ECE 646 – Lecture 9

Modes of Operation of Block Ciphers

1

Required Reading

- W. Stallings, *Cryptography and Network Security*,

  Chapter 7 Block Cipher Operation (Sections 7.2-7.6)

- A. Menezes et al., *Handbook of Applied Cryptography*,

  Chapter 7.2.2 Modes of operation

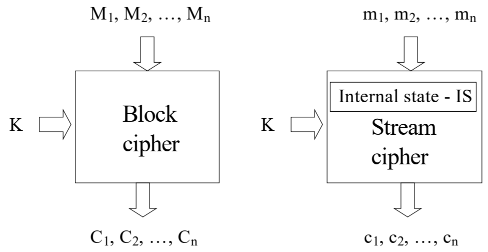
2

Recommended Reading

- NIST SP 800-38A
  Recommendation for Block Cipher Modes of Operation:
  Methods and Techniques,
  available at
  https://csrc.nist.gov/publications/detail/sp/800-38a/final

3

Block vs. stream ciphers



$C_i=f_K(M_i)$

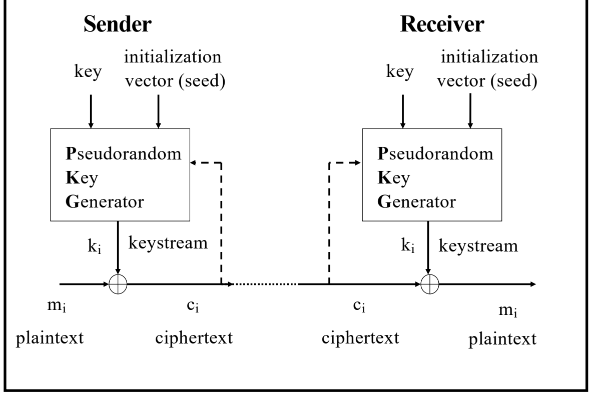
$c_i = f_K(m_i, IS_i)$ $IS_{i+1}=g_K(m_i, IS_i)$

Every block of ciphertext is a function of only **one** corresponding **block** of plaintext

Every block of ciphertext is a function of the **current block** of plaintext and the current **internal state** of the cipher

4

Typical stream cipher


Sender
Receiver
key
initialization vector (seed)
Pseudorandom Key Generator
k_i
keystream
m_i
c_i
plaintext
ciphertext
key
initialization vector (seed)
Pseudorandom Key Generator
k_i
keystream
c_i
m_i
ciphertext
plaintext

5

Standard modes of operation of block ciphers

Block ciphers	**Stream ciphers**
ECB mode	**Counter mode** **OFB mode** **CFB mode** **CBC mode**

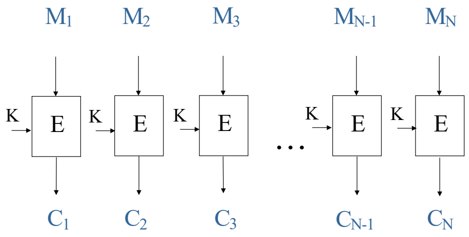
6

ECB (Electronic CodeBook) mode

7

Electronic CodeBook Mode – ECB

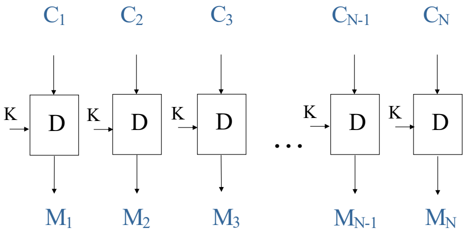
Encryption



$C_i = E_K(M_i)$ for i=1..N

8

Electronic CodeBook Mode – ECB
Decryption



$M_i = E_K(C_i)$ for i=1..N

9

Criteria for Comparison of Modes of Operation

- hiding repeating message blocks
- speed
- capability for parallel processing and pipelining during encryption / decryption
- use of block cipher operations (encryption only or both)
- capability for preprocessing during encryption / decryption
- capability for random access for the purpose of reading / writing
- number of plaintext and ciphertext blocks required for exhaustive key search
- error propagation in the message after modifying / deleting one block / byte / bit of the corresponding ciphertext

10

Block Cipher Modes of Operation
Basic Features (1)

	ECB	CTR	OFB	CFB	CBC
Hiding repeating plaintext blocks	No				
Basic speed	s_{ECB}				
Capability for parallel processing and pipelining	Encryption and decryption				
Cipher operations	Encryption and decryption				
Preprocessing	No				
Random access	R/W				

11

Block Cipher Modes of Operation
Basic Features (2)

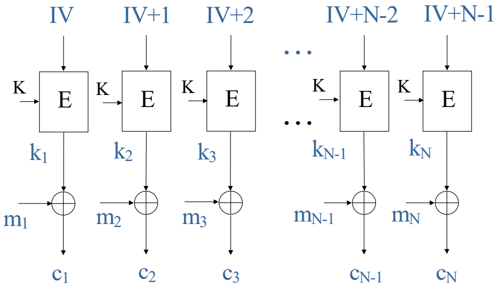
	ECB	CTR	OFB	CFB	CBC
Security against the exhaustive key search attack					
Minimum number of the message and ciphertext blocks needed	1 plaintext block, 1 ciphertext block				
Error propagation in the decrypted message					
Modification of j-bits	L bits				
Deletion of j bits	Current and all subsequent				
Integrity	No				

12

Counter Mode

13

Counter Mode - CTR
Encryption

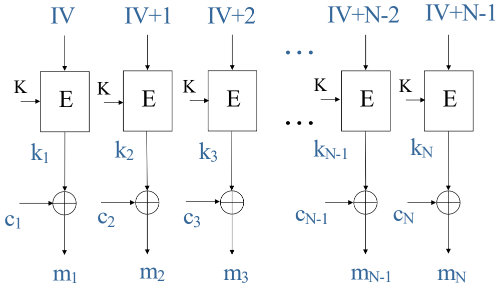


$c_i = m_i \oplus k_i$

$k_i = E_K(IV+i-1)$ for i=1..N

14

Counter Mode - CTR
Decryption

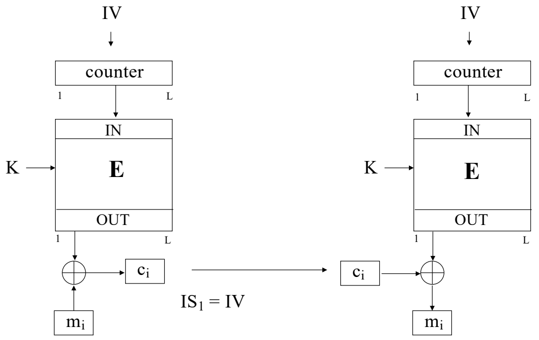


$m_i = c_i \oplus k_i$

$k_i = E_K(IV+i-1)$ for i=1..N

15

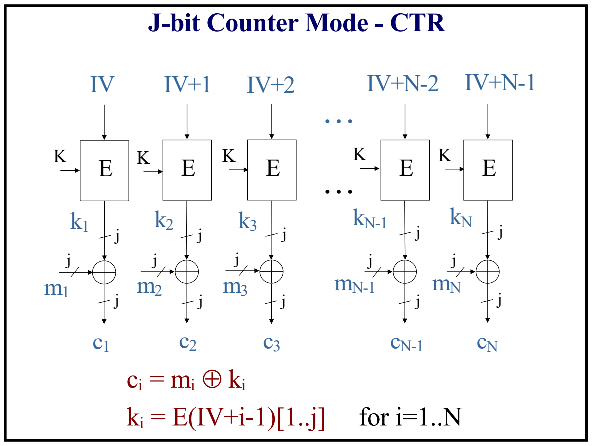
Counter Mode - CTR



$IS_1 = IV$

$c_i = E_K(IS_i) \oplus m_i$
$IS_{i+1} = IS_i+1$

16

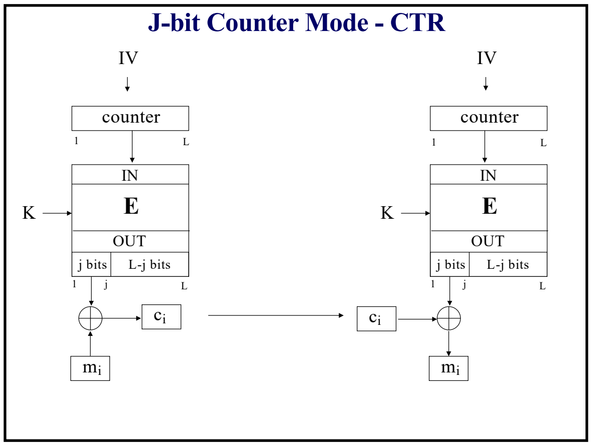


J-bit Counter Mode - CTR

$c_i = m_i \oplus k_i$

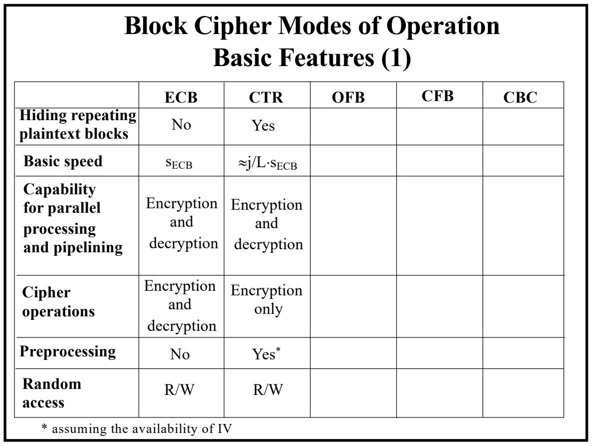
$k_i = E(IV+i-1)[1..j]$ for i=1..N

17



J-bit Counter Mode - CTR

18

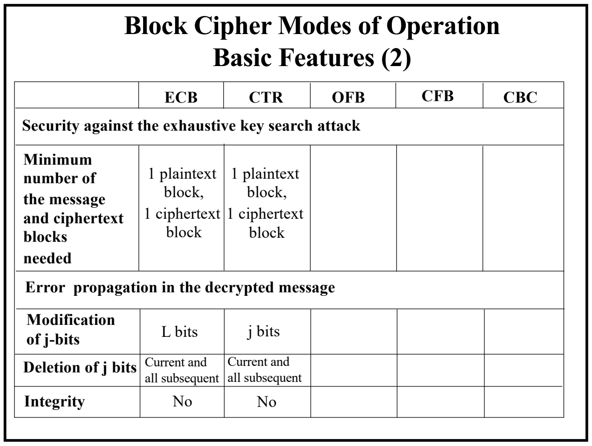


Block Cipher Modes of Operation Basic Features (1)

	ECB	CTR	OFB	CFB	CBC
Hiding repeating plaintext blocks	No	Yes			
Basic speed	s_{ECB}	$\approx j/L \cdot s_{ECB}$			
Capability for parallel processing and pipelining	Encryption and decryption	Encryption and decryption			
Cipher operations	Encryption and decryption	Encryption only			
Preprocessing	No	Yes*			
Random access	R/W	R/W			

* assuming the availability of IV

19



Block Cipher Modes of Operation Basic Features (2)

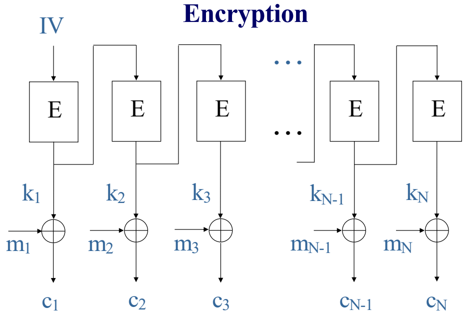
	ECB	CTR	OFB	CFB	CBC
Security against the exhaustive key search attack					
Minimum number of the message and ciphertext blocks needed	1 plaintext block, 1 ciphertext block	1 plaintext block, 1 ciphertext block			
Error propagation in the decrypted message					
Modification of j-bits	L bits	j bits			
Deletion of j bits	Current and all subsequent	Current and all subsequent			
Integrity	No	No			

20

OFB (Output FeedBack) Mode

21

Output Feedback Mode - OFB Encryption

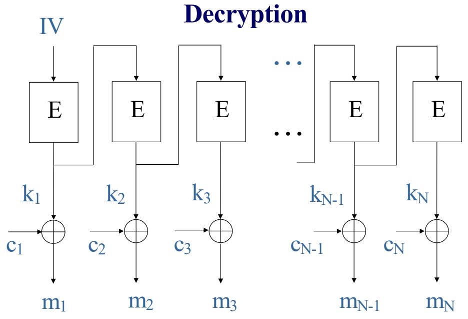


$c_i = m_i \oplus k_i$

$k_i = E_K(k_{i-1})$ for i=1..N, and $k_0 = IV$

22

Output Feedback Mode - OFB Decryption

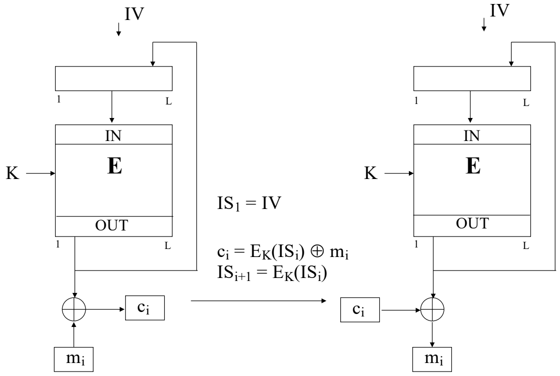


$m_i = c_i \oplus k_i$

$k_i = E_K(k_{i-1})$ for i=1..N, and $k_0 = IV$

23

Output Feedback Mode - OFB



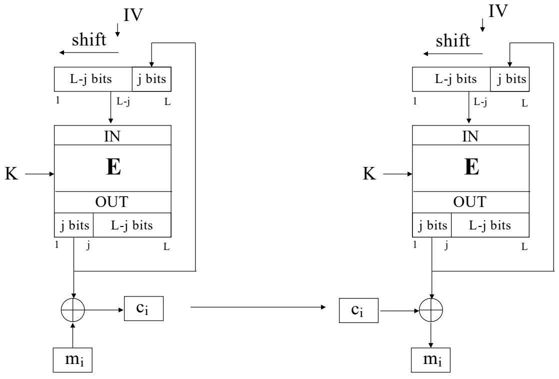
$IS_1 = IV$

$c_i = E_K(IS_i) \oplus m_i$

$IS_{i+1} = E_K(IS_i)$

24

J-bit Output Feedback Mode - OFB



25

Block Cipher Modes of Operation
Basic Features (1)

	ECB	CTR	OFB	CFB	CBC
Hiding repeating plaintext blocks	No	Yes	Yes		
Basic speed	s_{ECB}	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$		
Capability for parallel processing and pipelining	Encryption and decryption	Encryption and decryption	None		
Cipher operations	Encryption and decryption	Encryption only	Encryption only		
Preprocessing	No	Yes*	Yes*		
Random access	R/W	R/W	No		

* assuming the availability of IV

26

Block Cipher Modes of Operation
Basic Features (2)

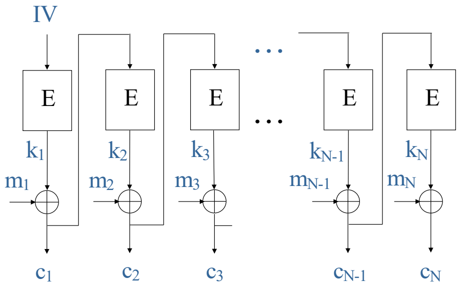
	ECB	CTR	OFB	CFB	CBC
Security against the exhaustive key search attack					
Minimum number of the message and ciphertext blocks needed	1 plaintext block, 1 ciphertext block	1 plaintext block, 1 ciphertext block	2 plaintext blocks, 2 ciphertext blocks (for j=L)		
Error propagation in the decrypted message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

27

CFB (Cipher FeedBack) Mode

28

Cipher Feedback Mode - CFB
Encryption

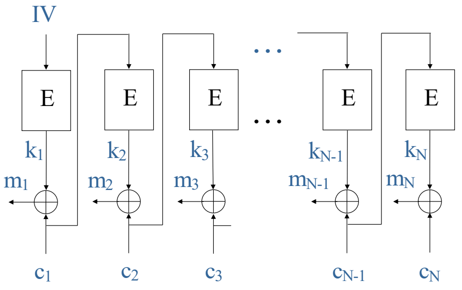


$c_i = m_i \oplus k_i$

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

29

Cipher Feedback Mode - CFB
Decryption

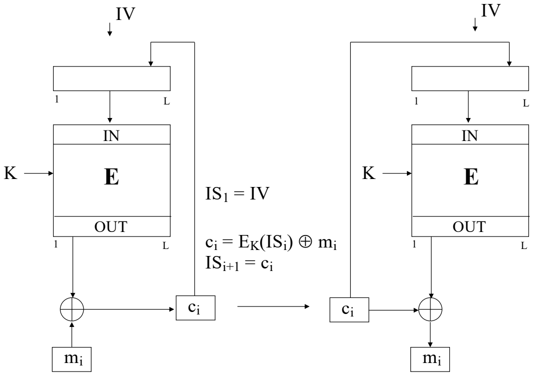


$m_i = c_i \oplus k_i$

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

30

Cipher Feedback Mode - CFB



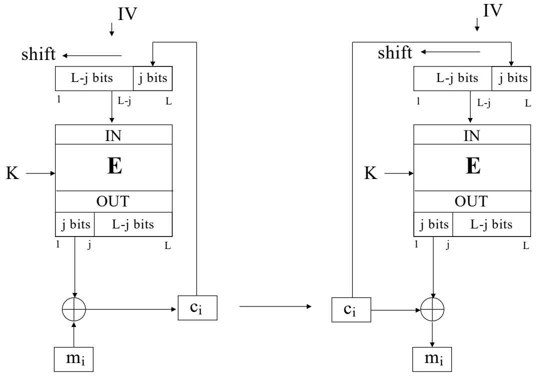
$IS_1 = IV$

$c_i = E_K(IS_i) \oplus m_i$

$IS_{i+1} = c_i$

31

J-bit Cipher Feedback Mode - CFB



32

Block Cipher Modes of Operation Basic Features (1)

	ECB	CTR	OFB	CFB	CBC
Hiding repeating plaintext blocks	No	Yes	Yes	Yes	
Basic speed	s_{ECB}	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	
Capability for parallel processing and pipelining	Encryption and decryption	Encryption and decryption	None	Decryption only	
Cipher operations	Encryption and decryption	Encryption only	Encryption only	Encryption only	
Preprocessing	No	Yes*	Yes*	No	
Random access	R/W	R/W	No	R only	

* assuming the availability of IV

33

Block Cipher Modes of Operation Basic Features (2)

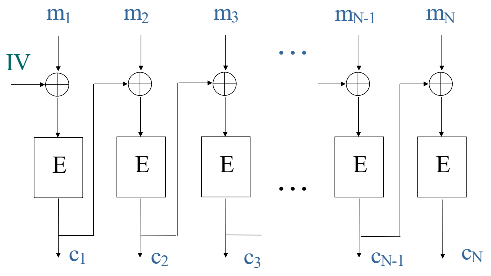
	ECB	CTR	OFB	CFB	CBC
Security against the exhaustive key search attack					
Minimum number of the message and ciphertext blocks needed	1 plaintext block, 1 ciphertext block	1 plaintext block, 1 ciphertext block	2 plaintext blocks, 2 ciphertext blocks (for j=L)	1 plaintext block, 2 ciphertext blocks (for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

34

CBC (Cipher Block Chaining) Mode

35

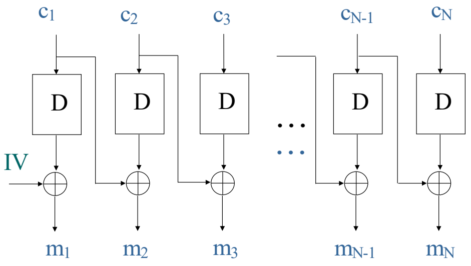
Cipher Block Chaining Mode - CBC Encryption



$c_i = E_K(m_i \oplus c_{i-1})$ for i=1..N c_0=IV

36

Cipher Block Chaining Mode - CBC Decryption



$m_i = D_K(c_i) \oplus c_{i-1}$ for $i=1..N$ $c_0=IV$

37

Block Cipher Modes of Operation Basic Features (1)

	ECB	CTR	OFB	CFB	CBC
Hiding repeating plaintext blocks	No	Yes	Yes	Yes	Yes
Basic speed	s_{ECB}	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx s_{ECB}$
Capability for parallel processing and pipelining	Encryption and decryption	Encryption and decryption	None	Decryption only	Decryption only
Cipher operations	Encryption and decryption	Encryption only	Encryption only	Encryption only	Encryption and decryption
Preprocessing	No	Yes*	Yes*	No	No
Random access	R/W	R/W	No	R only	R only

* assuming the availability of IV

38

Block Cipher Modes of Operation Basic Features (2)

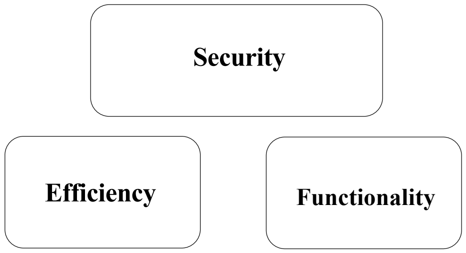
	ECB	CTR	OFB	CFB	CBC
Security against the exhaustive key search attack					
Minimum number of the message and ciphertext blocks needed	1 plaintext block, 1 ciphertext block	1 plaintext block, 1 ciphertext block	2 plaintext blocks, 2 ciphertext blocks (for j=L)	1 plaintext block, 2 ciphertext blocks (for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

39

New modes of operation

40

Evaluation Criteria for Modes of Operation



41

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**

42

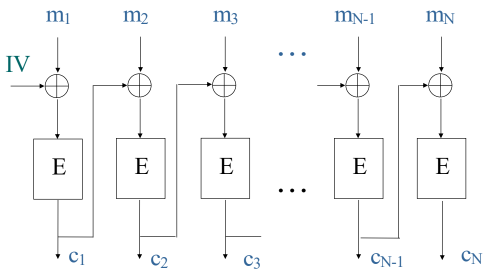
Evaluation criteria (2)

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

43

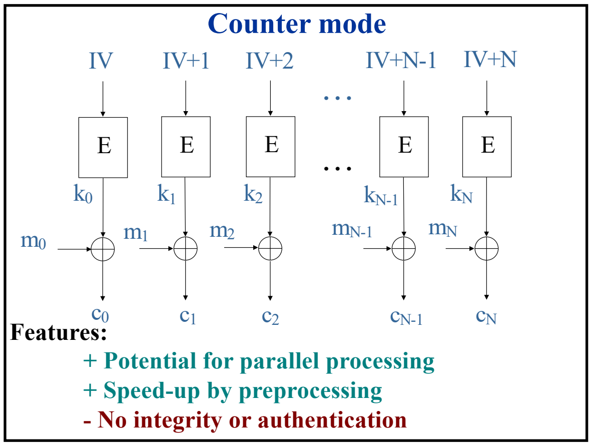
CBC



Problems:

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

44

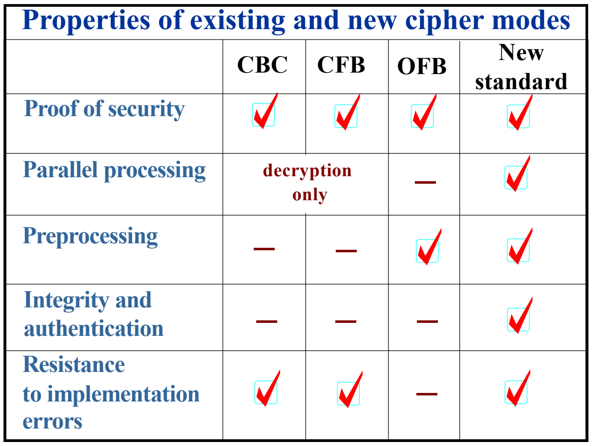


Counter mode

Features:

+ Potential for parallel processing
+ Speed-up by preprocessing
- No integrity or authentication

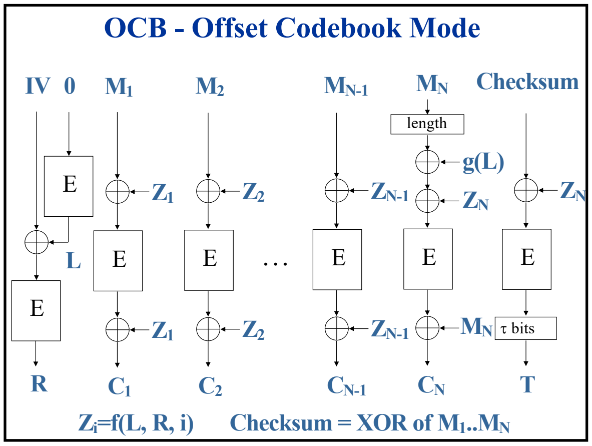
45



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	✓	✓	–	✓

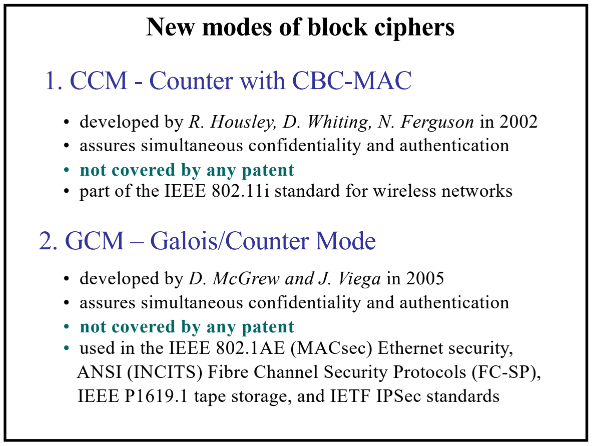
46



OCB - Offset Codebook Mode

Z_i=f(L, R, i) Checksum = XOR of $M_1..M_N$

47



New modes of block ciphers

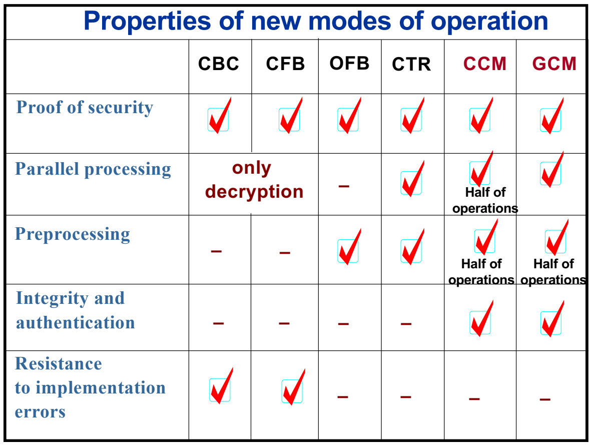
1. CCM - Counter with CBC-MAC

- developed by *R. Housley, D. Whiting, N. Ferguson* in 2002
- assures simultaneous confidentiality and authentication
- **not covered by any patent**
- part of the IEEE 802.11i standard for wireless networks

2. GCM – Galois/Counter Mode

- developed by *D. McGrew and J. Viega* in 2005
- assures simultaneous confidentiality and authentication
- **not covered by any patent**
- used in the IEEE 802.1AE (MACsec) Ethernet security, ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, and IETF IPSec standards

48



Properties of new modes of operation

	CBC	CFB	OFB	CTR	CCM	GCM
Proof of security	✓	✓	✓	✓	✓	✓
Parallel processing	only decryption		–	✓	✓ Half of operations	✓
Preprocessing	–	–	✓	✓	✓ Half of operations	✓ Half of operations
Integrity and authentication	–	–	–	–	✓	✓
Resistance to implementation errors	✓	✓	–	–	–	–