Encrypting a Large Massage

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Output Feedback Mode (OFB)
4. Cipher Feedback Mode (CFB)

Electronic Code Book (ECB)

- Break the message into 64-bit blocks (padding the last one) and encrypt each block with the secret key.
- ***Two problems*:**
- 1. two identical plain text block produce two identical cipher text blocks
  2. blocks can be rearranged or modified.

Cipher Block Chaining (CBC)

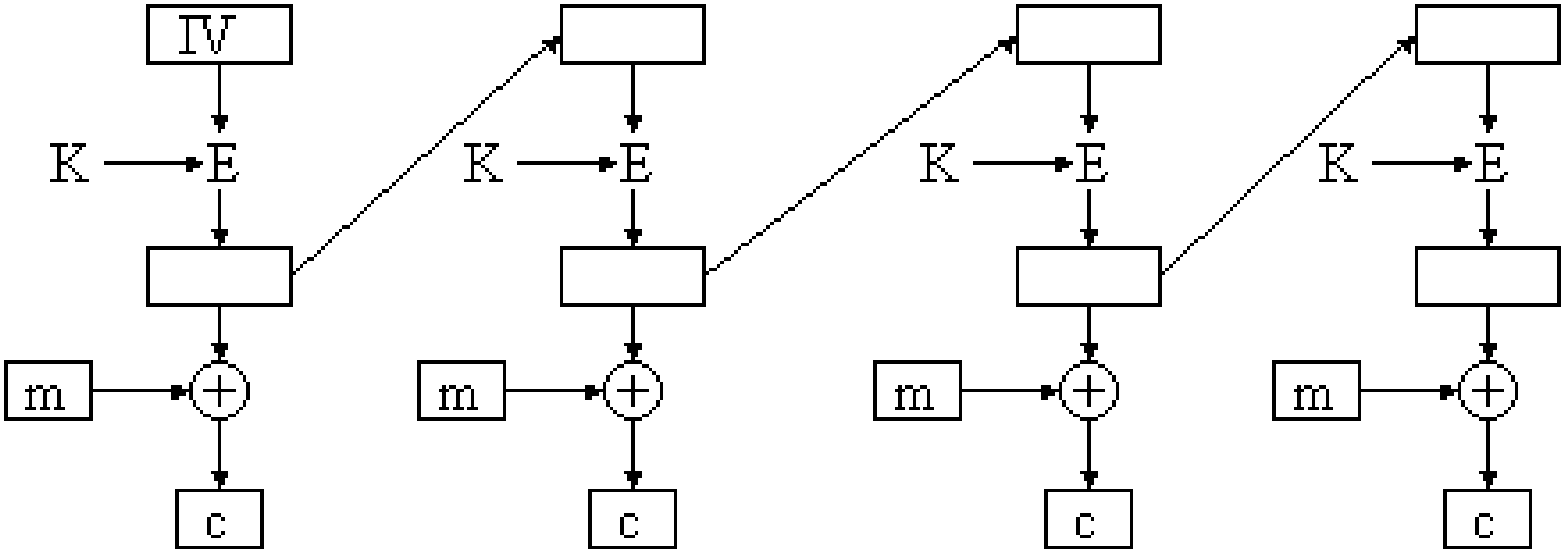
- Two identical plain text messages produce two different cipher text messages.
  (e.g., continue holding, continue holding, ..., start attach)

Output Feedback Mode (OFB)

- Encryption/decryption is performed by ®ing the message with one-time pad generated as follows:

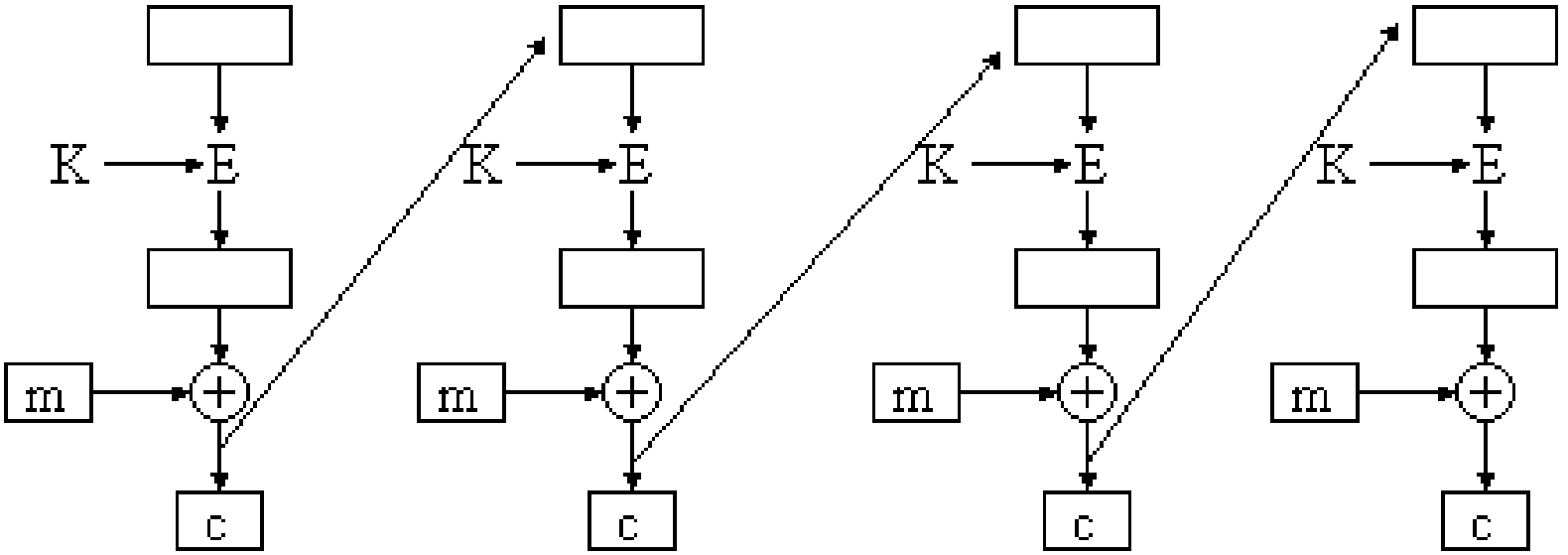
- 1. A 64-bit random IV is generated (and is transmitted with the encrypted message).

Output Feedback Mode (OFB)



Cipher Feedback Mode (CFB)

- . A 64-bit random IV is generated (and is transmitted with the encrypted message). 2. b_1 is the DES encryption of IV with the secret key.


K
E
m
c
K
E
m
c
K
E
m
c
K
E
m
c

International Data Encryption Algorithm

- DES algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications. However, its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours
- IDEA is a block cipher designed by Xuejia Lai and James L. Massey in 1991
- It is a minor revision of an earlier cipher, PES (Proposed Encryption Standard)
- IDEA was originally called IPES (Improved PES) and was developed to replace DES

Overview (cont’)

- IDEA was used as the symmetric cipher in early versions of the Pretty Good Privacy cryptosystem.
- PGP - Pretty Good Privacy
- general purpose application to protect (encrypt and/or sign) files
- can be used to protect e-mail messages
- can be used by corporations as well as individuals
- based on strong cryptographic algorithms (IDEA, RSA, SHA-1)

Detailed description of IDEA

- IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key
- The algorithm structure has been chosen such that when different key sub-blocks are used, the encryption process is identical to the decryption process

Applications of IDEA

- Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government
- The IDEA algorithm can easily be embedded in any encryption software. Data encryption can be used to protect data transmission and storage. Typical fields are:
  - Audio and video data for cable TV, pay TV, video conferencing, distance learning
  - Sensitive financial and commercial data
  - Email via public networks
  - Smart cards

Conclusion

- As electronic communications grow in importance, there is also an increasing need for data protection
- When PGP was designed, the developers were looking for maximum security. IDEA was their first choice for data encryption
- The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation

Multiple Encryption DES

- Called 3-DES
- Use two keys, k1 and k2.