



The diagram illustrates a cryptographic system, likely a stream cipher, showing the flow of data through various components. The system is divided into two main sections: Encryption and Decryption.

Encryption Section:

- Plaintext:** The input data to be encrypted.
- Key Stream:** A sequence of pseudo-random bits generated from a **Key** and a **Pseudo-Random Number Generator (PRNG)**.
- Encryption Process:** The Plaintext is combined with the Key Stream using a logical operation (likely XOR) to produce the **Ciphertext**.

Decryption Section:

- Ciphertext:** The encrypted data received.
- Key Stream:** The same sequence of pseudo-random bits generated from the same **Key** and **PRNG** as used in encryption.
- Decryption Process:** The Ciphertext is combined with the Key Stream using the same logical operation (likely XOR) to recover the original **Plaintext**.

The diagram also shows the internal structure of the PRNG, which includes a **Shift Register** and a **Feedback Function** that generates the pseudo-random key stream.

$$H \quad (\quad)$$

0 0000000000 _____ 000000000000
0 0 000000000000000000 00
0
0 0 0000000000 _____ 000000000000
0 000