Listen

Stream and Block Ciphers

Module Three investigates two broad classes of ciphers: stream ciphers and block ciphers.

Stream Ciphers

A stream cipher is a cipher algorithm in which the plaintext is encoded one symbol at a time and then transmitted. One method of implementing a stream cipher is to generate an apparently random sequence of 1s and 0s and then use that sequence to encode each letter. The key to encrypting and decrypting the message is to know how the random-looking sequence is generated. One way of generating such a random-looking sequence is to use a feedback shift register. A feedback shift register is a function that generates a sequence of 1s and 0s; typically, they are easy to implement as electronic circuits. Feedback shift registers can be linear if the underlying function is linear, but they are otherwise nonlinear.

One specific stream cipher studied in this module is RC4, which stands for "Rivest Cipher 4," a symmetric stream cipher designed by Ron Rivest in 1987. It's a widely used encryption algorithm known for its simplicity and speed. RC4 operates by generating a pseudorandom stream of bits, which is then XORed with the plaintext to produce ciphertext. The key setup involves initializing a permutation of 256 bytes based on the secret key, and the keystream is generated from this permutation. While RC4 is known for its speed and efficiency in software implementations, vulnerabilities have been discovered in RC4 over the years, and it's no longer considered secure for modern cryptographic purposes.

Block Ciphers

A block cipher encodes a block of data, usually 5 or 10 letters or pieces of data at a time, and then transmits the entire coded block. One specific block encryption scheme studied in this module is the Hill cipher. The Hill cipher is a symmetric block cipher used for encryption. The encryption algorithm operates on blocks of plaintext (usually pairs of letters) and uses a matrix-based approach for encryption and decryption. The encryption key is a square matrix, and the plaintext is divided into blocks, which are then multiplied by the key matrix to produce the ciphertext. Decryption involves multiplying the ciphertext by the inverse of the key matrix to recover the original plaintext.

While the Hill cipher is relatively straightforward to understand, it is vulnerable to attacks when the key matrix is not carefully chosen. As such, it is not widely used in modern cryptographic applications and has been replaced by more secure block ciphers like AES (Advanced Encryption Standard), which will be studied in later modules.

To adapt block ciphers for various cryptographic applications, different operation modes are commonly used. For example, in the Electronic Codebook (ECB) mode, each plaintext block is encrypted independently with the same key. This means that identical plaintext blocks result in

identical ciphertext blocks. As such, this mode may not be suitable for encrypting large amounts of data due to its vulnerability to patterns in the plaintext. Other common modes such as Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) have other benefits/tradeoffs that will be examined.