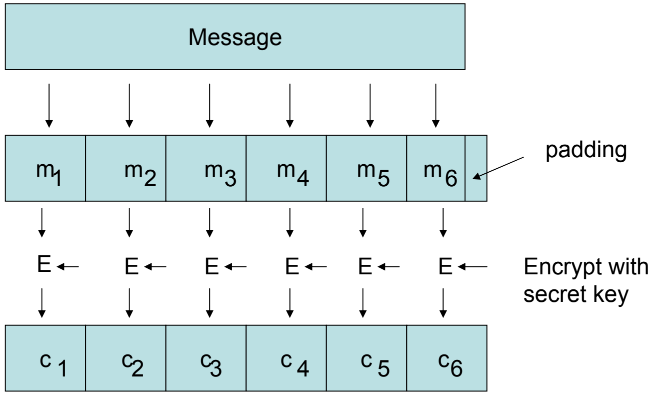
Implementing Encryption/Decryption

Enciphering a stream of data and generating MACs

Implementing Encryption/Decryption

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- K-bit Cipher Feedback Mode (CFB)
- K-bit Output Feedback Mode (OFB)
- Counter Mode (CTR)

Electronic Codebook Encryption



Message

m_1 m_2 m_3 m_4 m_5 m_6

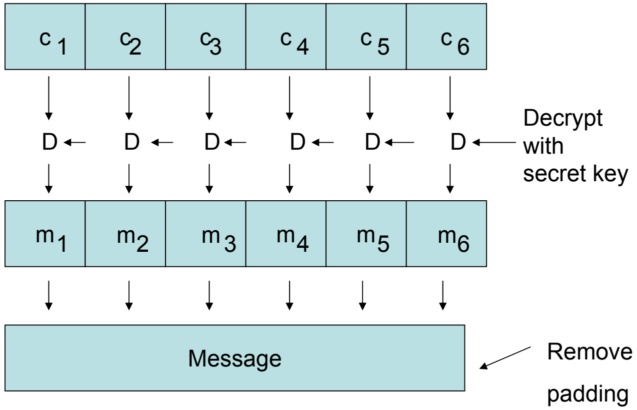
padding

E E E E E E

Encrypt with secret key

c_1 c_2 c_3 c_4 c_5 c_6

Electronic Codebook Decryption



c_1 c_2 c_3 c_4 c_5 c_6

D D D D D D

Decrypt with secret key

m_1 m_2 m_3 m_4 m_5 m_6

Message

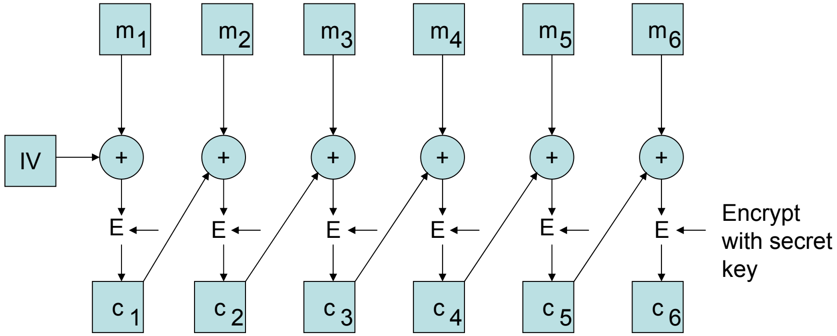
Remove padding

Attacking ECB Implementation

- Identical plaintext blocks
- → identical ciphertext blocks

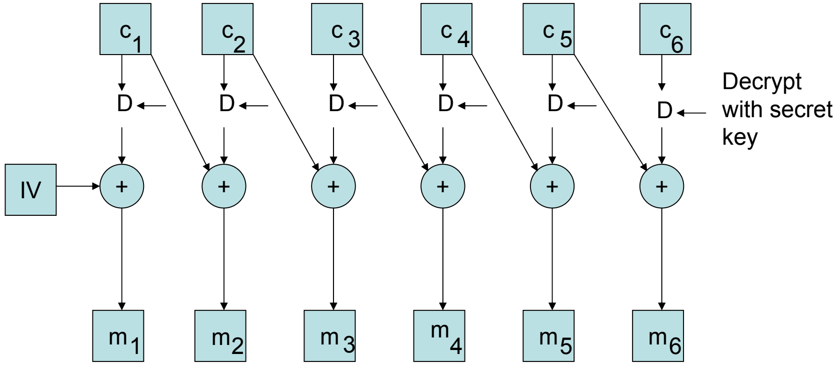
- Rearrange blocks
- Duplicate blocks

Cipher Block Chaining (CBC) Encryption

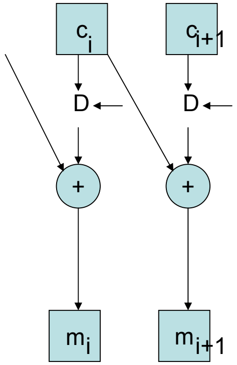


N.B. IV (initialisation vector) may be omitted but could have security implications In which case it should be chosen at random.

Cipher Block Chaining (CBC) Decryption



Attacking CBC (i)



Changing c_i gives predictable change in m_{i+1} but unpredictable m_i

Attacking CBC (ii)

Rearranging ciphertext contiguous pair c_i, c_{i+1} moves m_{i+1} to desired position

Prevent attacks (i) and (ii) with a CRC

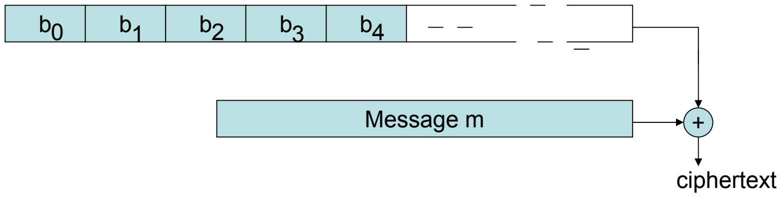
Output feedback Mode (OFB) Encryption

Manipulate random 64 bit number $b_0$as follows

$b_0 \rightarrow E \rightarrow b_1 \rightarrow E \rightarrow b_2 \rightarrow E \rightarrow b_3 \rightarrow E \rightarrow b_4$etc to produce one time pad $b_0 b_1 b_2 b_3 b_4$ etc

Then add mod 2 to message to give ciphertext

N.B. initial random number b_0 must also be sent

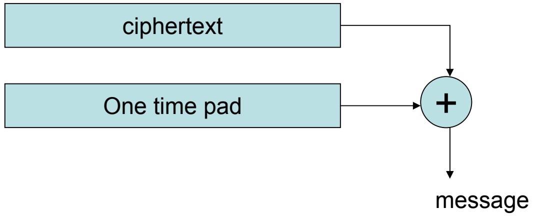


Output Feedback Mode (OFB) Decryption

Receive b_0 and ciphertext

Create one time pad b_0 b_1 b_2 $b_3$etc

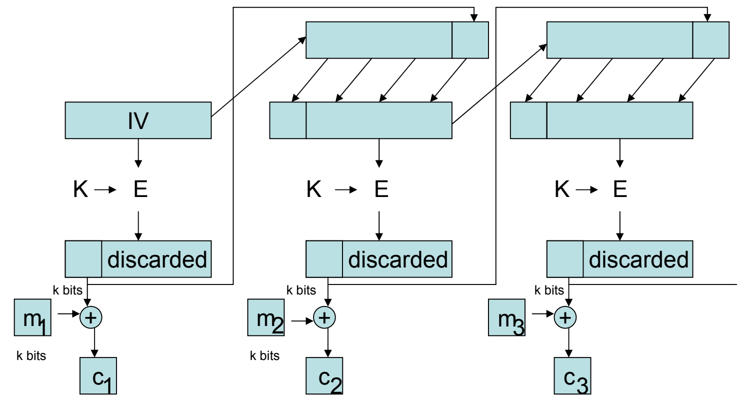
Add ciphertext mod 2 to one time pad



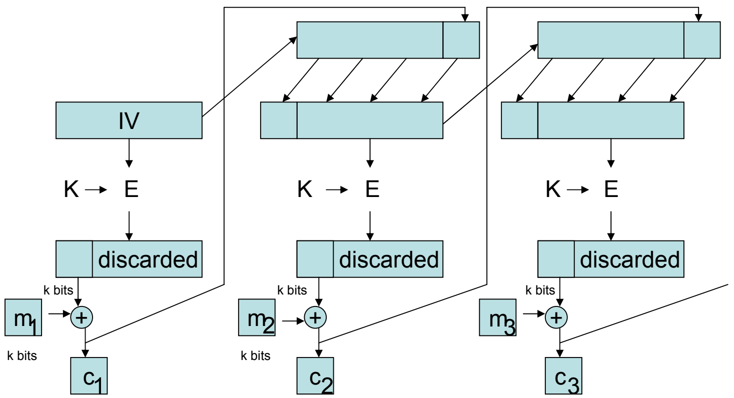
Features of OFB

- Very fast (mod 2 is simple to execute)
- May prepare one time pad in advance
- Errors in ciphertext do not multiply in plain text (cf CBC)
- Not limited to 64 bit blocks of plaintext
- Easy to modify if plaintext/ciphertext blocks are known

k-bit OUTPUT FEEDBACK MODE (OFB)



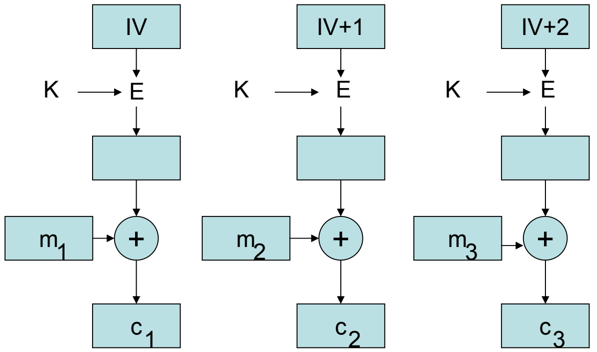
k-bit CIPHER FEEDBACK MODE (CFB)



Features of CFB

- Sync follows removal or addition of bytes (8-bit CFB allows resync after 8 bytes)
- Protection against rearrangement of ciphertext (cf CBC)

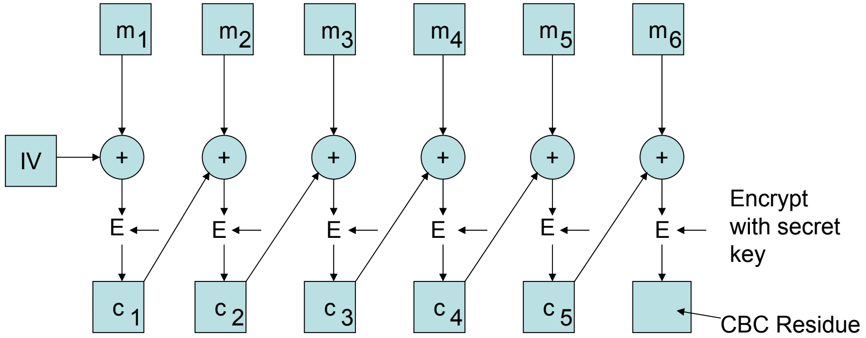
Counter Mode



Features of Counter Mode

- Stream may be pre-computed (cf OFB)
- May decrypt at any point
- Useful for table look ups

Message Authentication Code MAC

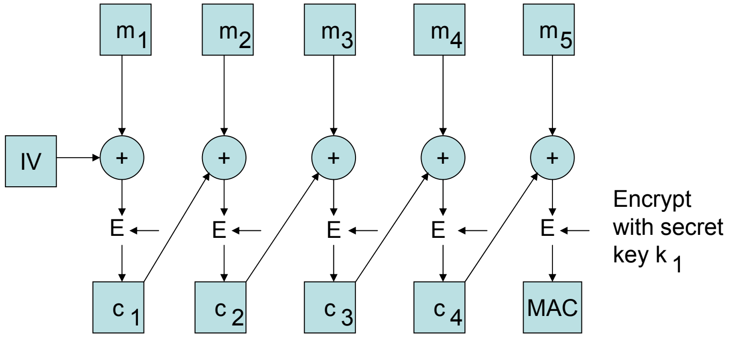


N.B. CBC residue is a function of entire message and E and may be used as a MAC

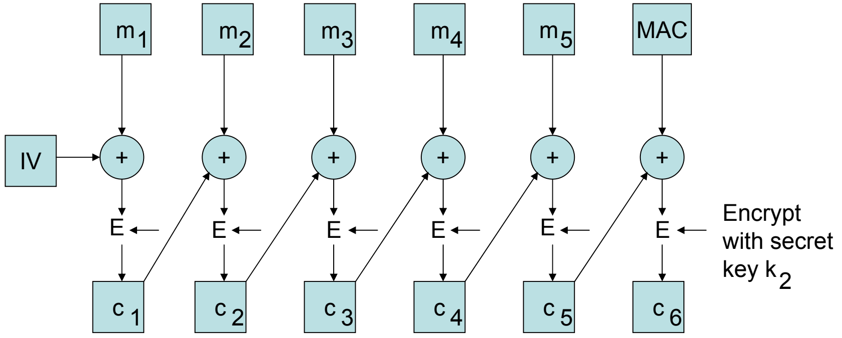
Privacy and Integrity

- MAC ensures integrity and may be used without encryption (e.g. payment messages)
- A CBC residue cannot be used as a MAC if CBC encryption is employed with the same key
- Use separate keys for MAC and encryption

Privacy and Integrity MAC Generation



Privacy and Integrity Encryption


m1
m2
m3
m4
m5
MAC
IV
+
E
c 1
c 2
c 3
c 4
c 5
c 6
Encrypt with secret key k 2