Scribe: Cryptography and Network Security (Class.29)

Rohit(17CS30028)

22-Oct-2020

1 Output Feedback Mode

The main advantage of the OFB method is that bit errors in transmission do not propagate in the encryption.

For example, if as a bit error occurs in C1 as ciphertext, only the recovered value of P1 as plaintext is affected; subsequent plaintext units are not corrupted. With CFB, C1 as ciphertext also serves as input to the shift register and therefore causes additional corruption downstream in this mode.

The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than is CFB in the modes of operation.

2 Modern modes proposed for AES

IEPM
CCM
EAX
GCM
OCB

3 Authenticated Encryption With Associated Data (AEAD)

AEAD is a variant of AE that allows a recipient to check the integrity of both the encrypted and unencrypted information in a message. AEAD binds associated data (AD) to the ciphertext and to the context where it is supposed to appear so that attempts to ”cut-and-paste” a valid ciphertext into a different context are detected and rejected.It is required, for example, by network packets or frames where the header needs visibility, the payload needs confidentiality, and both need integrity and authenticity.

4 Merkel Puzzle Description

Bob generates 2^n messages containing, "This is message X. This is the symmetrical key Y", where X is a randomly generated identifier, and Y is a randomly generated secret key meant for symmetrical encryption. Hence, both X and Y are unique to each message. All the messages are encrypted in a way such that a user may conduct a brute force attack on each message with some difficulty. Bob sends all the encrypted messages to Alice.

Alice receives all the encrypted messages, and randomly chooses a single message to brute force. After Alice discovers both the identifier X and the secret key Y inside that message, she encrypts her clear text with the secret key Y, and sends that identifier (in cleartext) with her cipher text to Bob.

Bob looks up the secret key paired with that identifier, since he's the one who generated them in the first place, and deciphers Alice's cipher text with that secret key.