Exam Topics

1) Hill Cipher
2) ADFGVX
3) DES
4) AES
Block Cipher Modes

1. Easiest/Most Natural: Electronic Codebook Mode (the one not to use in practice)

\[ P = P_0, P_1, P_2, \ldots, P_{m-1} \]  
Split into blocks of the appropriate size

\[ C = E_k(P_0) \cdot E_k(P_1) \cdot E_k(P_2) \cdots E_k(P_{m-1}) \]

weakness: if \( P_i = P_j \) then \( C_i = C_j \)

strength: Can be parallelized!

2. Cipher Block Chaining

\[ C_1 = E_k(P_1 \oplus IV) \]

\[ C_{i+1} = E_k(P_{i+1} \oplus C_i) \]

Strength: Same plaintext blocks not encrypted into same ciphertext blocks

weakness: Can’t be parallelized

\( IV \) = known to sender + receiver, not known to outsider.
Figure 7.5  s-bit Cipher Feedback (CFB) Mode

We can define CFB mode as follows.

<table>
<thead>
<tr>
<th>CFB</th>
<th>( I_i = IV )</th>
<th>( I_i = IV )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( I_j = \text{LSB}<em>{b-s}((I</em>{j-1}) | C_{j-1}) ) ( j = 2, \ldots, N )</td>
<td>( I_j = \text{LSB}<em>{b-s}((I</em>{j-1}) | C_{j-1}) ) ( j = 2, \ldots, N )</td>
<td></td>
</tr>
<tr>
<td>( O_j = E(K, I_j) ) ( j = 1, \ldots, N )</td>
<td>( O_j = E(K, I_j) ) ( j = 1, \ldots, N )</td>
<td></td>
</tr>
<tr>
<td>( C_j = P_j \oplus \text{MSB}_s(O_j) ) ( j = 1, \ldots, N )</td>
<td>( P_j = C_j \oplus \text{MSB}_s(O_j) ) ( j = 1, \ldots, N )</td>
<td></td>
</tr>
</tbody>
</table>

Although CFB can be viewed as a stream cipher, it does not conform to the typical construction of a stream cipher. In a typical stream cipher, the cipher takes
Output Feedback Mode

\[ O_i = E_k(\text{Nonce}), \quad O_{i+1} = E_k(O_i) \]

\[ C_i = P_i \oplus O_i, \quad P_i = C_i \oplus O_i \]

Nonce means that for each message, the IV changes!

Counter Mode

\[ O_i = E_k(\text{Counter}_i) \]

Counter\_i is a pre-generated sequence.

Most common "counter" is simply to start at some number and add 1 each time \( \mod 2^b \). (\( b = \text{block size} \))

\[ C_i = P_i \oplus O_i \]