SNS COLLEGE OF ENGINEERING
Kurumbapalayam (Po), Coimbatore – 641 107
AN AUTONOMOUS INSTITUTION
Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IOT & CS INCLUDING BCT)

Block cipher modes of operation

RC4 (Rivest Cipher 4) is one of the most well-known stream ciphers, developed by Ron Rivest in 1987. It is widely used for encrypting data in a way that each byte of plaintext is combined with a corresponding byte of a keystream to produce the ciphertext.

Key Characteristics of RC4:

1. **Stream Cipher**: RC4 operates on data one byte at a time (as opposed to block ciphers, which operate on fixed-size blocks of data). The keystream is generated dynamically based on an initial key and is XORed with the plaintext to produce the ciphertext.
2. **Simplicity**: The RC4 algorithm is known for its simplicity and speed in both hardware and software implementations. It uses a variable-length key (typically between 40 and 2048 bits), which is a major factor in its widespread use in protocols like SSL/TLS and WEP (Wi-Fi encryption).
3. **Keystream Generation**: RC4 generates a pseudo-random keystream of bytes using a key scheduling algorithm (KSA) and a pseudo-random generation algorithm (PRGA). These steps are as follows:
    - **Key Scheduling Algorithm (KSA)**: The key, which is a sequence of bytes, initializes the state of a permutation array of size 256 (called S). This array is then shuffled based on the key.
    - **Pseudo-Random Generation Algorithm (PRGA)**: The state array is used to generate the keystream. Each byte of the keystream is produced by selecting a value from the shuffled array, then updating the state array for the next value.
4. **Encryption/Decryption**: The encryption of plaintext with RC4 is simply XORing the plaintext with the keystream byte by byte. The same operation can be used for decryption as well, since XOR is a symmetric operation.
    - **Encryption**: Ciphertext = Plaintext XOR Keystream
    - **Decryption**: Plaintext = Ciphertext XOR Keystream

Security Considerations:

RC4 was widely used for many years, but it has been found to have multiple vulnerabilities, and its use in modern cryptography is discouraged:

1. **Weaknesses in the Keystream**: Early bytes of the RC4 keystream are biased and can leak information about the key. This makes RC4 vulnerable to various attacks, especially if the same key is reused.
2. **RC4 in SSL/TLS**: RC4 was used in older versions of SSL/TLS, but due to its weaknesses, it has been deprecated in favor of more secure algorithms like AES.
3. **Flaw in WEP**: RC4 was used in WEP (Wired Equivalent Privacy) for Wi-Fi security, but due to key reuse and poor initialization vecto