# ICT - Unit 3 : Block Cipher

Dr A Chamundeswari, Professor, Dept of CSE, SSNCE

September 13, 2021

# Table of contents

# 6.2.1 Substitution-Permutation Networks

- SPN is a model of block cipher.
- A block cipher must behave like a random permutation
- There are $2^\ell!$ permutations on $\ell$-bit strings, so representing an arbitrary permutation.
- Example: 24 permutation on a 2-bit string for a single block.
- Each bit of the output is changed with probability roughly half.

# The confusion-diffusion paradigm.

- For perfect secrecy, shannon introduced confusion and diffusion operations.
- Confusion : relationship between plain and ciphertext are hiden. eg.substitution table, look table is used.
- Diffusion : the influence of one each plain text bit is spread over many cipher text. eg. Permutation bits.
- Confusion and diffusion together called a round are repeated multiple times.
- Changing a single bit of the input will affect all the bits of the output.

# Substitution Permutation Networks(SPN)

- Direct implementation of the confusion-diffusion paradigm.
- key, k specify an arbitary permutation f, substitution function S called S-box, f(x)=S(k $\oplus$ x)
- For x=64 block length, 8 bit S -box, cipher is obtained in a series of rounds, for each round the following sequence of operations, key mixing, substitution, permutation.
- The output of each round is fed as inut to the next round. After the last there is a final key-mixing step, and the result is the output of the cipher.

1. *Key mixing:* Set $x := x \oplus k$, where $k$ is the current-round sub-key;
2. *Substitution:* Set $x := S_1(x_1) \| \cdots \| S_8(x_8)$, where $x_i$ is the $i$th byte of $x$;
3. *Permutation:* Permute the bits of $x$ to obtain the output of the round.

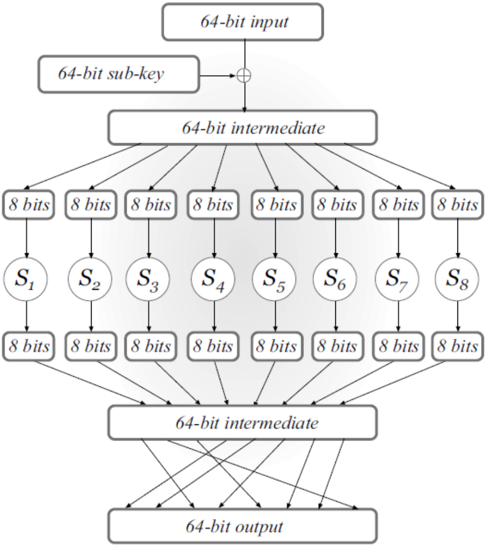


**FIGURE 6.3**: A single round of a substitution-permutation network.

# SPN

- Different sub-keys (or round keys) are used in each round.
- The actual key of the block cipher is sometimes called the **master key**.
- The round **sub-keys** are derived from the master key according to a **key schedule**.
- An r-round SPN has r (full) rounds of key mixing, S-box substitution, and application of a mixing permutation, followed by a final key-mixing step.
- An r-round SPN, $r + 1$ sub-keys are used.

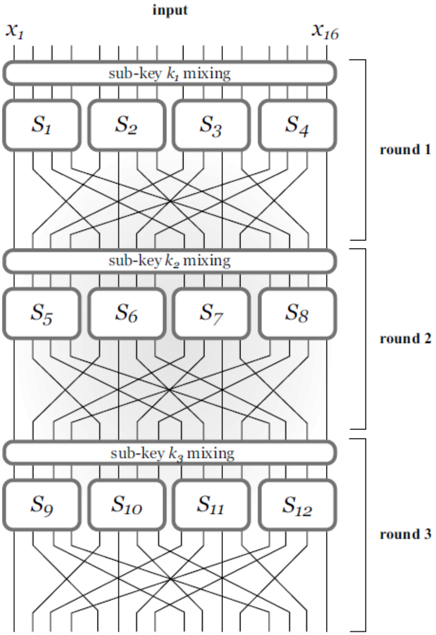


FIGURE 6.4: A substitution-permutation network.

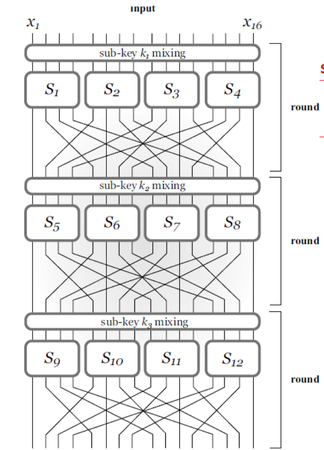


FIGURE 6.4: A substitution-permutation network.

round 1

x=1001 1100 1011 1001

sub-key,k=1000 1001 0011 1100 (xor)

0001 0101 1000 0101

0001 1100 1110 1100

1000 0000 0001 0000

sub-key $k_1$ mixing

substitution-

| P | 00 |
|---|---|
| 0000 | 1111 |
| 0001 | 0001 |
| 0010 | 1010 |
| 0011 | 0111 |
| 0100 | 1000 |
| 0101 | 1100 |
| 0110 | 1011 |
| 0111 | 0000 |
| 1000 | 1110 |
| 1001 | 1001 |
| 1010 | 0100 |
| 1011 | 0110 |
| 1100 | 0101 |
| 1101 | 1101 |
| 1110 | 0010 |
| 1111 | 0011 |

permutation

| input | permutation |
|---|---|
| 0000 | 1101 |
| 0001 | 1000 |
| 0010 | 1001 |
| 0011 | 1100 |
| 0100 | 1010 |
| 0101 | 1110 |
| 0110 | 1011 |
| 0111 | 1111 |
| 1000 | 0111 |
| 1001 | 0110 |
| 1010 | 0011 |
| 1011 | 0101 |
| 1100 | 0000 |
| 1101 | 0100 |
| 1110 | 0001 |
| 1111 | 0010 |

# SPN

- Any **SPN is invertible** (given the key). Output of the SPN and the key it is possible to recover the input.
- Single round can be inverted and the entire SPN can be inverted by working from the final round back to the beginning.
- But inverting a single round is easy: the mixing permutation can easily be inverted since it is just a re-ordering of bits.
- Since the S-boxes are permutations (i.e., one-to-one), these too can be inverted.
- The result can then be XORed with the appropriate sub-key to obtain the original input.

# SPN - secure

- Highly secure block cipher depends on

  (1) the number of rounds

  (2) S-boxes

  (3) mixing permutations

  (4) key schedule

# SPN - avalanche effect

- **Avalanche effect:** Property in any block cipher is that a small change in the input must affect every bit of the output.
- S-boxes have input/output size of 8 bits, and that the **block length of the cipher is 128 bits**

1 After the first round, the intermediate values differ in exactly two bit positions.

2. The mixing permutation applied at the end of the first round spreads the two bit-positions where the intermediate results differ into two different S-boxes in the second round.
3. Continuing the same argument, we expect 8 bits of the intermediate value to be affected after the 3rd round,
4. 16 bits to be affected after the 4th round.

4. **All 128 bits** of the output to be affected at the end of the **7th round**.

## 6.2.2 Feistel Networks

- Feistel networks offer another approach for constructing block ciphers.
- **S-boxes used in SPNs need not be invertible** in fesitel networks, thus making them harder to design.
- A Feistel network operates in a series of rounds and the round functions need not be invertible.
- Constructed from components like S-boxes and mixing permutations
- A Feistel network can deal with any round functions.

# Feistel Networks

- Balanced Feistel network, the ith round function $\widehat{f_i}$ takes as input a sub-key $k_i$ and an $\ell/2$ -bit string and outputs an $\ell/2$-bit string.
- sub key is derived from master key.
- $\mathrm{f}_i : \{ 0,1 \}^{\ell/2} \rightarrow \{ 0,1 \}^{\ell/2}$ via $\mathrm{f}_i\ (\mathrm{R}) = \widehat{f_i}(k_i,\mathrm{R})$
- round functions $\widehat{f_i}$ are fixed and publicly known, but the $f_i$ depend on the master key and so are not known to the attacker.

# Feistel Networks

- The ith round of a Feistel network operates as follows.
- The input to the round is divided into two halves denoted $L_{i-1}$ and $R_{i-1}$
- If the block length of the cipher is $\ell$ bits, then $L_{i-1}$ and $R_{i-1}$ each has length $\ell/2$.

  $\ell = 64 bits, L_{i-1} = 32 bits, R_{i-1}$ =32 bits

- The output ($L_i$,$R_i$) of the round is

  $L_i := R_{i-1}$

  $R_i := L_{i-1} \oplus f_i(R_{i-1})$

# Feistel Networks

- In an r-round Feistel network, the $\ell$-bit input to the network is parsed as ($L_0$,$R_0$), and the output is the $\ell$-bit value ($L_r$,$R_r$) obtained after applying all r rounds.

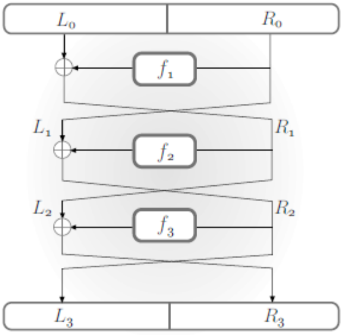


**FIGURE 6.5:** A three-round Feistel network.

# Feistel Networks

$$f_i\ (\mathrm{R}) = \widehat{f_i}(k_i,\mathrm{R})$$

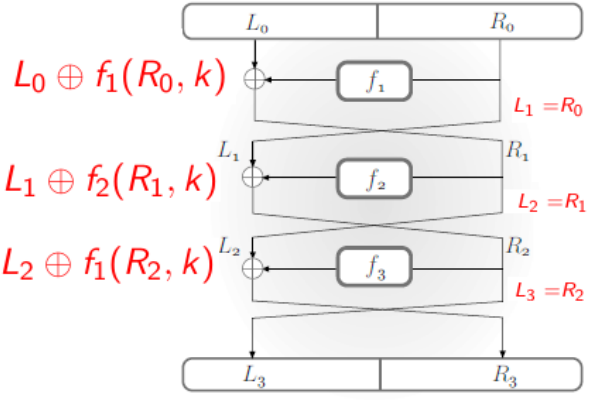


**FIGURE 6.5:** A three-round Feistel network.

# Feistel Networks

## Inverting a Feistal network

- A feistel network is invertible regardless of $\mathrm{f}_i$
- Each round of the network can be inverted if the $\mathrm{f}_i$ are known.
- Given the ith round $(L_i,\ R_i)$ , compute $(L_{i-1},\ R_{i-1})$

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f_i(R_{i-1}, k)$$

$$f_i(R_{i-1}, k) \oplus R_i = L_{i-1} \oplus f_i(R_{i-1}, k) \underline{\oplus f_i(R_{i-1}, k)}$$

$$\begin{aligned} L_{i-1} &= L_{i-1} \\ &= R_i \oplus f_i(R_{i-1}, k) \\ &= R_i \oplus f_i(L_i, k) \end{aligned}$$

$$L_{i-1} = R_i \oplus f_i(L_i, k) \ \&\ R_{i-1} = L_i$$

## 6.2.3 DES The Data Encryption Standard

- The DES block cipher is a **16-round Feistel network** with a **block length of 64 bits** and a **key length of 56 bits**.
- DES is vulnerable to**brute-force attacks**, due to its short key length of 56 bits.
- Triple-DES
- The DES round function $\widehat{f}$ sometimes called the **DES mangler function**

## 6.2.3 DES The Data Encryption Standard

- **key schedule :** A sequence of 48-bit sub-keys $k_1, \dots, k_{16}$ derived from the 56-bit master key
- 56 bits of the master key are divided into two halves a left half and a right half each containing 28 bits.
- In **each round**, the **left-most 24 bits** of the sub-key are taken as some subset of the 28 bits in the left half of the master key, and the **right-most 24 bits** of the round sub-key are taken as some subset of the 28 bits in the right half of the master key.

# The DES round function

- DES uses a Feistel structure
- $\widehat{f}(k_i, R)$ with $k_i \in \{ 0,1 \}^{48}$ and $R \in \{0,1\}^{32}$
- R is expanded to 48 bits value $R^{'}$, $R^{'} = \mathrm{E(R)}$ where E is called the expansion function.
- $R^{'}$ 48 bits long is XORed with $k_i$ 48 bits long, and the resulting value is divided into 8 blocks, each of which is 6 bits long.
- S$-$box that takes a 6 bit input and yields a 4-bit output. S-box results are not invertible.
- A mixing permutation is then applied to the bits of this result to obtain the final output.
- Public data : mixing permutation, Secret: Master key

# The DES round function

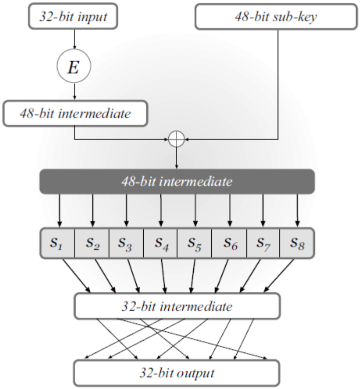


**FIGURE 6.6**: The DES mangler function.

# The DES avalanche effect.

- The DES avalanche effect. The design of the mangler function ensures that DES exhibits a strong avalanche effect.

# 6.2.5 AES The Advanced Encryption Standard

## The AES construction.

- The AES block cipher has a 128-bit block length and can use 128-, 192-, or 256-bit keys.
- The length of the key affects the **key schedule**
- AES is essentially a **substitution-permutation network**
- A 4-by-4 array of bytes called the **state** is modified in a series of rounds.
- The state is initially set equal to the input.
- Operations applied to the state in a series of **four stages** during each round:
- Stage 1 : AddRoundKey, Stage 2: SubBytes, Stage 3 : ShiftRows, Stage 4 : MixColumns, in the final round, MixColumns is replaced with AddRoundKey.
- The number of rounds depends on the key length. Ten rounds are used for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key.

# Security of AES.

- No practical cryptanalytic attacks
- AES constitutes an excellent choice for any cryptographic scheme that requires a (strong) pseudorandom permutation
- It is free, standardized, efficient, and highly secure.

# References


- Introduction to Modern Cryptography, Second Edition, Jonathan Katz, Yehuda Lindell, CRC Press, Tylor and Francis group, 2015.