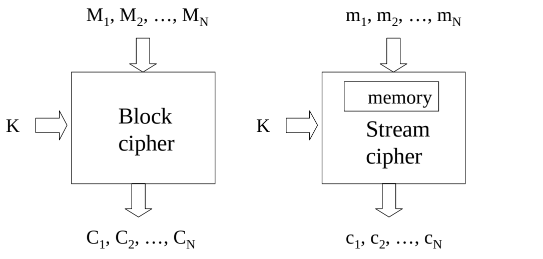
ECE 297:11 Lecture 6

Modes of operation of secret-key block ciphers

Block vs. stream ciphers



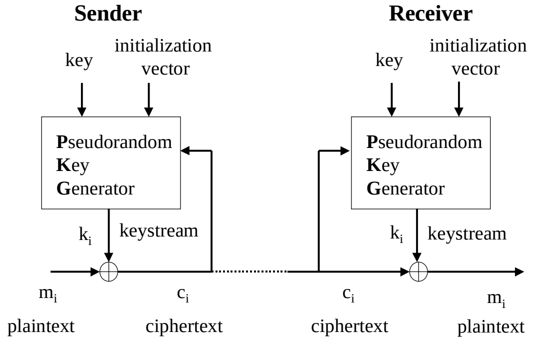
$C_i = f_K(M_i)$

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

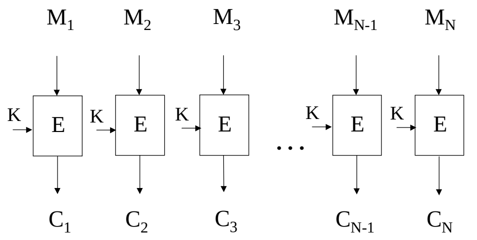
$c_i = f_K(m_i, m_{i-1}, \ldots, m_2, m_1)$

Every block of ciphertext is a function of the **current and all proceeding blocks** of plaintext

Typical stream cipher

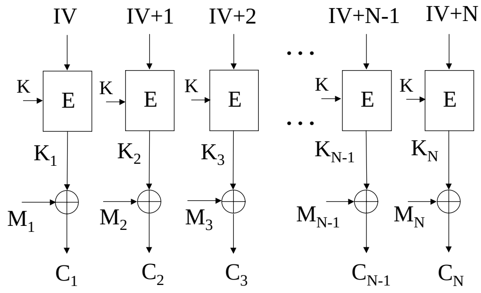


Electronic Codebook Mode - ECB



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

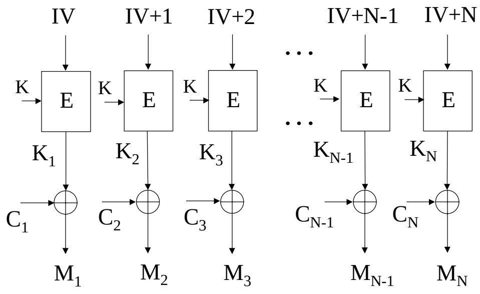
Counter Mode - CTR
Encryption



$C_i = M_i \oplus K_i$

$K_i = E(IV+i-1)$ for i=1..N

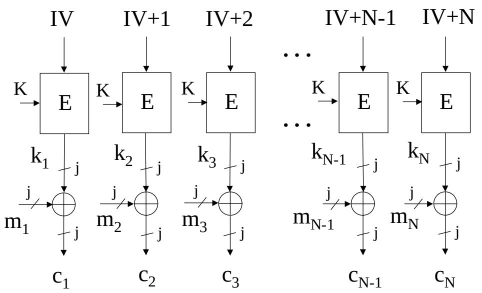
Counter Mode - CTR
Decryption



$M_i = C_i \oplus K_i$

$K_i = E(IV+i-1)$ for i=1..N

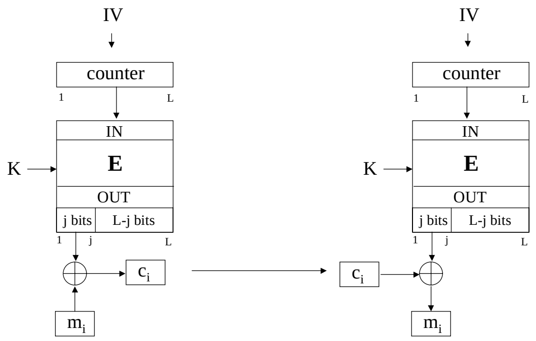
J-bit Counter Mode - CTR



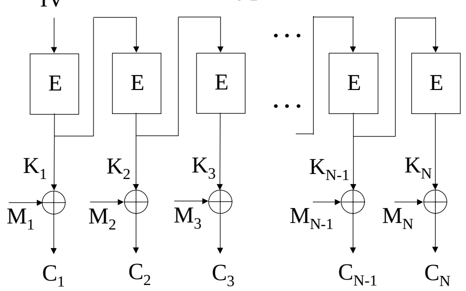
$c_i = m_i \oplus k_i$

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

J-bit Counter Mode - CTR



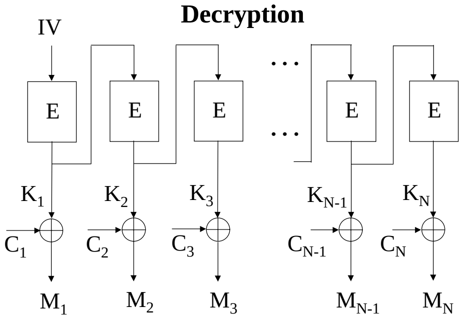
Output Feedback Mode - OFB Encryption



$C_i = M_i \oplus K_i$

$K_i = E(K_{i-1})$ for $i=1..N$, and $K_0 = IV$

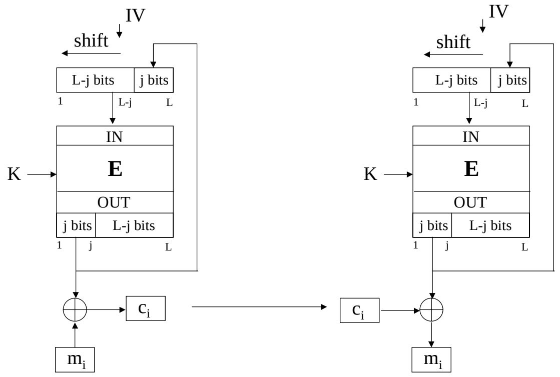
Output Feedback Mode - OFB Decryption



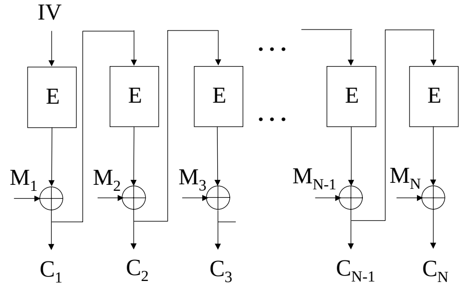
$M_i = C_i \oplus K_i$

$K_i = E(K_{i-1})$ for i=1..N, and $K_0 = IV$

J-bit Output Feedback Mode - OFB



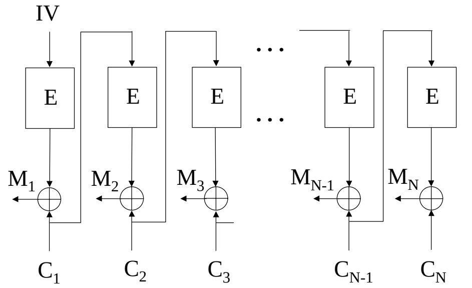
Cipher Feedback Mode - CFB Encryption



$C_i = M_i \oplus K_i$

$K_i = E(C_{i-1})$ for i=1..N, and $C_0 = IV$

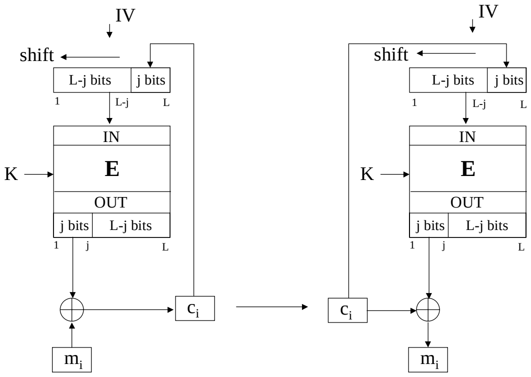
Cipher Feedback Mode - CFB Decryption



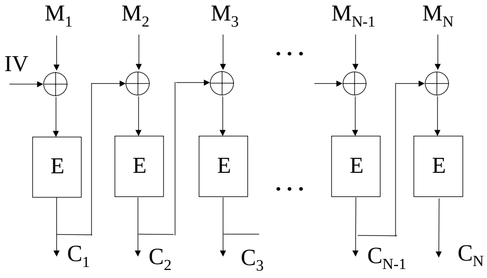
$C_i = M_i \oplus K_i$

$K_i = E(C_{i-1})$ for i=1..N, and $C_0 = IV$

J-bit Cipher Feedback Mode - CFB

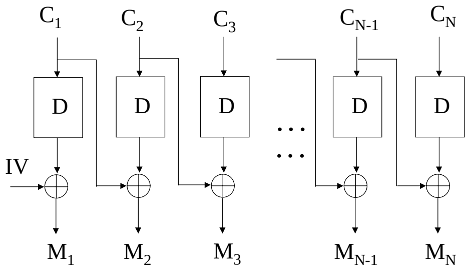


Cipher Block Chaining Mode - CBC Encryption



$C_i = E(M_i \oplus C_{i-1})$ for i=1..N C_0=IV

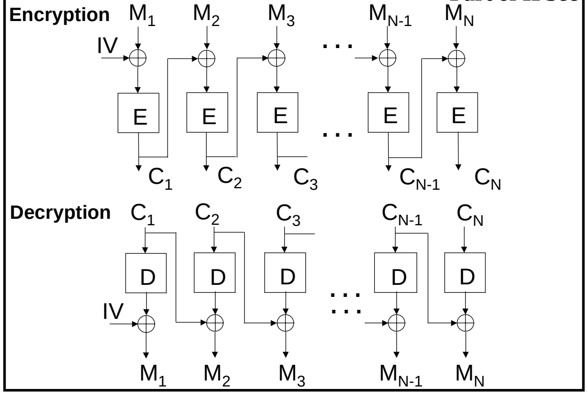
Cipher Block Chaining Mode - CBC Decryption



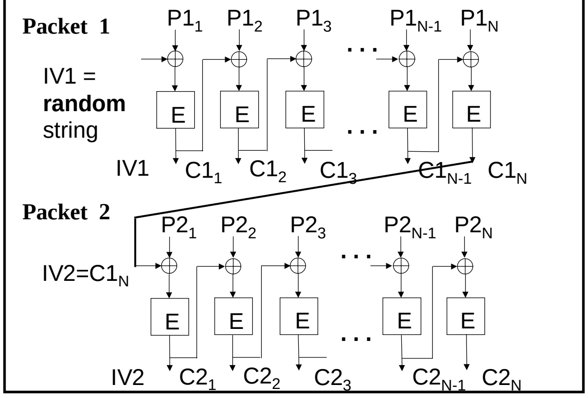
$M_i = D(C_i) \oplus C_{i-1}$ for i=1..N C_0=IV

Modes of operation: CBC

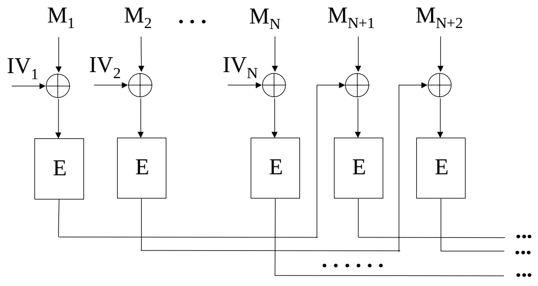
RFC 2405
Part of IPSec



CBC: Implementation Issues: Encryption



Interleaved operating modes



$C_i = E(M_i \oplus IV_i)$ for i=1 to N,

$C_i = E(M_i \oplus C_{i-N})$ for i>N

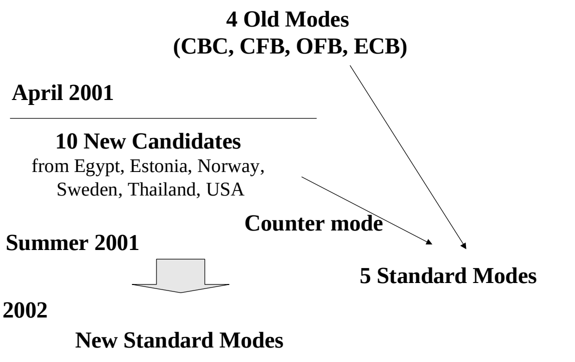
Block Cipher Modes of Operation Basic Features (1)

	ECB	**CTR**	**OFB**	**CFB**	**CBC**
Security	weak	strong	strong	strong	strong
Basic speed	s_{ECB}	$\approx s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx j/L \cdot s_{ECB}$	$\approx s_{ECB}$
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

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	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
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

Operating Modes Contest



4 Old Modes
(CBC, CFB, OFB, ECB)

April 2001

10 New Candidates
from Egypt, Estonia, Norway,
Sweden, Thailand, USA

Counter mode

Summer 2001

5 Standard Modes

2002

New Standard Modes

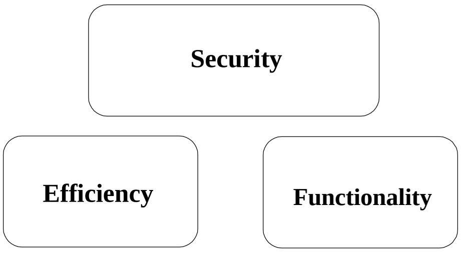
Modes submitted to the contest (1)

	Full name	Authors	Institution
2DEM	2D-Encryption Mode	A. A. Belal, M. A. Abdel-Gawad	Alexandria University, **Egypt**
ABC	Accumulated Block Chaining	L. Knudsen	U. of Bergen **Norway**
CTR	Counter Mode	H. Lipmaa, P. Rogaway, D. Wagner	**Finland, Estonia, USA, Thailand**
IACBC	Integrity Aware CBC	C. Jutla	IBM, **USA**
IAPM	Integrity Aware Parallalizable Mode	C. Jutla	IBM, **USA**

Modes submitted to the contest (2)

	Full name	Authors	Institution
IGE	Infinite Garble Extension	V. D. Gligor, P. Donescu	VDG, Inc., **USA**
KFB	Key Feedback Mode	J. Håstad, M. Naslund	NADA, Ericsson **Sweden**
OCB	Offset Codebook	P. Rogaway	**UCSD, USA, Thailand**
PCFB	Propagating Cipher Feedback	H. Hellström	StreamSec, **Sweden**
XCBC	eXtended CBC Encryption	V. D. Gligor, P. Donescu	VDG, Inc., **USA**

Evaluation Criteria for Modes of Operation



Evaluation criteria (1)

Security

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

Efficiency

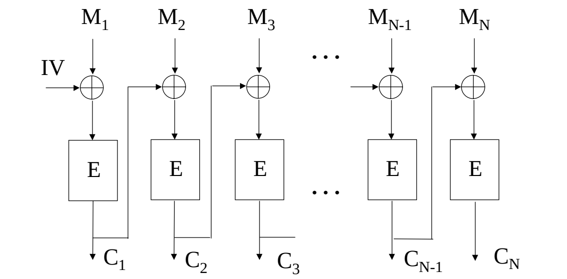
- number of calls of the block cipher
- **capability for parallel processing**
- memory/area requirements
- initialization time
- **capability for preprocessing**

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

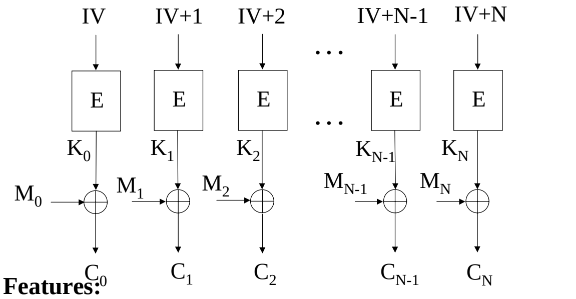
Modes of operation: Current standard - CBC



Problems:

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

Counter mode



Features:

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

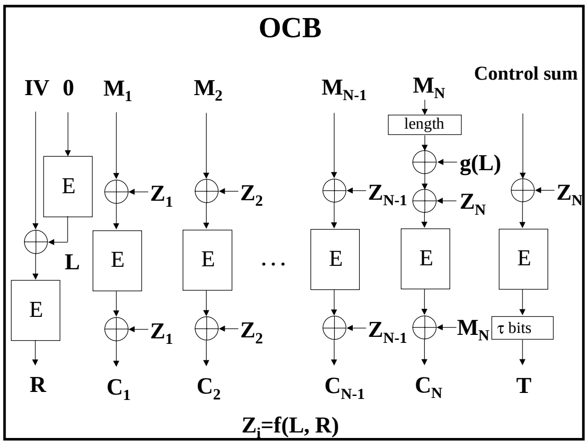
Properties of existing and new cipher modes

	CBC	**CFB**	**OFB**	**New standard**
Proof of security	✓	✓	✓	✓
Parallel processing	**decryption only**		–	✓
Preprocessing	–	–	✓	✓
Integrity and authentication	–	–	–	✓
Resistance to implementation errors	✓	✓	–	✓

Encryption with authentication

	Full name	Authors	Institutions
IACBC	Integrity Aware CBC	C. Jutla	**IBM** (**patent**)
IAPM	Integrity Aware Parallalizable Mode	C. Jutla	**IBM** (**patent**)
XCBC-XOR	eXtended CBC Encryption	V. D. Gligor, P. Donescu	**VDG, Inc.,** (**patent**)
XECB-XOR	eXtended ECB Encryption	V. D. Gligor, P. Donescu	**VDG, Inc.,** (**patent**)
OCB	Offset Codebook	P. Rogaway	**UCSD**, USA, Thailand

OCB



Z_i=f(L, R)