CPA Secure Encryption

Input: A key of length seed_size, an initialization vector of length seed_size, a message of arbitrary length.

Output: Cipher text

Algorithm:

Encryption in this use case is performed in output feedback mode.

The message of arbitrary length is divided into blocks of seed_size.

Each cipher is computed with the help of PRF(key,r) and the message block.

The cipher block is the xor operation of the above two results.

The initialization vector is updated and is used for the encryption of next message block, thus making it output feedback mode.

Returns original IV || cipher text

Decryption is same as encryption with message being the cipher text and initialization vector being the prefix of cipher text of length seed_size.