**AMRUTHESH**

**241059041**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**Introduction**

The Data Encryption Standard (DES) was developed in the 1970s by IBM and later adopted as a federal standard by the National Institute of Standards and Technology (NIST). Despite its historical importance, DES is now considered obsolete due to its vulnerabilities.

**1. DES Algorithm Overview**

**Structure:**

* **Key Size:** 56 bits
* **Block Size:** 64 bits
* **Rounds:** 16

**Mechanism:**

1. **Initial Permutation (IP):** The plaintext is permuted according to a fixed table.
2. **Round Function:** DES uses 16 rounds of encryption, where each round applies a series of transformations including substitution, permutation, and XOR operations with a subkey.
3. **Final Permutation (FP):** The result of the 16 rounds is permuted to produce the ciphertext.

**Key Generation:**

* **Subkeys:** The 56-bit key is divided into 16 subkeys, each 48 bits long, used in the 16 rounds of encryption.

**2. Limitations of DES**

**Key Size:**

* **Brute-Force Attacks:** The 56-bit key size is relatively small by modern standards. Advances in computational power have made it feasible to perform a brute-force attack, where all possible keys are tested to decrypt the ciphertext. In 1998, the Electronic Frontier Foundation demonstrated the feasibility of such attacks using dedicated hardware.

**Cryptographic Strength:**

* **Weaknesses:** DES’s block size of 64 bits is also considered inadequate for modern security requirements. The limited block size makes it vulnerable to certain attacks like birthday attacks, where the probability of two blocks of data having the same encryption pattern increases with the amount of data processed.

**Technological Advancements:**

* **Computational Power:** As hardware capabilities advanced, the time required to crack DES through brute-force attacks decreased significantly. DES's security was compromised as the cost of performing such attacks became cheaper and more accessible.

**3. Transition to AES**

Due to the vulnerabilities of DES, it was eventually replaced by the Advanced Encryption Standard (AES) in 2001. AES, with key sizes of 128, 192, or 256 bits and a block size of 128 bits, provides much stronger security and is resistant to brute-force attacks.

**Conclusion**

While DES played a significant role in the history of cryptography, its limitations in key size and block size led to its replacement by more secure algorithms like AES. Understanding DES’s weaknesses highlights the importance of adapting cryptographic standards to evolving technological landscapes.