Cryptlography and Network Security

Unit-III

Session 17

Dr. V. K. Pachghare

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

International Data Encryption Algorithm

(IDEA)

Overview

- A symmetric encryption block cipher

Overview

- A symmetric encryption block cipher
- Mixing of three incompatible algebraic operations on 16-bit blocks:
  - bitwise XOR
  - addition modulo 2^{16} and
  - multiplication modulo $2^{16} + 1$

Overview

- A symmetric encryption block cipher
- Mixing of three incompatible algebraic operations on 16-bit blocks:
  – bitwise XOR
  – addition modulo 2^{16} and
  – multiplication modulo $2^{16} + 1$
- Avoids the use of any lookup tables or S-boxes

Detailed description

- Plaintext and ciphertext Block: 64-bit

Detailed description

- Plaintext and cipher text Block: 64-bit
- Key: 128-bit

Detailed description

- Plaintext and cipher text Block: 64-bit
- Key: 128-bit
- There are total eight and half rounds

Detailed description

- Plaintext and cipher text Block: 64-bit
- Key: 128-bit
- There are total eight and half rounds
- The first eight rounds are identical.

Detailed description

- Plaintext and cipher text Block: 64-bit
- Key: 128-bit
- There are total eight and half rounds
- The first eight rounds are identical.
- The last round is a half round which uses only first four steps (operations) of the other rounds

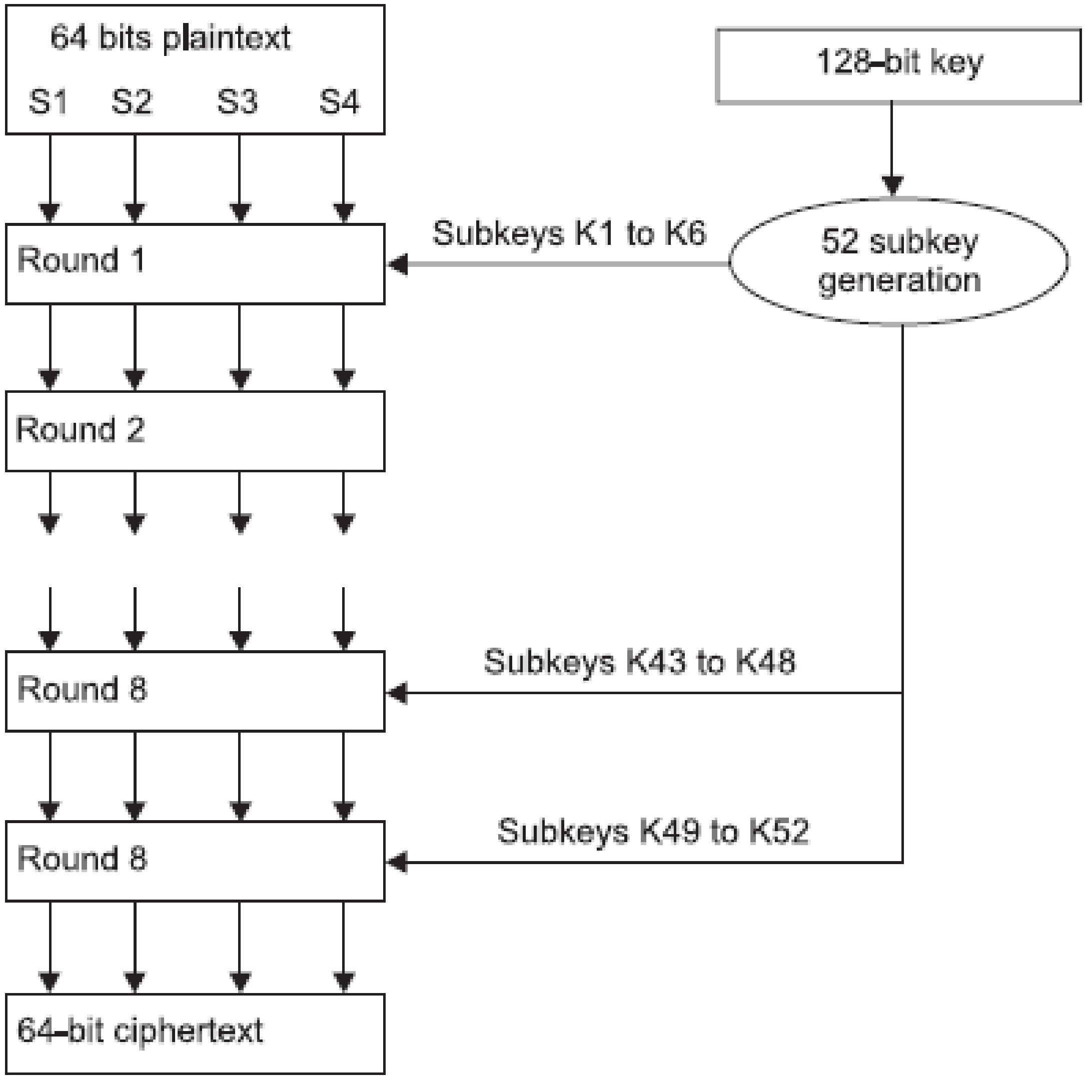
- The encryption process is identical to the decryption process

- The encryption process is identical to the decryption process
- But the subkeys for decryption are different from encryption

- Each round except last round uses 6 sub-keys of 16-bit each.

- Each round except last round uses 6 sub-keys of 16-bit each.
- Last round uses 4 sub-keys.

- Each round except last round uses 6 sub-keys of 16-bit each.
- Last round use 4 sub-keys.
- Total of 52 (= 8 x 6 + 4) different 16-bit sub-keys have to be generated from the 128-bit key


64 bits plaintext
S1
S2
S3
S4
128–bit key
Round 1
Subkeys K1 to K6
52 subkey generation
Round 2
Round 8
Subkeys K43 to K48
Round 8
Subkeys K49 to K52
64–bit ciphertext

Working

The working of IDEA is divided into two parts:

- Key generation
- Encryption

Key Generation

- Total nine rounds.

Key Generation

- Total nine rounds.
- Total 52 subkeys of 16 bits are required for encryption.

Key Generation

- Total nine rounds.
- Therefore, total 52 subkeys of 16 bits are required for encryption.
- Same number of keys are required for decryption.

- The first step of the algorithm is to generate 52 subkeys, K_1 to K_{52}.
- The original key for IDEA is 128-bit key.
- This key is used to generate the subkeys

Subkey generation process

- **Step 1:**

  Split the 128-bit key into 8 parts of 16 bits each

  These parts are the first eight subkeys K_1 to K_8

Subkey generation process

- **Step 1:**

  Split the 128-bit key into 8 parts of 16 bits each

  These are the first eight subkeys K_1 to K_8

Bit position	1 to 16	17 to 32	33 to 48	49 to 64	65 to 80	81 to 96	97 to 112	113 to 128
Subkey	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8

Subkey generation process

- **Step 2:**
  - Then apply circular left shift by 25 bits position on the 128-bit key
  - Split the key again into eight parts of 16 bits each
  - This gives next 8 subkeys, i.e., K_9 to K_{16}.

Subkey generation process

- **Step 2:**
  - Then apply circular left shift by 25 bits position on the 128-bit key
  - Split the key again into eight parts of 16 bits each
  - This gives next 8 subkeys, i.e., K_9 to K_{16}.

Bit position	26 to 41	42 to 57	58 to 73	74 to 89	90 to 105	106 to 121	122 to 9	10 to 25
Subkey	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}

- **Step 3:**
  - Repeat step 2 until all 52 subkeys are generated

- Subkeys K_{17} to K_{24} are generated by starting from bit number 51 of the original key.

- Subkeys K_{17} to K_{24} are generated by starting from bit number 51 of the original key.
- Subkeys K_{25} to K_{32} are generated by starting from bit number 76 of the original key.

- Subkeys K_{17} to K_{24} are generated by starting from bit number 51 of the original key.
- Subkeys K_{25} to K_{32} are generated by starting from bit number 76 of the original key.
- Subkeys K_{33} to K_{40} are generated by starting from bit number 101 of the original key.

- Subkeys K_{17} to K_{24} are generated by starting from bit number 51 of the original key.
- Subkeys K_{25} to K_{32} are generated by starting from bit number 76 of the original key.
- Subkeys K_{33} to K_{40} are generated by starting from bit number 101 of the original key.
- Subkeys K_{41} to K_{48} are generated by starting from bit number 125 of the original key.

- Subkeys K_{17} to K_{24} are generated by starting from bit number 51 of the original key.
- Subkeys K_{25} to K_{32} are generated by starting from bit number 76 of the original key.
- Subkeys K_{33} to K_{40} are generated by starting from bit number 101 of the original key.
- Subkeys K_{41} to K_{48} are generated by starting from bit number 125 of the original key.
- Subkeys K_{49} to K_{52} are generated by starting from bit number 22 of the original key

- The repetitions in the subkeys are avoided due to circular left shift of 25 bits

Key generation for Decryption

- For generation of subkeys for decryption, subkeys for encryption are used in reverse order
- Suppose the key for encryption is denoted by K and the key for decryption is denoted by Z.
- K_1 to K_{52} denotes the subkeys for encryption
- Z_1 to Z_{52} denotes the subkeys for decryption

- For generation of subkeys for decryption, subkeys for encryption are used in reverse order
- For first four keys of decryption round 1, first four keys of last round of encryption are used
- i.e., encryption subkeys K_{49} to K_{52} are used to generate decryption subkeys Z_1 to Z_4.
- For generation of these subkeys, multiplicative inverse and additive inverse are used.

- For last two keys of decryption round 1, last two keys of eighth round of encryption are used
- i.e., encryption subkeys K_{47} to K_{48} are used to generate decryption subkeys Z_5 to Z_6.

Subkeys for encryption

	R-1	R-2	R-3	R-4	R-5	R-6	R-7	R-8	R-9
K-1	K_1	K_7	K_{13}	K_{19}	K_{25}	K_{31}	K_{37}	K_{43}	K_{49}
K-2	K_2	K_8	K_{14}	K_{20}	K_{26}	K_{32}	K_{38}	K_{44}	K_{50}
K-3	K_3	K_9	K_{15}	K_{21}	K_{27}	K_{33}	K_{39}	K_{45}	K_{51}
K-4	K_4	K_{10}	K_{16}	K_{22}	K_{28}	K_{34}	K_{40}	K_{46}	K_{52}
K-5	K_5	K_{11}	K_{17}	K_{23}	K_{29}	K_{35}	K_{41}	K_{47}	
K-6	K_6	K_{12}	K_{18}	K_{24}	K_{30}	K_{36}	K_{42}	K_{48}	

Subkeys for decryption

	R-1	R-2	R-3	R-4	R-5	R-6	R-7	R-8	R-9
K-1	Z_1	Z_7	Z_{13}	Z_{19}	Z_{25}	Z_{31}	Z_{37}	Z_{43}	Z_{49}
K-2	Z_2	Z_8	Z_{14}	Z_{20}	Z_{26}	Z_{32}	Z_{38}	Z_{44}	Z_{50}
K-3	Z_3	Z_9	Z_{15}	Z_{21}	Z_{27}	Z_{33}	Z_{39}	Z_{45}	Z_{51}
K-4	Z_4	Z_{10}	Z_{16}	Z_{22}	Z_{28}	Z_{34}	Z_{40}	Z_{46}	Z_{52}
K-5	Z_5	Z_{11}	Z_{17}	Z_{23}	Z_{29}	Z_{35}	Z_{41}	Z_{47}	
K-6	Z_6	Z_{12}	Z_{18}	Z_{24}	Z_{30}	Z_{36}	Z_{42}	Z_{48}	

Subkeys for encryption

	R-1	R-2	R-3	R-4	R-5	R-6	R-7	R-8	R-9
K-1	K_1	K_7	K_{13}	K_{19}	K_{25}	K_{31}	K_{37}	K_{43}	K_{49}
K-2	K_2	K_8	K_{14}	K_{20}	K_{26}	K_{32}	K_{38}	K_{44}	K_{50}
K-3	K_3	K_9	K_{15}	K_{21}	K_{27}	K_{33}	K_{39}	K_{45}	K_{51}
K-4	K_4	K_{10}	K_{16}	K_{22}	K_{28}	K_{34}	K_{40}	K_{46}	K_{52}
K-5	K_5	K_{11}	K_{17}	K_{23}	K_{29}	K_{35}	K_{41}	K_{47}	
K-6	K_6	K_{12}	K_{18}	K_{24}	K_{30}	K_{36}	K_{42}	K_{48}	

Subkeys for decryption first round

	R-1	R-9/R-8	R-1
K-1	Z_1	K_{49}	$(K_{49})^{-1}$mod $(2^{16}+1)$
K-2	Z_2	K_{50}	$-(K_{50})$mod (2^{16})
K-3	Z_3	K_{51}	$-(K_{51})$mod (2^{16})
K-4	Z_4	K_{52}	$(K_{52})^{-1}$mod $(2^{16}+1)$
K-5	Z_5	K_{47}	K_{47}
K-6	Z_6	K_{48}	K_{48}

Subkeys for decryption second round

	R-2	R-8/R-7	
K-1	Z_7	K_{43}	$(K_{43})^{-1}\text{mod } (2^{16}+1)$
K-2	Z_8	K_{44}	$-(K_{44})\text{mod } (2^{16})$
K-3	Z_9	K_{45}	$-(K_{45})\text{mod } (2^{16})$
K-4	Z_{10}	K_{46}	$(K_{46})^{-1}\text{mod } (2^{16}+1)$
K-5	Z_{11}	K_{41}	K_{41}
K-6	Z_{12}	K_{42}	K_{42}

Subkeys for decryption third round

	R-2	R-7/R-6	
K-1	Z_{13}	K_{37}	$(K_{37})^{-1} \bmod (2^{16}+1)$
K-2	Z_{14}	K_{38}	$-(K_{38}) \bmod (2^{16})$
K-3	Z_{15}	K_{39}	$-(K_{39}) \bmod (2^{16})$
K-4	Z_{16}	K_{40}	$(K_{40})^{-1} \bmod (2^{16}+1)$
K-5	Z_{17}	K_{35}	K_{35}
K-6	Z_{18}	K_{36}	K_{36}

Subkeys for decryption fourth round

	R-2	R-6/R-5	
K-1	Z_{19}	K_{31}	$(K_{31})^{-1} \bmod (2^{16}+1)$
K-2	Z_{20}	K_{32}	$-(K_{32}) \bmod (2^{16})$
K-3	Z_{21}	K_{33}	$-(K_{33}) \bmod (2^{16})$
K-4	Z_{22}	K_{34}	$(K_{34})^{-1} \bmod (2^{16}+1)$
K-5	Z_{23}	K_{29}	K_{29}
K-6	Z_{24}	K_{30}	K_{30}

Subkeys for decryption fifth round

	R-2	R-5/R-4	
K-1	Z_{25}	K_{25}	$(K_{25})^{-1} \bmod (2^{16}+1)$
K-2	Z_{26}	K_{26}	$-(K_{26}) \bmod (2^{16})$
K-3	Z_{27}	K_{27}	$-(K_{27}) \bmod (2^{16})$
K-4	Z_{28}	K_{28}	$(K_{28})^{-1} \bmod (2^{16}+1)$
K-5	Z_{29}	K_{23}	K_{23}
K-6	Z_{30}	K_{24}	K_{24}

Subkeys for decryption sixth round

	R-2	R-4/R-3	
K-1	Z_{31}	K_{19}	$(K_{19})^{-1} \bmod (2^{16}+1)$
K-2	Z_{32}	K_{20}	$-(K_{20}) \bmod (2^{16})$
K-3	Z_{33}	K_{21}	$-(K_{21}) \bmod (2^{16})$
K-4	Z_{34}	K_{22}	$(K_{22})^{-1} \bmod (2^{16}+1)$
K-5	Z_{35}	K_{17}	K_{17}
K-6	Z_{36}	K_{18}	K_{18}

Subkeys for decryption seventh round

	R-2	R-3/R-2	
K-1	Z_{37}	K_{13}	$(K_{13})^{-1} \bmod (2^{16}+1)$
K-2	Z_{38}	K_{14}	$-(K_{14}) \bmod (2^{16})$
K-3	Z_{39}	K_{15}	$-(K_{15}) \bmod (2^{16})$
K-4	Z_{40}	K_{16}	$(K_{16})^{-1} \bmod (2^{16}+1)$
K-5	Z_{41}	K_{11}	K_{11}
K-6	Z_{42}	K_{12}	K_{12}

Subkeys for decryption eight round

	R-8	R-2/R-1	
K-1	Z_{43}	K_7	$(K_7)^{-1} \bmod (2^{16}+1)$
K-2	Z_{44}	K_8	$-(K_8) \bmod (2^{16})$
K-3	Z_{45}	K_9	$-(K_9) \bmod (2^{16})$
K-4	Z_{46}	K_{10}	$(K_{10})^{-1} \bmod (2^{16}+1)$
K-5	Z_{47}	K_5	K_5
K-6	Z_{48}	K_6	K_6

Subkeys for decryption ninth round

	R-9	R-1	
K-1	Z_{49}	K_1	$(K_1)^{-1} \bmod (2^{16}+1)$
K-2	Z_{50}	K_2	$-(K_2) \bmod (2^{16})$
K-3	Z_{51}	K_3	$-(K_3) \bmod (2^{16})$
K-4	Z_{52}	K_4	$(K_4)^{-1} \bmod (2^{16}+1)$

Encryption

- Plaintext block is 64 bits

Encryption

- Plaintext block is 64 bits
- Divide the plaintext block into 4 sub blocks of 16 bits each.

Encryption

- Plaintext block is 64 bits
- Divide the plaintext block into 4 sub blocks of 16 bits each.
- Suppose sub blocks are P_1, P_2, P_3, P_4

Encryption

- There are total nine rounds, eight complete and one half rounds.

Encryption

- There are total nine rounds, eight complete and one half rounds.
- The encryption is done using 52 subkeys

Encryption

- There are total nine rounds, eight complete and one half rounds.
- The encryption is done using 52 subkeys
- The first eight rounds use 6 subkeys each

Encryption

- There are total nine rounds, eight complete and one half rounds.
- The encryption is done using 52 subkeys
- The first eight rounds use 6 subkeys each
- The last round uses 4 subkeys.

Encryption

- There are total nine rounds, eight complete and one half rounds.
- The encryption is done using 52 subkeys
- The first eight rounds use 6 subkeys each
- The last round uses 4 subkeys.
- So, the first round uses subkeys K_1 to K_6

Encryption

- There are total nine rounds, eight complete and one half rounds.
- The encryption is done using 52 subkeys
- The first eight rounds use 6 subkeys each
- The last round uses 4 subkeys.
- So, the first round uses subkeys K_1 to K_6
- Each round have 14 steps

Encryption

- There are total nine rounds, eight complete and one half rounds.
- The encryption is done using 52 subkeys
- The first eight rounds use 6 subkeys each
- The last round uses 4 subkeys.
- So, the first round uses subkeys K_1 to K_6
- First eight rounds have 14 steps
- Last round has 4 steps

Operation Used

- Multiplication modulo $2^{16}+1$
  - Ex. $P_1 * K_1 \bmod (2^{16}+1)$
- Addition modulo 2^{16}
  - Ex. $(P_1 + K_1) \bmod 2^{16}$
- XOR

ALGORITHM

1. Multiplication modulo $2^{16}+1$ between P_1 and the first subkey K_1. The result is $S_{1.}$

$$(P_1)_{10} * (K_1)_{10} \bmod 65537 = S_{1.}$$

ALGORITHM

1. Multiplication modulo $2^{16}+1$ between P_1 and the first subkey K_1. The result is $S_{1.}$
2. Addition modulo 2^{16} between P_2 and the second subkey K_2. The result is $S_{2.}$

$$(P_2)_{10} + (K_2)_{10} \text{mod } 65536 = S_{2.}$$

ALGORITHM

1. Multiplication modulo $2^{16}+1$ between P_1 and the first subkey K_1. The result is $S_{1.}$
2. Addition modulo 2^{16} between P_2 and the second subkey K_2. The result is $S_{2.}$
3. Addition modulo 2^{16} between P_3 and the third subkey K_3. The result is $S_{3.}$

ALGORITHM

1. Multiplication modulo $2^{16}+1$ between P_1 and the first subkey K_1. The result is $S_{1.}$
2. Addition modulo 2^{16} between P_2 and the second subkey K_2. The result is $S_{2.}$
3. Addition modulo 2^{16} between P_3 and the third subkey K_3. The result is $S_{3.}$
4. Multiplication modulo $2^{16}+1$ between P_4 and the fourth subkey K_4. The result is $S_{4.}$

5. Apply XOR between S_1 and S_3. The result is $S_{5.}$

5. Apply XOR between S_1 and S_3. The result is $S_{5.}$

6. Apply XOR between S_2 and S_4. The result is $S_{6.}$

5. Apply XOR between S_1 and S_3. The result is $S_{5.}$

6. Apply XOR between S_2 and S_4. The result is $S_{6.}$

7. Multiplication modulo $2^{16}+1$ between S_5 and the fifth subkey K_5. The result is S_7.

5. Apply XOR between S_1 and S_3. The result is S_5.

6. Apply XOR between S_2 and S_4. The result is S_6.

7. Multiplication modulo $2^{16}+1$ between S_5 and the fifth subkey K_5. The result is S_7.

8. Addition modulo 2^{16} between S_6 and S_7. The result is S_8.

5. Apply XOR between S_1 and S_3. The result is S_5.

6. Apply XOR between S_2 and S_4. The result is S_6.

7. Multiplication modulo $2^{16}+1$ between S_5 and the fifth subkey K_5. The result is S_7.

8. Addition modulo 2^{16} between S_6 and S_7. The result is S_8.

9. Multiplication modulo $2^{16}+1$ between S_8 and the sixth subkey K_6. The result is S_9.

5. Apply XOR between S_1 and S_3. The result is S_5.

6. Apply XOR between S_2 and S_4. The result is S_6.

7. Multiplication modulo $2^{16}+1$ between S_5 and the fifth subkey K_5. The result is S_7.

8. Addition modulo 2^{16} between S_6 and S_7. The result is S_8.

9. Multiplication modulo $2^{16}+1$ between S_8 and the sixth subkey K_6. The result is S_9.

10. Addition modulo 2^{16} between S_7 and S_9. The result is S_{10}.

11. Apply XOR between S_1 and S_9. The result is S_{11}

11. Apply XOR between S_1 and S_9. The result is S_{11}

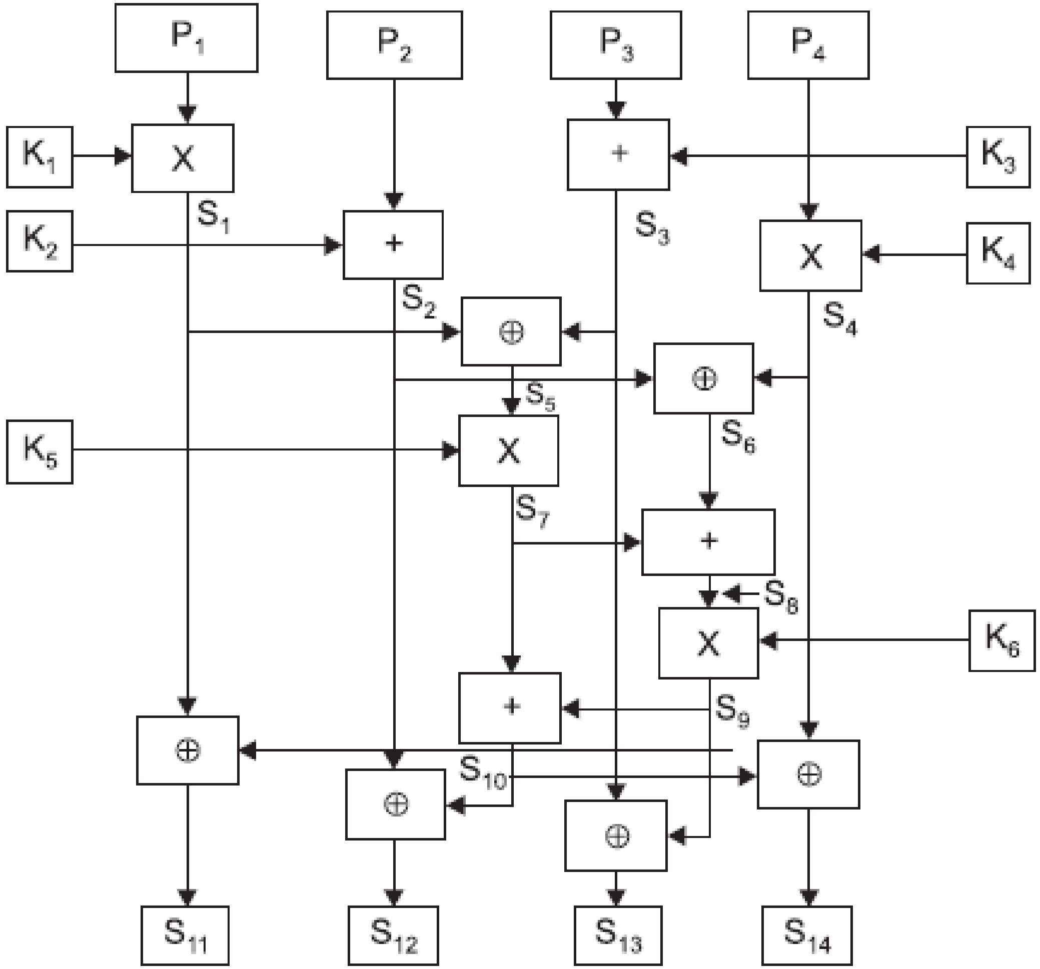
12. Apply XOR between S_2 and S_{10}. The result is S_{12}

11. Apply XOR between S_1 and S_9. The result is S_{11}

12. Apply XOR between S_2 and S_{10}. The result is S_{12}

13. Apply XOR between S_3 and S_9. The result is S_{13}

11. Apply XOR between S_1 and S_9. The result is S_{11}
12. Apply XOR between S_2 and S_{10}. The result is S_{12}
13. Apply XOR between S_3 and S_9. The result is S_{13}
14. Apply XOR between S_4 and S_{10}. The result is S_{14}



X : Multiplication modulo $2^{16}+1$

+ : Addition modulo 2^{16}

⊕ : XOR operation

Round 9

1. Multiplication modulo $2^{16}+1$ between P_1 and the subkey K_{49}. The result is $C_{1.}$
2. Addition modulo 2^{16} between P_2 and the subkey K_{50}. The result is $C_{2.}$
3. Addition modulo 2^{16} between P_3 and the subkey K_{51}. The result is $C_{3.}$
4. Multiplication modulo $2^{16}+1$ between P_4 and the subkey K_{52}. The result is $C_{4.}$

Decryption

- The computational process used for decryption of the ciphertext is essentially the same as that used for encryption
- The only difference is that each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption

Questions ?