SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA —AICTE and Accredited by NAAC —UGC with 'A+' Grade Approved by AICTE,
New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19EC4O2- WIRELESS ADHOC AND SENSOR NETWORKS

IV ECE/ VII SEMESTER

UNIT 5 —SECURITY ISSUES IN AD HOC / SENSOR NETWORKS

DES AND TRIPLE DES DETECTION SYSTEMS

What is DES?

- DES, which stands for Data Encryption Standard, is a symmetric key algorithm for encrypting and decrypting electronic data.
- It was developed by IBM in the 1970s and later adopted by the U.S. National Institute of Standards and Technology (NIST) as a federal standard in 1977.
- DES became widely used for securing sensitive information and communications.
- Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security.
- DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences.

DES - Key Features

- Symmetric Key Algorithm:

- DES is a symmetric key algorithm, meaning the same key is used for both encryption and decryption. The key length is 56 bits.

- Block Cipher:

- DES operates on fixed-size blocks of data, specifically 64-bit blocks. Each 64-bit block of plaintext is processed through a series of transformations to produce the corresponding ciphertext.

- Feistel Network Structure:

- DES uses a Feistel network structure, which involves splitting the input block into two halves and processing each half separately. The output from one half is combined with the other half to produce the final result.

- Key Generation:

The 56-bit key used in DES is typically chosen by the user. However, due to the key length and the algorithm's susceptibility to certain types of attacks, DES became vulnerable to brute-force attacks over time.

DES - Key Features

- Symmetric Key Algorithm:

- DES is a symmetric key algorithm, meaning the same key is used for both encryption and decryption. The key length is 56 bits.

- Block Cipher:

- DES operates on fixed-size blocks of data, specifically 64-bit blocks. Each 64-bit block of plaintext is processed through a series of transformations to produce the corresponding ciphertext.

- Feistel Network Structure:

- DES uses a Feistel network structure, which involves splitting the input block into two halves and processing each half separately. The output from one half is combined with the other half to produce the final result.

- Key Generation:

The 56-bit key used in DES is typically chosen by the user. However, due to the key length and the algorithm's susceptibility to certain types of attacks, DES became vulnerable to brute-force attacks over time.

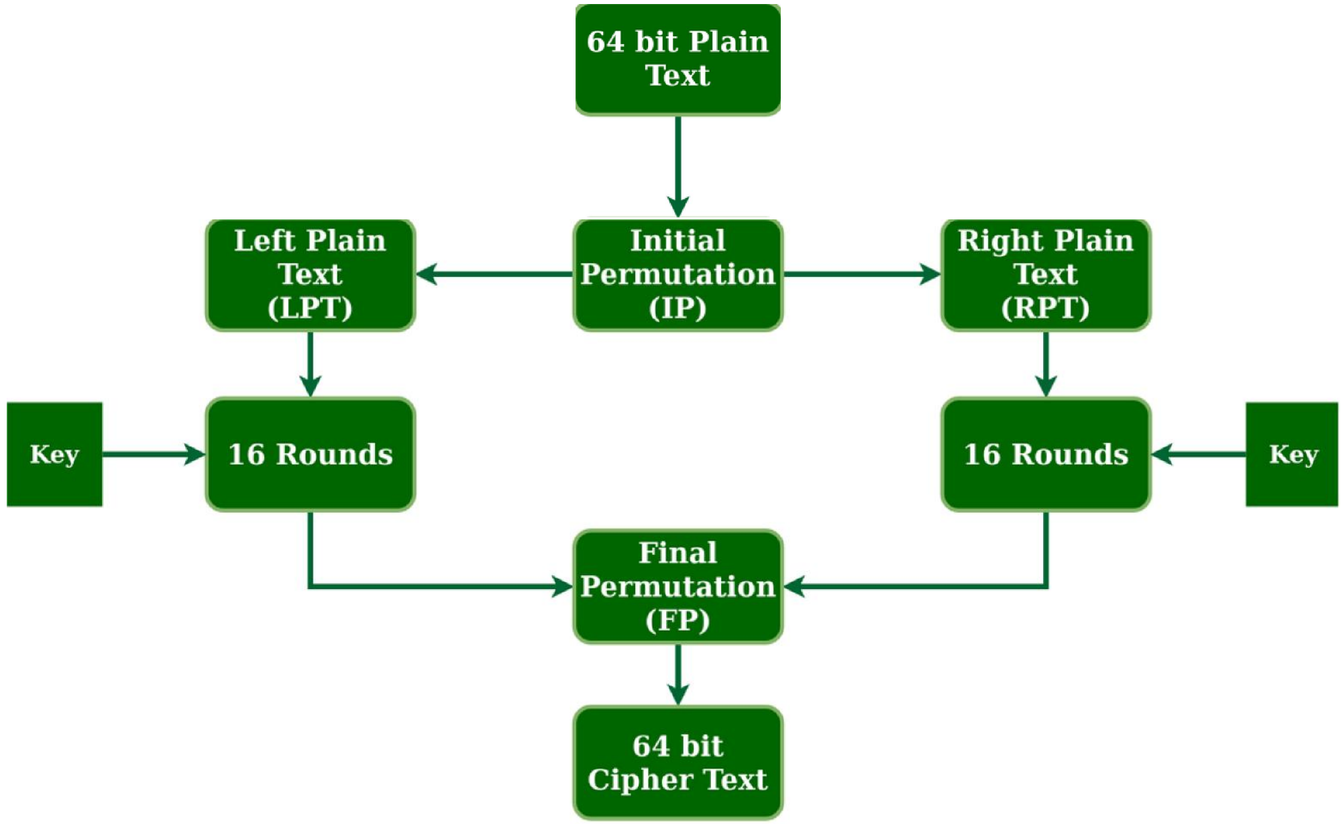
DES - Workin8

- The discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.
- DES is based on the two fundamental attributes of cryptography: substitution and transposition .
- DES consists of 16 steps, each of which is called a round.
- Each round performs the steps of substitution and transposition.

The overview of steps are as follows:

1. In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
2. The initial permutation is performed on plain text.
3. Next, the initial permutation (IP) produces two halves of the permuted block - Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now each LPT and RPT go through 16 rounds of the encryption process.
5. In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
6. The result of this process produces 64-bit ciphertext.

DES - Overview of Steps



Broad Level Steps in DES

DES - Encryption process

- Initial Permutation (IP):
  - The 64-bit plaintext block undergoes an initial permutation to rearrange its bits.
- Key Generation:
  - The 56-bit key is used to generate 16 subkeys, each 48 bits long, through a process known as key scheduling.
- Rounds of Encryption:

- DES consists of 16 rounds of encryption. In each round, the right half of the data is processed through a series of functions that involve the use of the subkeys.

- Feistel Network Operation:
  - The subkeys are mixed with the data during each round, adding complexity to the encryption process.
- Final Permutation (FP):
  - After the 16 rounds, a final permutation is applied to the data to produce the ciphertext.

DES - Security concerns

- Key Length:

- The relatively short key length of 56 bits makes DES susceptible to brute-force attacks. Advances in computing power rendered DES insecure over time.

- Cryptanalysis:

- Various cryptanalytic techniques, such as differential cryptanalysis, were developed to exploit weaknesses in the DES algorithm.

DES served as a standard for several decades, but its vulnerability to modern computing power led to its deprecation. In 2001, NIST recommended the use of more secure algorithms, particularly the Advanced Encryption Standard (AES), which became the successor to DES for secure data encryption.

DES - Security concerns

- Key Length:

- The relatively short key length of 56 bits makes DES susceptible to brute-force attacks. Advances in computing power rendered DES insecure over time.

- Cryptanalysis:

- Various cryptanalytic techniques, such as differential cryptanalysis, were developed to exploit weaknesses in the DES algorithm.

DES served as a standard for several decades, but its vulnerability to modern computing power led to its deprecation. In 2001, NIST recommended the use of more secure algorithms, particularly the Advanced Encryption Standard (AES), which became the successor to DES for secure data encryption.

Triple DES Detection Systems

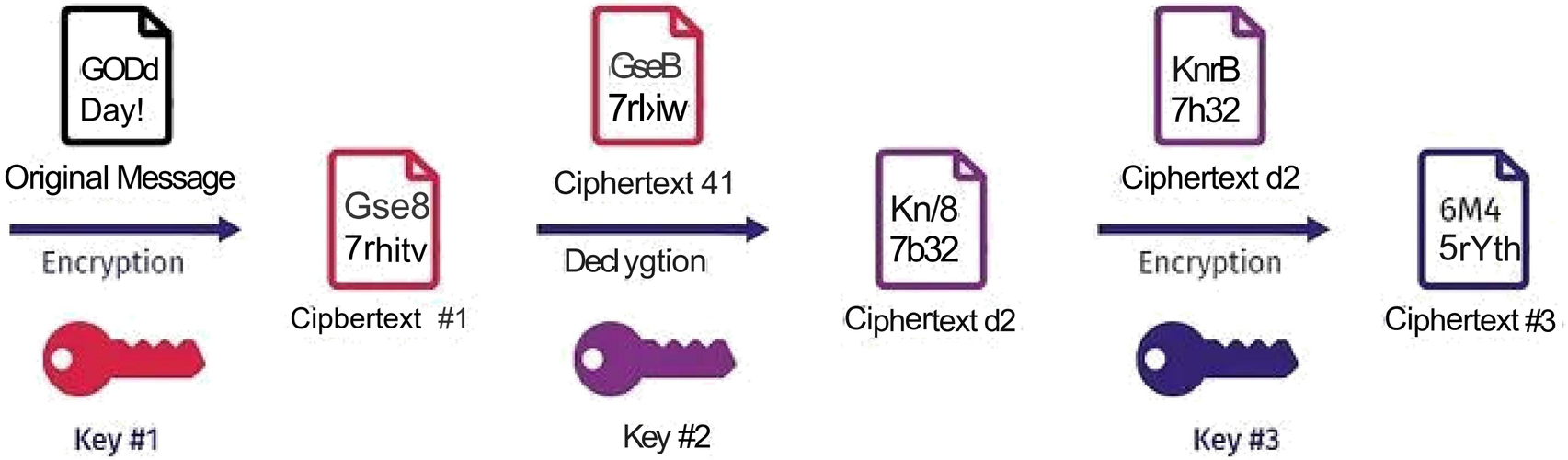
- Triple DES (3DES) is a modified version of the Data Encryption Standard (DES) algorithm that was developed by IBM in the 1970s.
- DES was widely used in the 1980s and 1990s, but its 56-bit key size was deemed insufficient for modern security needs.
- As a result, in the late 1990s, the National Institute of Standards and Technology (NIST) started a project to find a new encryption standard that would be more secure than DES.
- Detection systems for Triple DES (3DES) are designed to identify the use or presence of the Triple DES encryption algorithm in network traffic or systems.
- Triple DES is an enhancement of the original Data Encryption Standard (DES) and involves applying the DES algorithm three times in sequence, using either two or three different keys.

Triple DES - Key Features

- Block Cipher Encryption:
  - 3DES is a block cipher encryption algorithm that operates on 64-bit blocks of plaintext at a time.
- Symmetric Key Encryption:
  - 3DES uses a symmetric key encryption system, meaning that the same key is used for both encryption and decryption.
- Triple Layer Encryption:
  - 3DES uses three different keys to encrypt the plaintext three times, hence the name Triple DES.
- Variable Key Size:
  - 3DES supports variable key sizes, ranging from 128 to 192 bits, offering enhanced security compared to DES.

Triple DES - Working

How Triple DES (TDEA)Works



Triple DES - Encryption and Decryption

Encryption Process:

- Initial Permutation:

  - The 64-bit plaintext is subjected to an initial permutation.

- Three Rounds of Encryption:

  - The plaintext is encrypted three times, each time using a different key, to create three layers of encryption.

- Final Permutation:

  - After the three rounds of encryption, a final permutation is applied to the output to produce the ciphertext.

Decryption Process:

- The decryption process of 3DES is simply the reverse of the encryption process, with the ciphertext being fed into the algorithm and the steps being performed in reverse order, using the three keys in reverse order.

Triple DES - Advantages

- Advantages:
- Enhanced Security:

  - The triple-layered encryption technique of 3DES provides enhanced security compared to DES.

- Compatible:

  - 3DES is backward compatible with DES, which means that it can be used in legacy systems that still use DES.

- Customizable Key Sizes:

  - 3DES supports variable key sizes, which makes it more adaptable to different security needs.

- Limitations:
- Slow Speed:

  - The triple-layered encryption process of 3DES makes it slower than other encryption algorithms.

- Limited Key Size Options:

  While 3DES supports variable key sizes, the maximum key size is only 192 bits.

References

- https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/?ref=lbp
- https://cyberw1ng.medium.com/triple-des-3des-encryption-features-process-advantages-and-applications-2023-587e5a092789