Computer Security Assignment 2

Venkatesh Viswanathan - vviswana - 50290589

21st September 2018

1 Expression for Encryption and Decryption Modes

1.1 Expression for Encryption and Decryption Modes in CFB mode

CFB mode is the Cipher FeedBack mode.

Expression for CFB mode encryption of a stream cipher

$I_i = LSB(IV_{i-1}||C_{i-1})$
$X_i = E(K, I_i)$
$C_i = m_i \oplus S_r(X_i)$
$C_i = m_i \oplus S_r(E(K, I_i))$
$C_i = m_i \oplus S_r(E(K, LSB(IV_{i-1}||C_{i-1})))$

The above are the equations for CFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
m -Message
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

Expression for CFB mode decryption of a stream cipher

$I_i = LSB(IV_{i-1}||P_{i-1})$
$X_i = E(K, I_i)$
$P_i = C_i \oplus S_r(X_i)$
$P_i = C_i \oplus S_r(E(K, I_i))$
$P_i = C_i \oplus S_r(E(K, LSB(IV_{i-1}||P_{i-1})))$

The above are the equations for CFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
P_i - Plain Text
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

1.2 Expression for Encryption and Decryption Modes in OFB mode

OFB mode is the Output FeedBack mode.

Expression for OFB mode encryption of a stream cipher

$I_i = LSB(IV_{i-1}||S_r(X_{i-1}))$
$X_i = E(K, I_i)$
$C_i = m_i \oplus S_r(X_i)$
$C_i = m_i \oplus S_r(E(K, I_i))$
$C_i = m_i \oplus S_r(E(K, LSB(IV_{i-1}||S_r(X_{i-1}))))$

The above are the equations for OFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
m 0.9cm-Message
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

Expression for OFB mode decryption of a stream cipher

$I_i = LSB(IV_{i-1}||S_r(X_{i-1}))$
$X_i = E(K, I_i)$
$P_i = C_i \oplus S_r(X_i)$
$P_i = C_i \oplus S_r(E(K, I_i))$
$P_i = C_i \oplus S_r(E(K, LSB(IV_{i-1}||S_r(X_{i-1}))))$