

# ECE 646 - Lecture 8

## Extensions of DES

### Modes of operation of block ciphers

1

---

---

---

---

## Extending the Life of DES

2

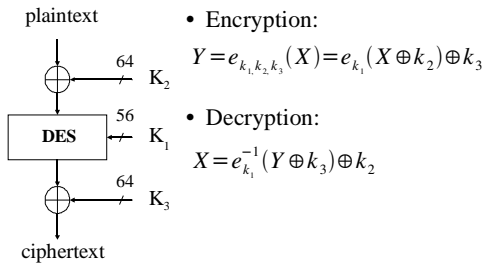
---

---

---

---

### Key Whitening



3

---

---

---

---

## DESX

*Rivest, 1988*

- Uses Key Whitening with:
  - Key =  $(K_1, K_2)$
  - $K_3$  = hash function  $(K_1, K_2)$
  - Total Key Length 120 bits
- Caution: Key Whitening protects against exhaustive key search, but not against differential and linear cryptanalysis

4

---

---

---

---

## Multiple Encryption

5

---

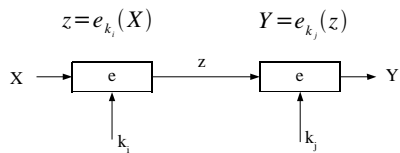
---

---

---

## Double Encryption

- Keyspace is  $|k| = 2^k \cdot 2^k = 2^{2k}$



6

---

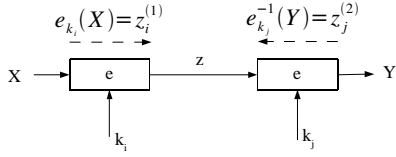
---

---

---

## Meet in the Middle Attack

- Keyspace is  $|k|=2^k \cdot 2^k = 2^{2k}$



---

---

---

---

---

## Meet in the Middle Attack

- Input: some pairs  $(x', y')$ ,  $(x'', y'')$ , ...
- Idea: compute  $z_i^{(1)} = e_{k_i}(x')$  and  $z_j^{(2)} = e_{k_j}^{-1}(y')$
- Problem: find matching pair  $z_i^{(1)} = z_j^{(2)}$

---

---

---

---

---

## Procedure

- Compute look-up table for all  $(z_i^{(1)}, k_i)$ ,  $i=1,2,\dots,2^k$
- Find matching  $z_j^{(2)}$ 
  - a) compute  $e_{k_j}^{-1}(y') = z_j^{(2)}$
  - b) if  $z_j^{(2)}$  is in look-up table then  $z_i^{(1)} = z_j^{(2)}$ , check a few other pairs for this  $k_i$  and  $k_j$
  - c) if  $k_i$  and  $k_j$  are fine, stop, otherwise go back to a)

---

---

---

---

---

## Meet in the Middle Attack

Q: How many additional pairs  
(x'', y''), (x''', y'''),... should we test?

10

---

---

---

---

- Possible key combinations:  $2^{2 \cdot 56}$
- Possible values for x' and y':  $2^{64}$
- Hence, possible mappings:  $E(x') = y'$ :

$$\frac{2^{2 \cdot 56}}{26} \cdot 64 = \frac{2^{112}}{2^{64}} = 2^{48}$$

- Use candidate key and check  $E(x'') = y''$ 
  - $2^n$  possible mappings
  - likelihood  $E(x'') = y''$  for random key  $1/2^{64}$

11

---

---

---

---

- Check third pair (x''', y''') using same  
“random” key as before
  - likelihood that  $E(x'') = y''$  and  $E(x''') = y'''$  is

$$\frac{1}{2^{64}} \cdot \frac{1}{2^{64}} = \frac{1}{2^{2 \cdot 64}} = \frac{1}{2^{128}}$$

- If we check t-1 additional pairs
  - likelihood that random key fulfills all  $E(x'')=y''$ ...

$$\frac{1}{2^{(t-1)64}}$$

12

---

---

---

---

- If “random” key is a candidate key
  - likelihood at least one fulfills all  $E(x^i)=y^i$ ... is

$$\frac{1}{2^{(t-1)64}} \cdot \frac{2^{2 \cdot 56}}{2^{64}} = 2^{2 \cdot 56 - t \cdot 64}$$

- Computational Complexity
  - Brute force:  $2^{2 \cdot 56} = 2^{112}$
  - Meet in the middle:  $2^{56}$  encryptions  
 $2^{56}$  decryptions  
 $= 2^{57}$  computations  
 and  $2^{56}$  memory locations

---



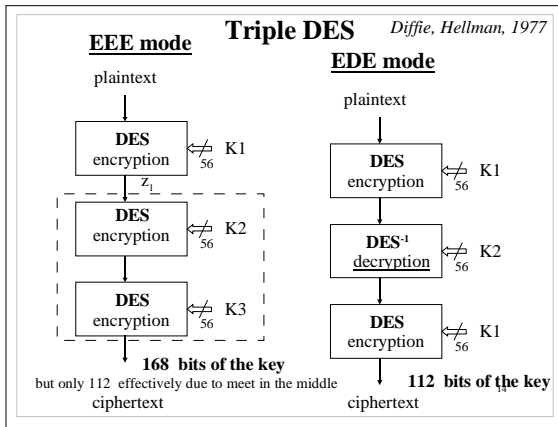
---



---



---




---



---



---



---

### Triple DES

**Advantages:**

- secure key length (112)
- increased compared to DES resistance to linear and differential cryptanalysis
- possibility of utilizing existing implementations of DES

**Disadvantages:**

- relatively slow, especially in software

---



---



---



---

## Modes of operation of secret-key block ciphers

16

---



---

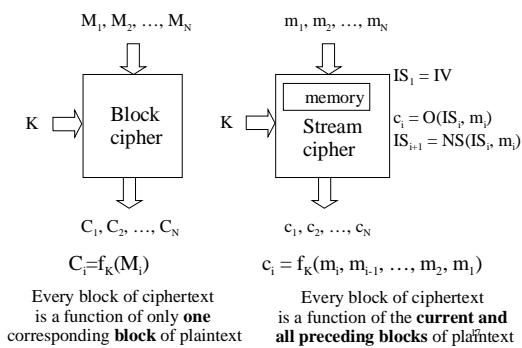


---



---

### Block vs. stream ciphers




---



---

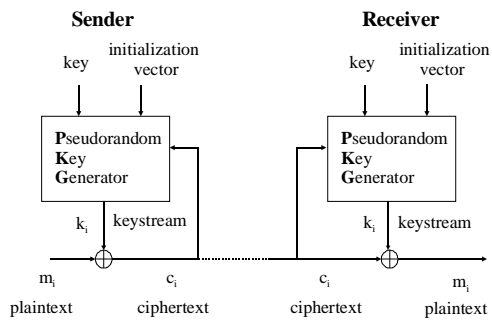


---



---

### Typical stream cipher




---



---



---



---

18

### Standard modes of operation of block ciphers

#### Block ciphers

ECB mode

#### Stream ciphers

Counter mode  
OFB mode  
CFB mode  
CBC mode

19

---

---

---

---

### ECB (Electronic CodeBook) mode

20

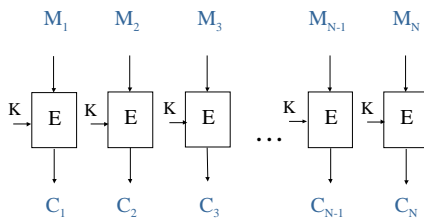
---

---

---

---

### Electronic CodeBook Mode - ECB



$$C_i = E_K(M_i) \quad \text{for } i=1..N$$

21

---

---

---

---

## Counter Mode

22

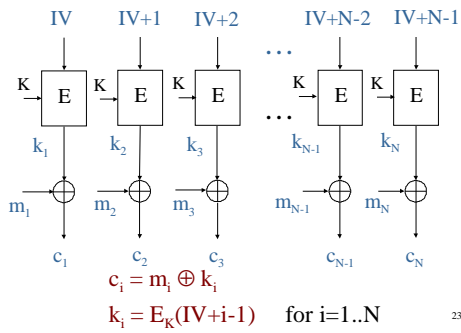
---

---

---

---

### Counter Mode - CTR Encryption



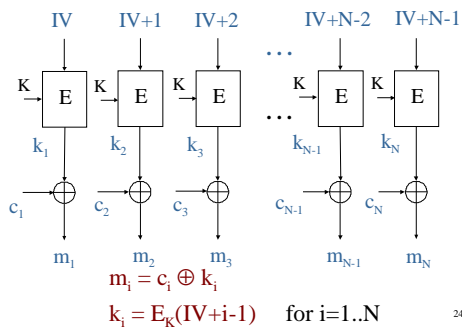
---

---

---

---

### Counter Mode - CTR Decryption

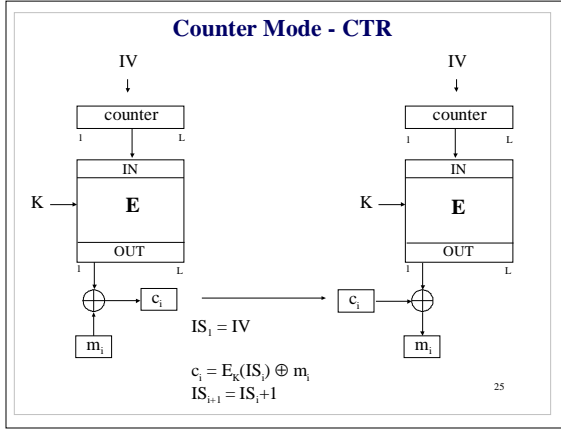


---

---

---

---




---

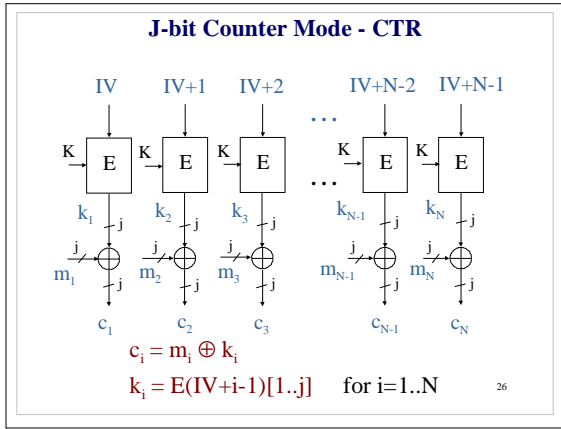
---

---

---

---

---




---

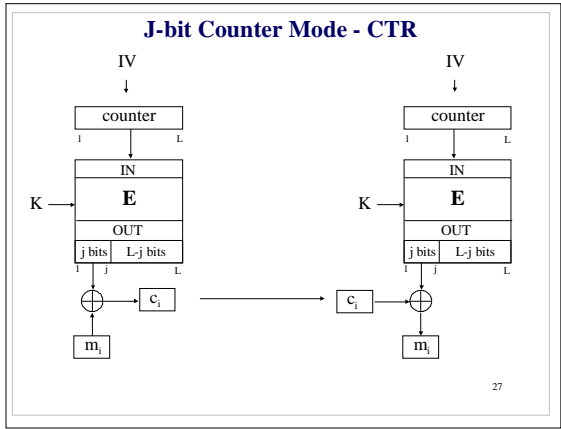
---

---

---

---

---




---

---

---

---

---

---

## OFB (Output FeedBack) Mode

28

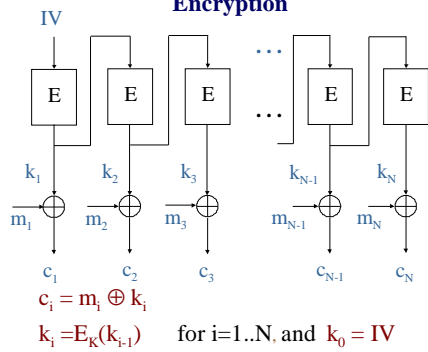
---

---

---

---

### Output Feedback Mode - OFB Encryption



29

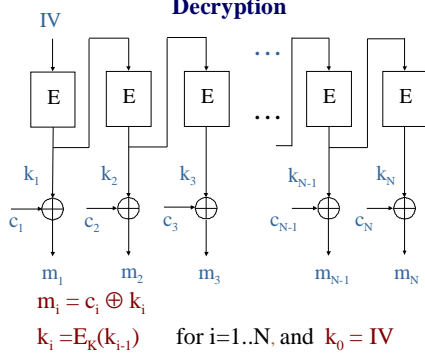
---

---

---

---

### Output Feedback Mode - OFB Decryption



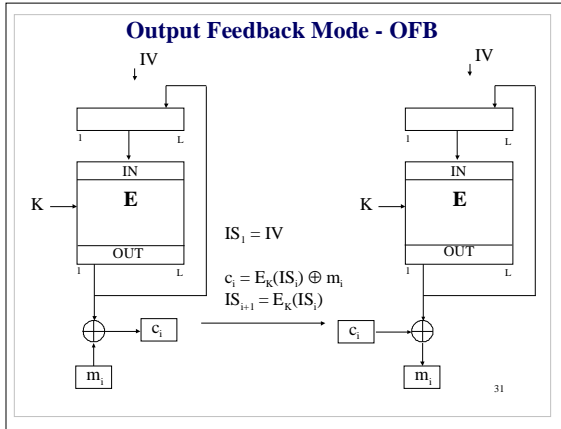
30

---

---

---

---




---



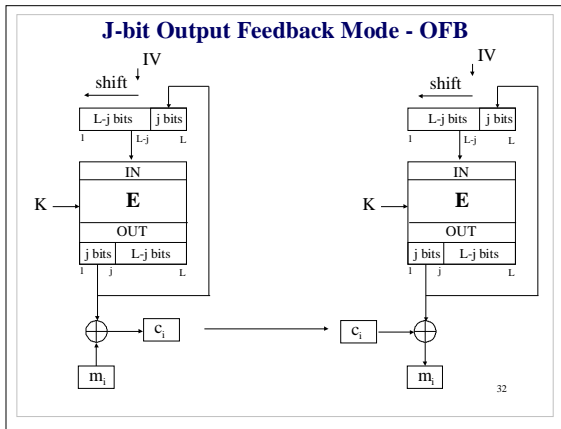
---



---



---




---



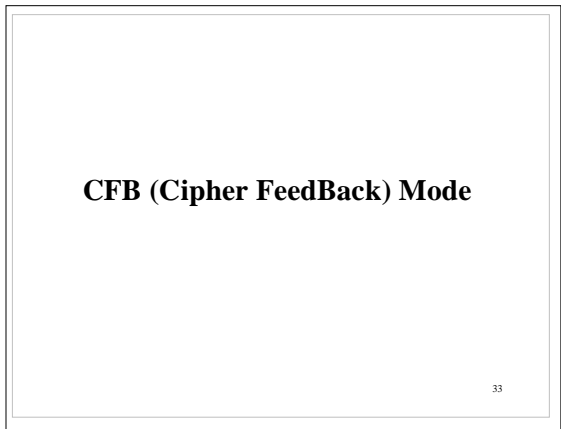
---



---



---




---



---

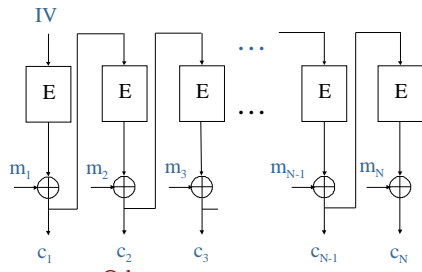


---



---

**Cipher Feedback Mode - CFB  
Encryption**



$$c_i = m_i \oplus k_i$$

$$k_i = E_K(c_{i-1}) \quad \text{for } i=1..N, \text{ and } c_0 = IV$$

34

---



---

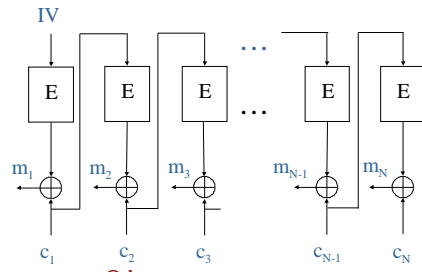


---



---

**Cipher Feedback Mode - CFB  
Decryption**



$$c_i = m_i \oplus k_i$$

$$k_i = E_K(c_{i-1}) \quad \text{for } i=1..N, \text{ and } c_0 = IV$$

35

---



---

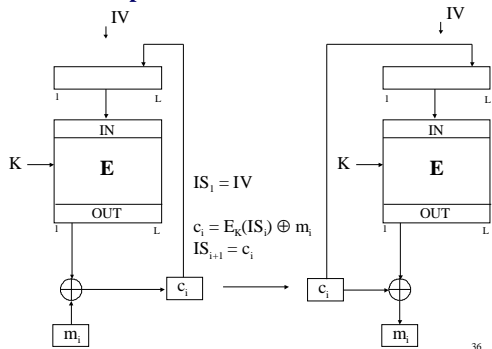


---



---

**Cipher Feedback Mode - CFB**



36

---



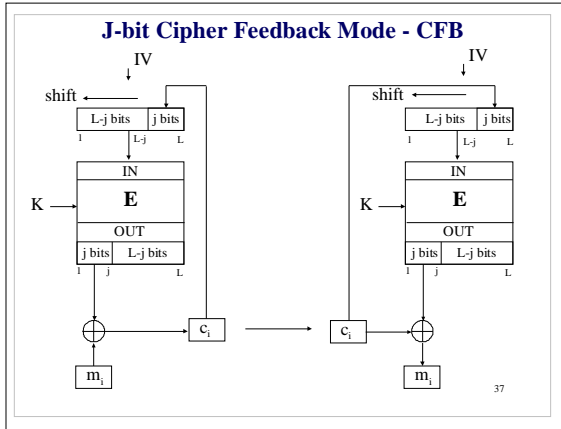
---



---



---




---



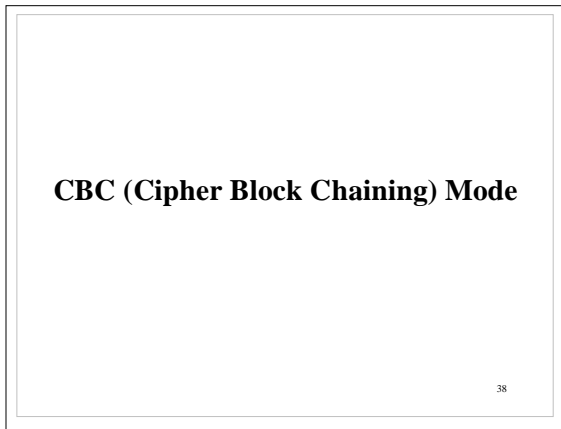
---



---



---




---



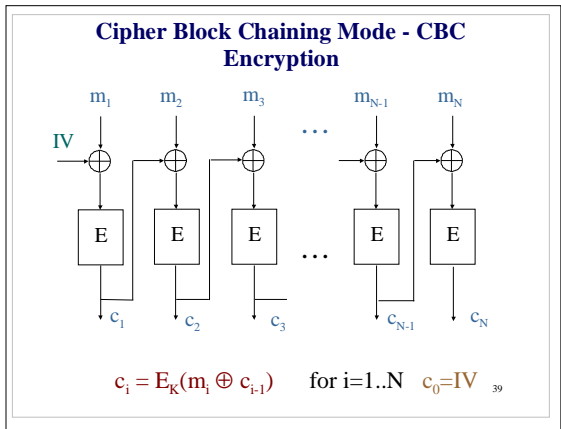
---



---



---




---



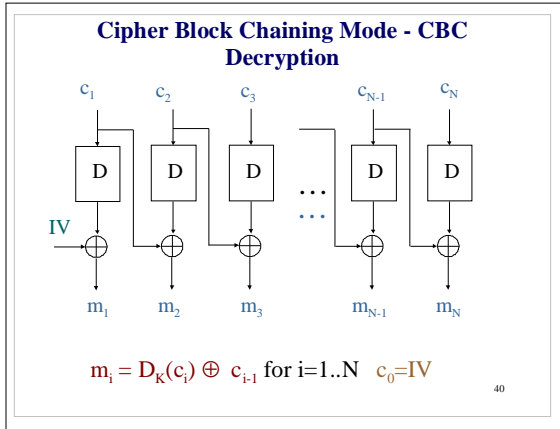
---



---



---




---



---



---



---

### Comparison among various modes

41

---



---



---



---

### Block Cipher Modes of Operation Basic Features (1)

	ECB	CTR	OFB	CFB	CBC
<b>Security</b>	weak	strong	strong	strong	strong
<b>Basic speed</b>	$s_{ECB}$	$\approx s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx s_{ECB}$
<b>Capability for parallel processing and pipelining</b>	Encryption and decryption	Encryption and decryption	None	Decryption only	Decryption only
<b>Cipher operations</b>	Encryption and decryption	Encryption only	Encryption only	Encryption only	Encryption and decryption
<b>Preprocessing</b>	No	Yes	Yes	No	No
<b>Random access</b>	R/W	R/W	No	R only	R only

42

---



---



---



---

### Block Cipher Modes of Operation Basic Features (2)

	ECB	CTR	OFB	CFB	CBC
<b>Security against the exhaustive key search attack</b>					
<b>Minimum number of the message and ciphertext blocks needed</b>	1 plaintext block, 1 ciphertext block	2 plaintext blocks, 2 ciphertext blocks	2 plaintext blocks, 2 ciphertext blocks (for $j=L$ )	1 plaintext blocks, 2 ciphertext blocks (for $j=L$ )	1 plaintext blocks, 2 ciphertext blocks
<b>Error propagation in the decrypted message</b>					
<b>Modification of j-bits</b>	L bits	j bits	j bits	L+j bits	L+j bits
<b>Deletion of j bits</b>	Current and all subsequent	Current and all subsequent	Current and all subsequent	L bits	Current and all subsequent
<b>Integrity</b>	No	No	No	No	No <sub>43</sub>

---

---

---

---

---

---

---

---

### New modes of operation

---

---

---

---

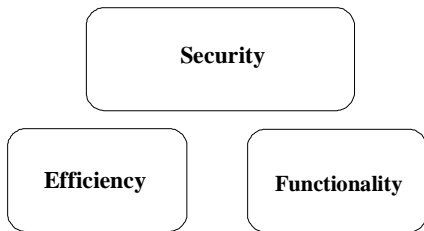
---

---

---

---

### Evaluation Criteria for Modes of Operation




---

---

---

---

---

---

---

---

### Evaluation criteria (1)

#### Security

- resistance to attacks
- **proof of security**
- random properties of the ciphertext

#### Efficiency

- number of calls of the block cipher
- **capability for parallel processing**
- memory/area requirements
- initialization time
- **capability for preprocessing**

46

---

---

---

---

### Evaluation criteria (2)

#### Functionality

- **security services**
  - confidentiality, **integrity, authentication**
- flexibility
  - variable lengths of blocks and keys
  - different amount of precomputations
  - requirements on the length of the message
- **vulnerability to implementation errors**
- requirements on the amount of keys, initialization vectors, random numbers, etc.
- error propagation and the capability for resynchronization
- patent restrictions

47

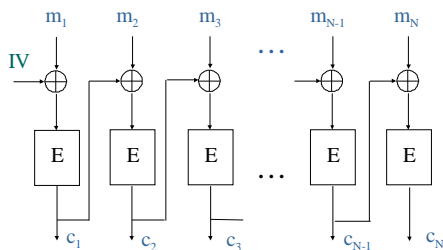
---

---

---

---

### CBC



#### Problems:

- **No parallel processing of blocks from the same packet**
- **No speed-up by preprocessing**
- **No integrity or authentication**

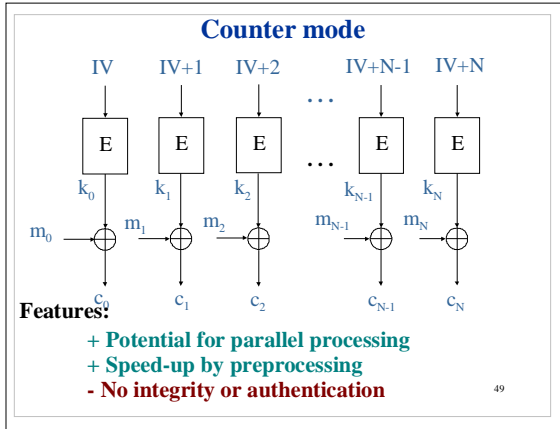
48

---

---

---

---




---



---



---



---

### Properties of existing and new cipher modes

	CBC	CFB	OFB	New standard
Proof of security	✓	✓	✓	✓
Parallel processing	decryption only		-	✓
Preprocessing	-	-	✓	✓
Integrity and authentication	-	-	-	✓
Resistance to implementation errors	✓	✓	-	✓ <small>50</small>

---



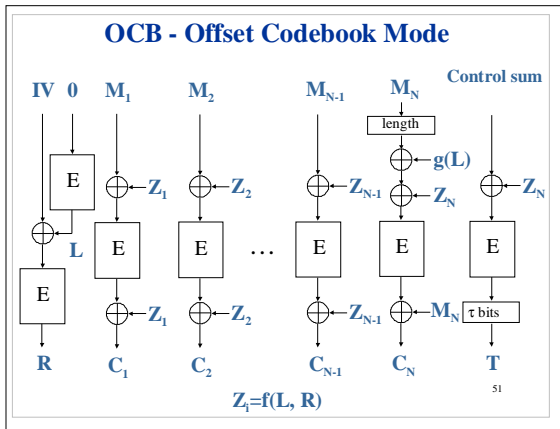
---



---



---




---



---



---



---