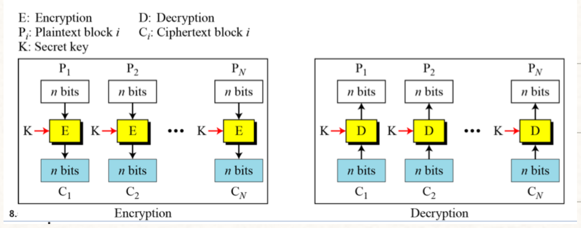
Chapter 8

Mode of Operation

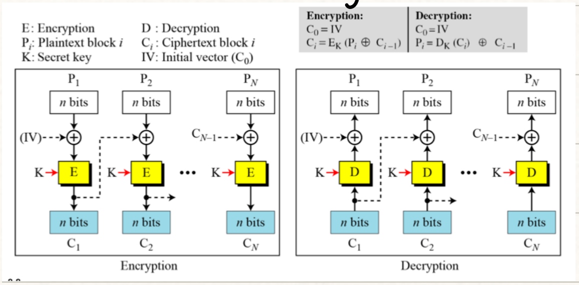
ECB Electronic CodeBook Mode

E : $C_i = E_K(P_i)$ D : $P_i = D_K(C_i)$



E: Encryption D: Decryption
P_i: Plaintext block i C_i: Ciphertext block i
K: Secret key

CBC Cipher Block Chaining Mode



E: Encryption D : Decryption
P_i: Plaintext block i C_i : Ciphertext block i
K: Secret key IV: Initial vector (C_0)

Encryption:	**Decryption:**
$C_0 = IV$	$C_0 = IV$
$C_i = E_K(P_i \oplus C_{i-1})$	$P_i = D_K(C_i) \oplus C_{i-1}$

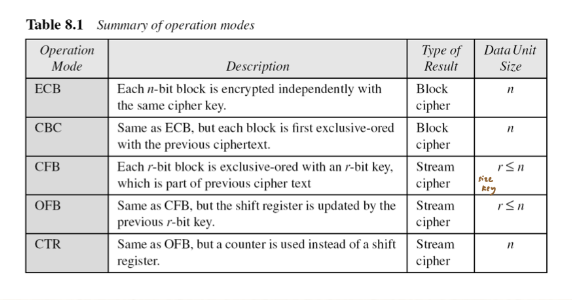
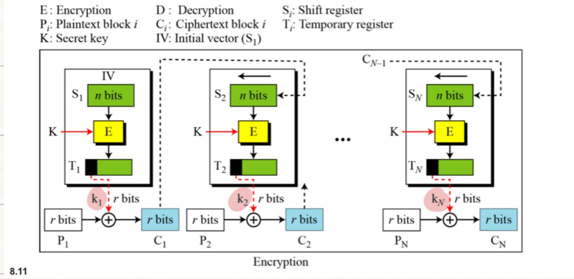


Table 8.1 *Summary of operation modes*

Operation Mode	*Description*	*Type of Result*	*Data Unit Size*
ECB	Each n-bit block is encrypted independently with the same cipher key.	Block cipher	n
CBC	Same as ECB, but each block is first exclusive-ored with the previous ciphertext.	Block cipher	n
CFB	Each r-bit block is exclusive-ored with an r-bit key, which is part of previous cipher text	Stream cipher	$r \leq n$ size key
OFB	Same as CFB, but the shift register is updated by the previous r-bit key.	Stream cipher	$r \leq n$
CTR	Same as OFB, but a counter is used instead of a shift register.	Stream cipher	n

Stream cipher

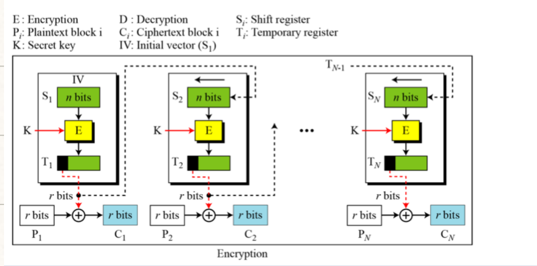
CFB Cipher Feedback Mode



E : Encryption D : Decryption S_i: Shift register
P_i: Plaintext block i C_i: Ciphertext block i T_i: Temporary register
K: Secret key IV: Initial vector (S_1)

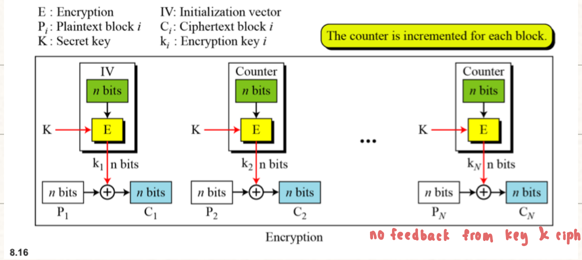
Encryption: $C_i = P_i \oplus \text{SelectLeft}_r\{E_K[\text{ShiftLeft}_r(S_{i-1}) \mid C_{i-1})]\}$
Decryption: $P_i = C_i \oplus \text{SelectLeft}_r\{E_K[\text{ShiftLeft}_r(S_{i-1}) \mid C_{i-1})]\}$

OFB Output Feedback Mode



E : Encryption D : Decryption S_i: Shift register
P_i: Plaintext block i C_i: Ciphertext block i T_i: Temporary register
K: Secret key IV: Initial vector (S_1)

CTR Counter Mode



E : Encryption IV: Initialization vector
P_i : Plaintext block i C_i: Ciphertext block i
K : Secret key k_i : Encryption key i

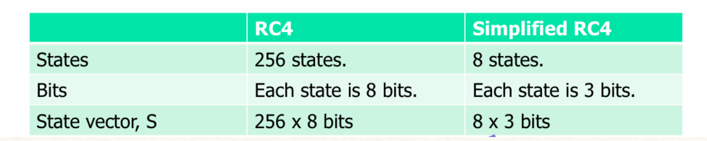
The counter is incremented for each block.

no feedback from key & cipher

Use of Stream Cipher

RC4

- byte oriented
- 8 bits p XoR c
- state : 2^{bit}



	RC4	Simplified RC4
States	256 states.	8 states.
Bits	Each state is 8 bits.	Each state is 3 bits.
State vector, S	256 x 8 bits	8 x 3 bits

Example

(Given)

4×3 bit key

k: [1 2 3 6]

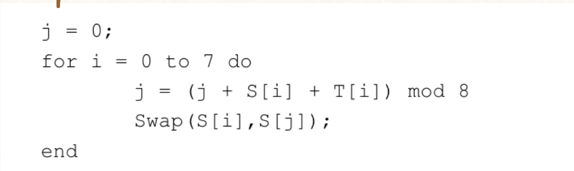
p: [1 2 2 2]

Step 1

s: [0 1 2 3 4 5 6 7] state

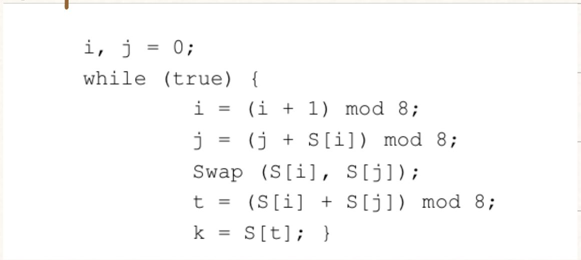
T: [1 2 3 6 1 2 3 6] k

Step 2



```
j = 0;
for i = 0 to 7 do
        j = (j + S[i] + T[i]) mod 8
        Swap(S[i],S[j]);
end
```

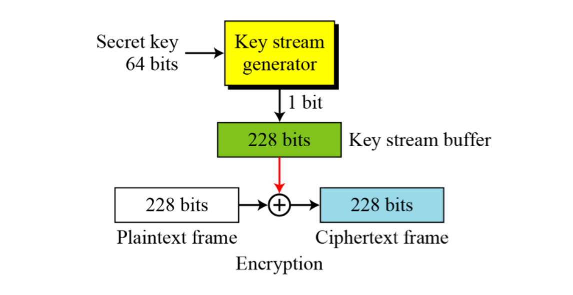
Step 3



```
i, j = 0;
while (true) {
        i = (i + 1) mod 8;
        j = (j + S[i]) mod 8;
        Swap (S[i], S[j]);
        t = (S[i] + S[j]) mod 8;
        k = S[t]; }
```

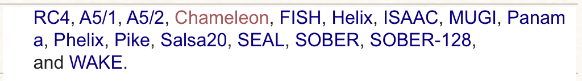
A5/1

- Global System for Comm (GSM) mobile telephone



Stream Cipher Usage

- wireless connection
- ChaCha



RC4, A5/1, A5/2, Chameleon, FISH, Helix, ISAAC, MUGI, Panama, Phelix, Pike, Salsa20, SEAL, SOBER, SOBER-128, and WAKE.

Key Management

- n(n-1)/2 keys, n entities

Key Generation

- diff symmetric key cipher need diff key size
(pseudorandom)
- random number generator