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)

$P = P_0 P_1 P_2 \dots P_{m-1}$] split into m 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

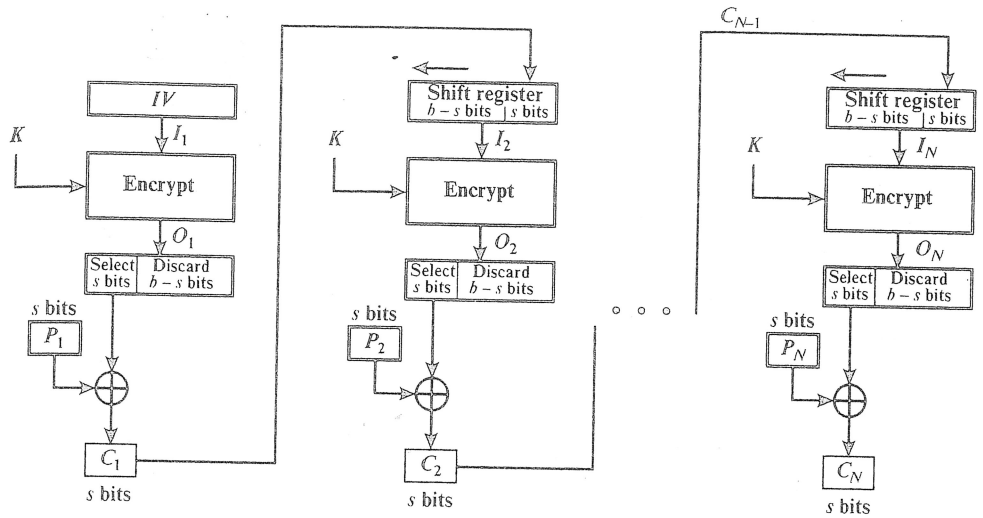
weakness: Can't be parallelized

IV = known to sender + receiver, not known to outsider.

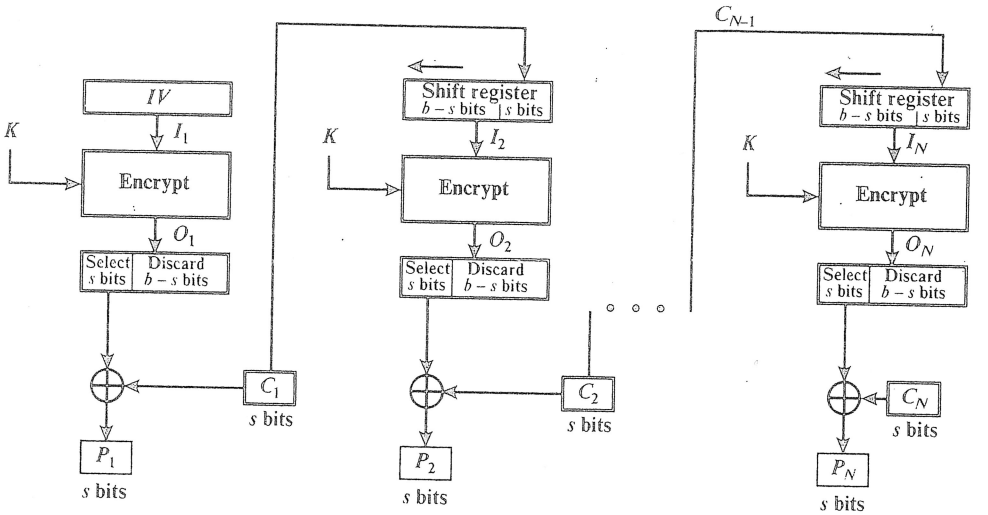
10/11/19 (3)

(3) Cipher Feedback Mode

Will scan in picture!



(a) Encryption



(b) Decryption

Figure 7.5 s-bit Cipher Feedback (CFB) Mode

We can define CFB mode as follows.

CFB	$I_1 = IV$			$I_1 = IV$	
	$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$	$j = 2, \ldots, N$		$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$	$j = 2, \ldots, N$
	$O_j = \text{E}(K, I_j)$	$j = 1, \ldots, N$		$O_j = \text{E}(K, I_j)$	$j = 1, \ldots, N$
	$C_j = P_j \oplus \text{MSB}_s(O_j)$	$j = 1, \ldots, N$		$P_j = C_j \oplus \text{MSB}_s(O_j)$	$j = 1, \ldots, N$

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

④ Output Feedback Mode

$$O_1 = E_K(\text{Nonce}), \quad O_{i+1} = E_K(O_i)$$

$$C_i = P_i \oplus O_i, \quad P_i = C_i \oplus O_i$$

Nonce means that for each message, the IV changes!

⑤ 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 = blocksize)

$$C_i = P_i \oplus O_i$$