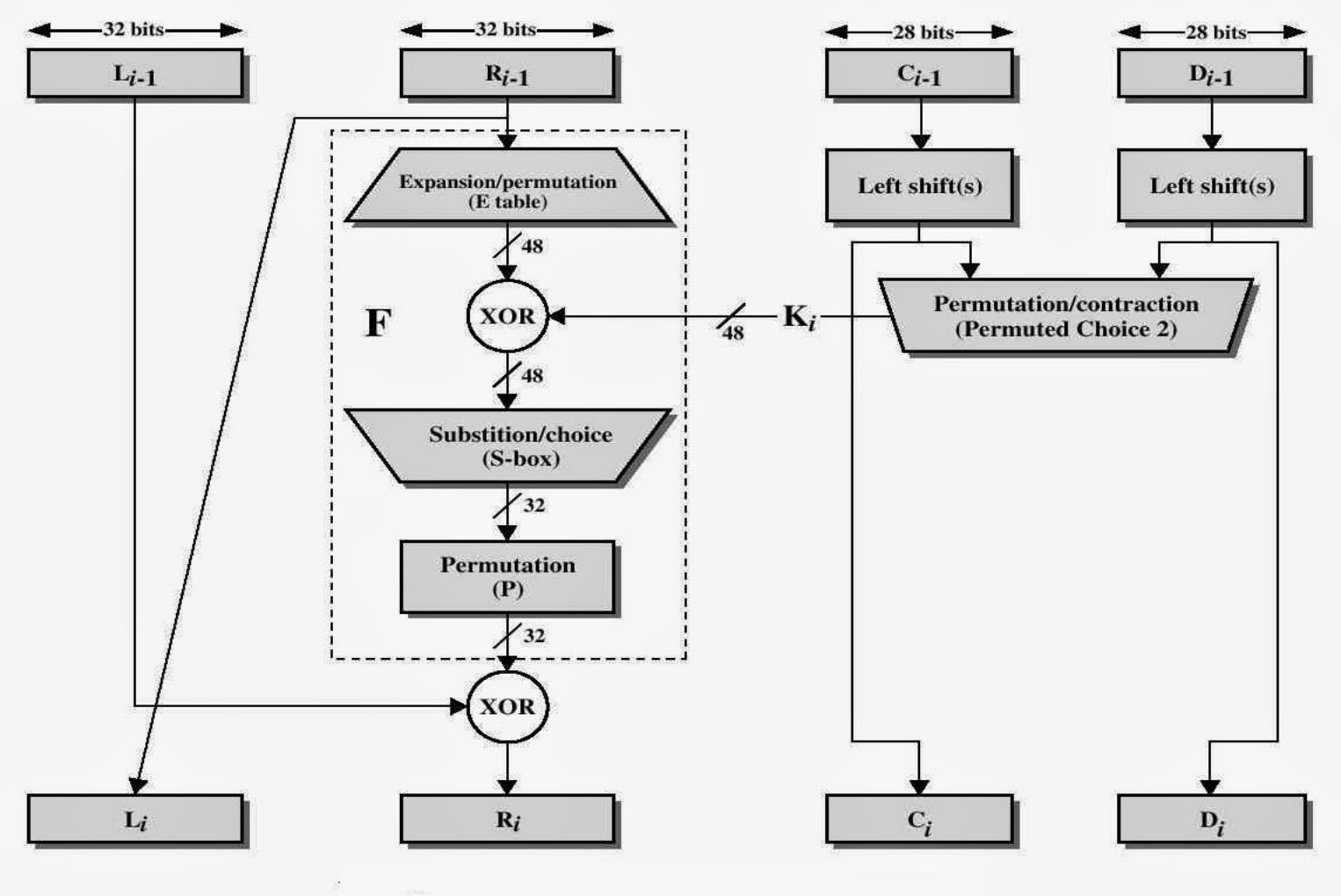


Analyzing Round Function

BEACH

- What exactly happens in this round function?
  - Vaguely we are generating the sub-keys
  - We have 16 rounds, so 16 keys should be generated
- What operations or what functions are happening within this round?

DES Round Function



Initial Permutation

BEACH

- First step of the data computation
- IP reorders the input data bits
- 64 bits → 8x8

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

Initial Permutation

BEACH

- Then the initial permutation will be permuted input as 64 bits

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

Expansion Permutation

BEACH

- Expand R 32 bits to 48 bits to fit the subkey by preforming the Expansion permutation (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	28
24	25	26	27	28	29
28	29	30	31	32	1

Permutated Choice 1

BEACH

- 56 bits pass through a permutation Choice one (PC-1)

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	21	4

Permutated Choice 2

BEACH

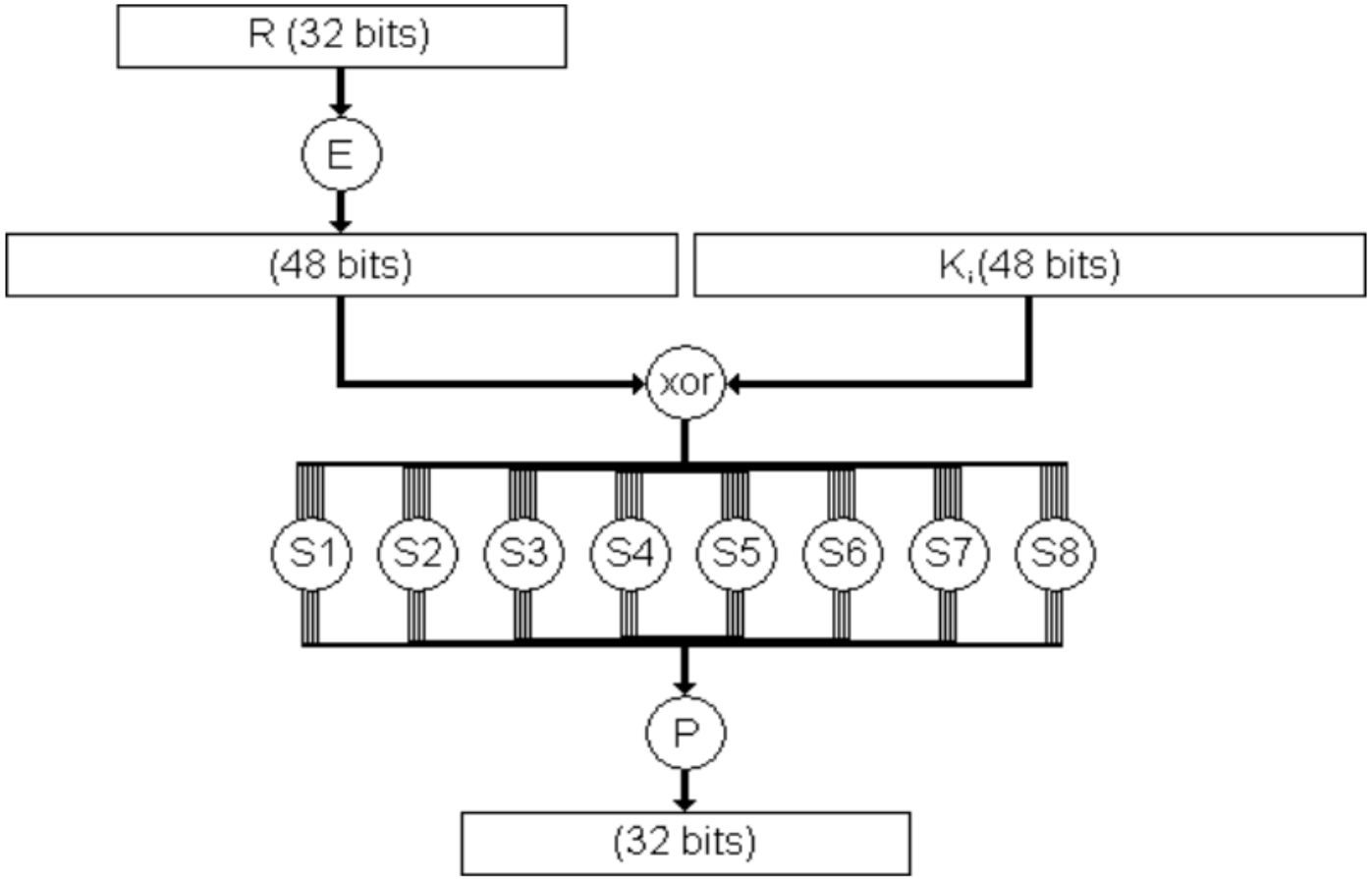
- Passes through permutation choice two (PC-2) to produce 48 bits

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Substitution Box (S-Box)

BEACH

- S-Box consists of 8 boxes, each of which accepts 6 bits as input and produces 4 bits output
- Input → 48 bit
- Output → 32 bit



Substitution Box (S-Box)

BEACH

- Consider 6-bits → 100110
- First and last = Rows
- B/w four bits = Colums

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

S-Box → Permutation

BEACH

- It means we have to follow some transposition order
- Rearrange the bits
- 32 bits in → 32 bits out

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

Inverse Initial Permutation(Final)

BEACH

- After the 16 rounds
- We will do a 32 bit swap
- This will be the ciphertext

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