Information and Networks Security

Block Ciphers Revision

Dr. Heba Rashed
Lecturer of Computer Science

The Feistel Cipher: Overview

The Feistel Cipher structure was developed to utilize a single algorithm for both encryption and decryption tasks.

It functions as a framework rather than a specific algorithm, making it ideal for designing customized encryption solutions tailored to specific security needs or constraints.

Feistel Specifications:

- **Input / Output Sizes:** The size can vary depending on the implementation.
- **Key Size:** The Feistel structure can be adapted to use different key lengths.
- **Rounds:** 16 rounds.

The Feistel Cipher: Pros And Cons

Pros:

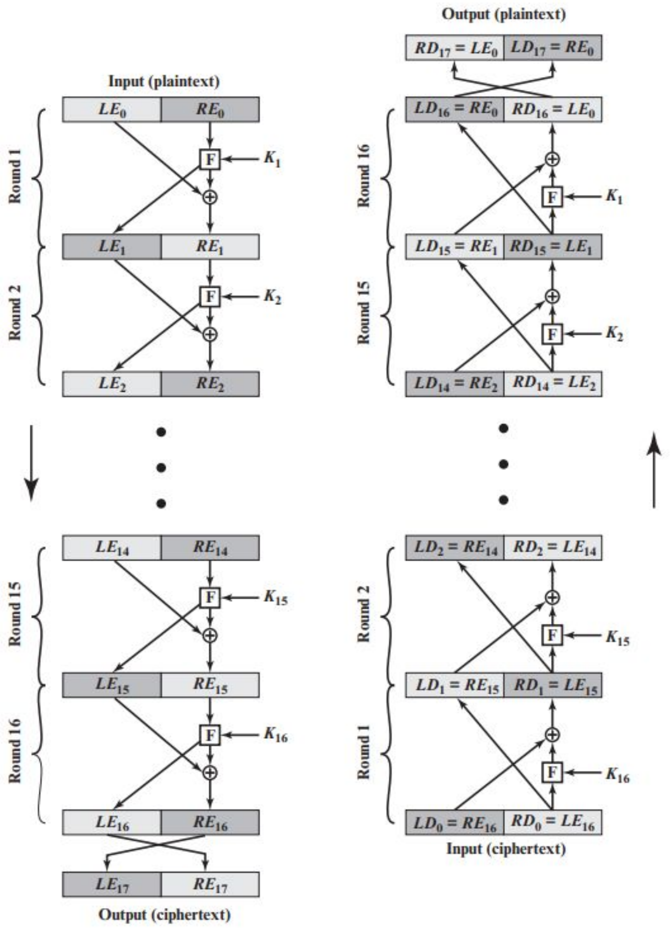
- Highly flexible, allowing for a wide range of block sizes and key lengths.
- It's symmetric, meaning the same key can be used for encryption and decryption.

Cons:

- The iterative nature of Feistel-based encryption can be slower compared to some non-Feistel ciphers, especially in hardware implementations.

The Feistel Cipher: Structure

- Splits data into two halves.
- Processes each half through several rounds of mixing and swapping.
- Uses subkeys derived from the main key.
- Each round applies a round function to one half of the data.
- Combines the results of the round function with the other half.
- Swaps the two halves before the next round.



The DES Cipher: Overview

DES (Data Encryption Standard) was developed to standardize cryptographic security for non-classified information across.

DES Specifications:

- **Input / Output Sizes:** Input and output sizes for DES are fixed at 64 bits.
- **Key Size:** Uses a 56-bit key (plus 8 bits for parity, total 64 bits).
- **Rounds:** 16 rounds.

The DES Cipher: Pros And Cons

Pros:

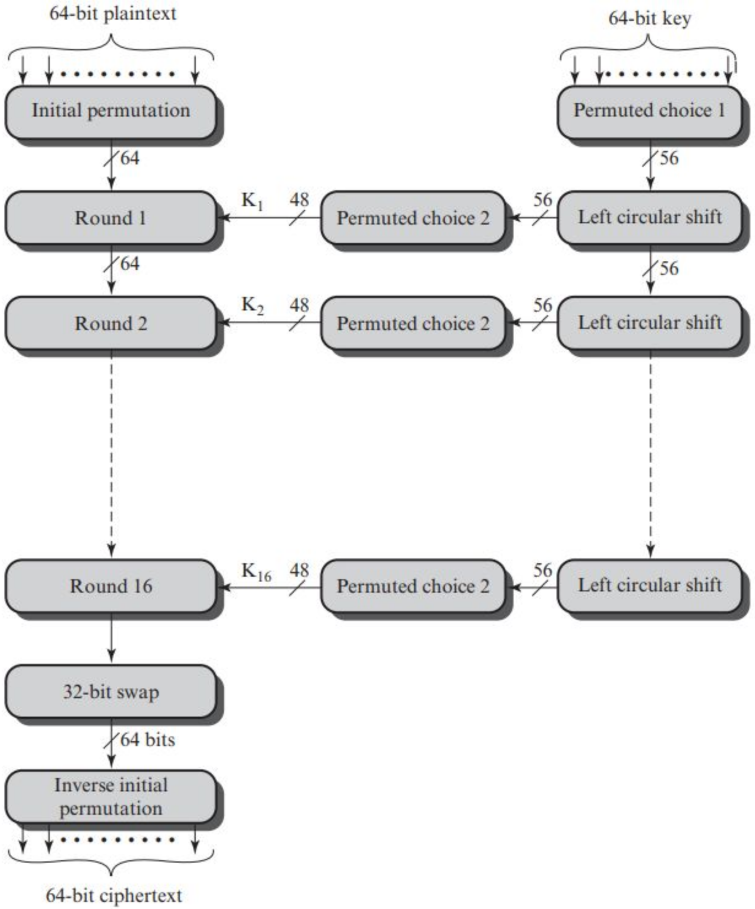
- Was highly secure against most attacks when initially released.
- It's simple and has been extensively tested.

Cons:

- Its key size of 56 bits is no longer considered secure against brute-force attacks.
- It was officially deprecated and replaced by AES.

The DES Cipher: Structure

1. Initial Permutation (IP)
2. 16 Rounds of Encryption
3. Final Permutation (FP)
4. Key Schedule Generates 48-bit round keys.



The DES Cipher: Why DES

- **Legacy Systems:** While DES is considered obsolete due to its vulnerability to brute-force attacks, Triple DES (3DES) is still used in legacy systems where upgrading to AES is not feasible due to hardware constraints or compatibility issues.

- **Intermediate Security Needs:** 3DES offers a higher level of security than DES and can be suitable for encrypting less sensitive information where the risk level does not justify the implementation of AES.

Blowfish & Twofish

Algorithm	Blowfish	Twofish
Blocksize	Encrypts data in 64-bit blocks	Operates on 128-bit blocks
Key Size	variable key size from 32 bits up to 448 bits	Can operate with key sizes of 128, 192, or 256 bits
Structure	● Utilizes a simple Feistel network with a series of 16 rounds. ● Its core relies on key-dependent S-boxes and a complex key schedule.	● More complex structure than Blowfish. ● Utilizes a Feistel-like network called a "Whitening" structure before and after a series of 16 rounds. ● Twofish's design includes pre-computed, key-dependent S-boxes.

Blowfish & Twofish Cont'd

Algorithm	Blowfish	Twofish
Design and Purpose	● Designed for speed and simplicity for systems with limited resources. ● Popular in software applications and systems for its straightforward implementation.	Created for the AES competition. It's structured to offer enhanced security for modern encryption needs.

Blowfish & Twofish Cont'd

	Blowfish	Twofish
Pros	● Very fast, especially in software implementations. ● It provides good security with a variable-length key, making it adaptable to different security needs.	● Offers flexibility in terms of key size. ● It's considered secure against known attacks and has been evaluated extensively during the AES selection process.
Cons	● The block size of 64 bits is now considered less secure against brute-force attacks due to advancements in computing power. ● The initial key setup can be slow.	While efficient, it can be slower than some of its competitors (like AES) in certain implementations.

The Blowfish Cipher: Why Blowfish

- **Small to Medium-Sized Databases:** Blowfish's efficient performance in software makes it suitable for encrypting small to medium-sized databases where quick encryption and decryption are necessary.

- **Systems with Limited Resources:** On systems where memory or CPU power is limited, Blowfish can be an effective choice due to its simplicity and lower resource requirements compared to AES.

The Twofish Cipher: Why Twofish

- **Flexible Key Size Requirements:** Twofish's support for key sizes of 128, 192, or 256 bits makes it versatile for different security needs, allowing for a balance between ***speed*** and **security**.

- **Software Implementations:** Twofish is efficient and can be a good choice for applications that require high security without the computational complexity of AES.

The AES Cipher: Overview

AES was developed to replace the Data Encryption Standard (DES) and to become the standard for a wide array of secure electronic data worldwide.

AES Specifications:

- **Input / Output Sizes:** AES processes data blocks of 128 bits.
- **Key Size:** Supports key sizes of 128, 192, or 256 bits.
- **Rounds:** 10, 12 or 14 rounds.

The AES Cipher: Pros And Cons

Pros:

- Highly secure, widely adopted, and tested.
- Efficient across different platforms and applications.

Cons:

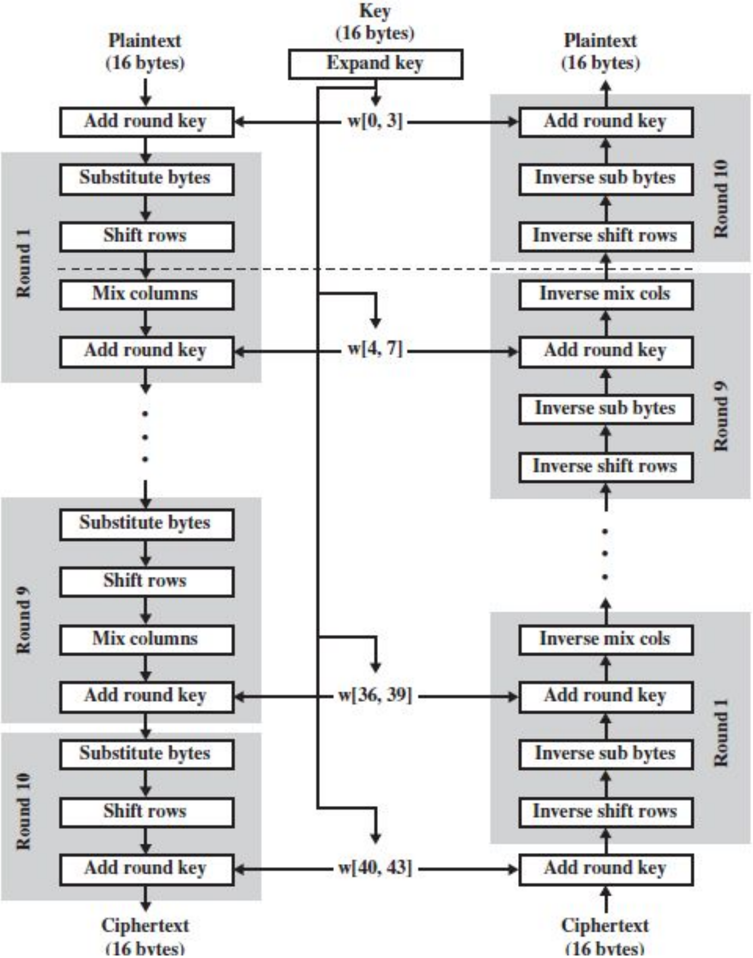
- Though very secure, theoretical attacks **(like side-channel attacks)** can exploit implementations, not the algorithm itself.

The AES Cipher: Structure

- Expand Key
- Add Round Key

A Round in AES:

1. Substitute Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key



The AES Cipher: Why AES

- **High Security Needs:** AES is often chosen for scenarios requiring the highest levels of security, such as government communications, financial transactions, and securing sensitive personal data.
- **Efficiency Across Platforms:** AES performs well on a wide variety of hardware and software, including small devices with limited processing power like smartphones and IoT devices.
- **Standardization Requirements:** AES, backed by National Institute of Standards and Technology (NIST), is the favored standard for organizations that prioritize strong data protection.

General Consideration

Choosing the right encryption method is crucial, balancing security with factors like speed, rules, and compatibility.

- **Security vs. Performance:** Some situations prioritize speed over maximum security, favoring algorithms like Blowfish or Twofish over AES, especially on older or slower systems.

- **Compliance and Industry Standards:** Certain industries have regulations specifying encryption standards, such as AES for financial data protection.

- **Data Size and Type:** The type and size of data being encrypted impact algorithm choice; some are better suited for certain data sizes or types.

Thank You

That’s all