Computer and Network Security: Block Modes

Kameswari Chebrolu

All the figures used as part of the slides are either self created or from the public domain with either 'creative commons' or 'public domain dedication' licensing. The public sites from which some of the figures have been picked include: http://commons.wikimedia.org (Wikipedia, Wikimedia and workbooks); http://www.sxc.hu and http://www.pixabay.com

Outline

- **Modern Cryptography**
  - Overview
  - **Confidentiality**
    - Background: Definition, Crypto-analysis, One Time Pads
    - Symmetric key encryption, **Block modes**
    - Asymmetric key encryption
  - Integrity (includes Authentication)
    - Hashes, MAC, Digital signature

Recap

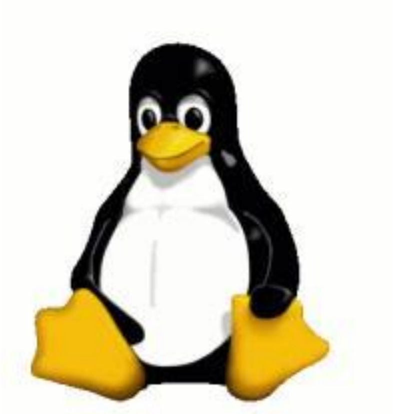
- Block Cipher operates on a block of plain/cipher text
- Examples: DES, 3-DES and AES
  - Confusion and Diffusion
  - Terms: Substitute, Permute, Mangle, Mix, Add-roundkey, Rounds
- How to encrypt a variable length message larger than block size?

Modes of Operation

- Specifies how an encryption algorithm is used in practice
- We have
  - Message divided into B1, B2, B3, ……. blocks (block length = n)
  - If message not a multiple of n?
    - For some modes, pad message before encryption to make it multiple of n
      - E.g. add 1 followed by zeros
    - Unpad after decryption
  - Key k
  - Block cipher algorithm like AES or DES

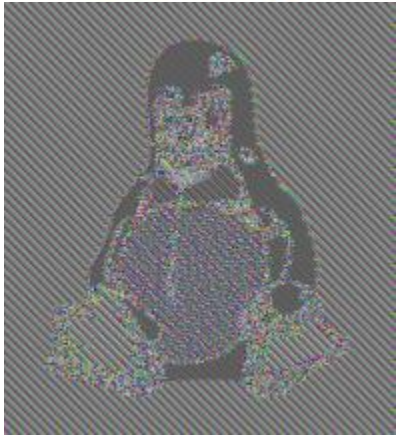
Electronic Code Book (ECB)

$$C_i = E_k(B_i) \text{ and } B_i = D_k(C_i)$$



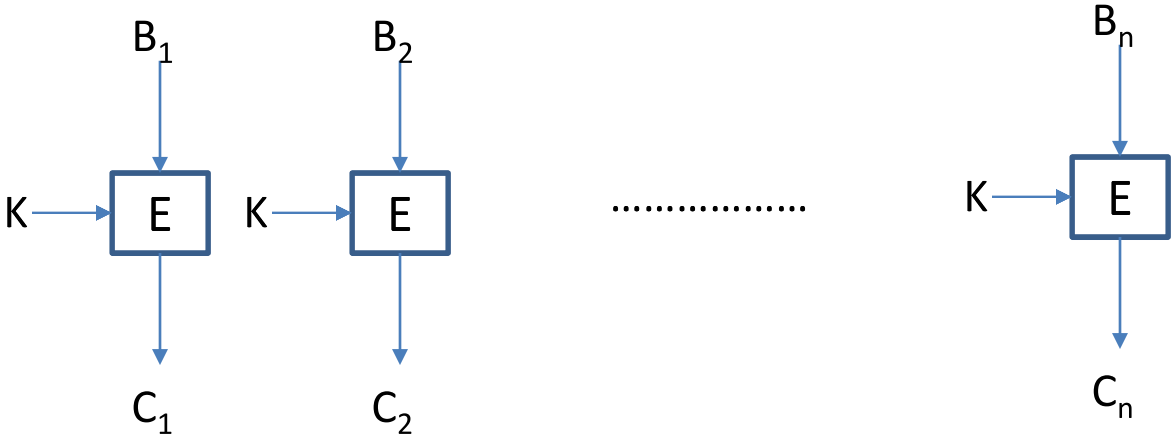
+ Simple
+ Tolerates losses
- May reveal patterns
- Can rearrange blocks to advantage

- ECB not used in practice
  - Good for encrypting random data like keys



ECB encoded image

Block Diagram



Example

Block1	Block2	Block3	Block4	Block5	Block6	Block7	Block8
Kamesw	ari	Pr	ofessor	I IT	Bombay	5	1,235.50
Bharga	v	Pr	ofessor	I IT	Bombay	5	1,235.50
Bhaska	R	Pr	ofessor	I IT	Bombay	8	1,175.00
Lakshm	I	Pr	ofessor	I IT	Bombay	8	9,775.00

- Can determine set of employees with identical salaries (last two blocks)
- Set of employees with same salary in 10,000’s range
- Change salary (copy last but one block of higher salary person to own)

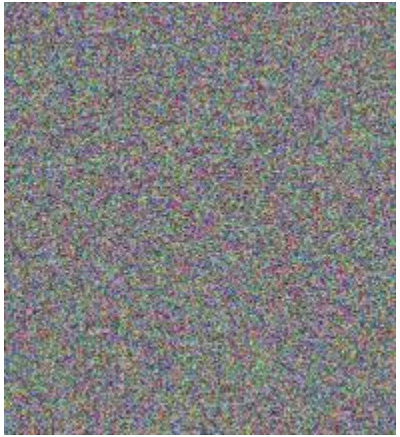
Cipher Block Chaining (CBC)

$$C_i = E_k(B_i \oplus C_{i-1}) \text{ and } B_i = D_k(C_i) \oplus C_{i-1}$$

- C_o: initialization vector (IV)
  – Has to be random each time. Why?
- Transmit IV with ciphertext

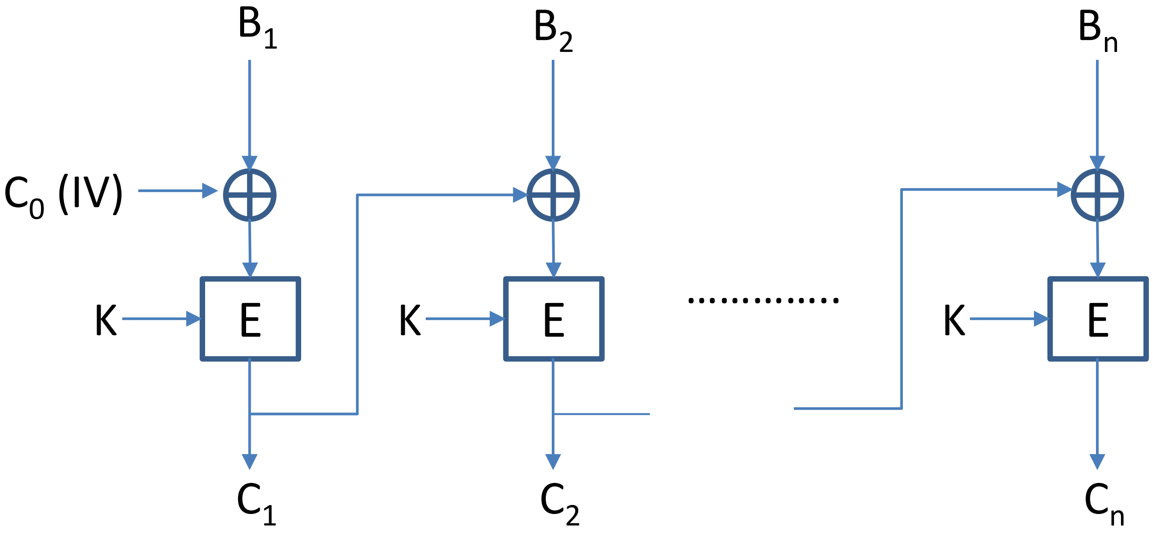
+ Does not reveal patterns

+ Decryption can happen in parallel (if all cipher text is available)



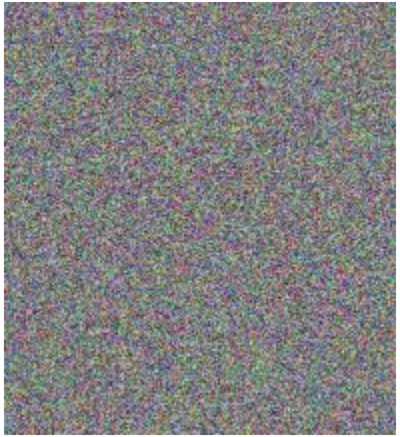
Non ECB mode

Block Diagram



$$C_i = E_k(B_i \oplus C_{i-1}) \text{ and } B_i = D_k(C_i) \oplus C_{i-1}$$

- Encryption needs to be in sequence
- Loss tolerance?
  - C_i is lost, i and i+1 blocks are lost
- Can modify blocks to advantage



Non ECB mode

Example

Block1	Block2	Block3	Block4	Block5	Block6	Block7	Block8
Kamesw	ari	Pr	ofessor	I IT	Bombay	5	1,235.50
Kamesw	ari	Pr	ofessor	I IT	Zxc%#FR	7	1,235.50

$$C_i = E_k(B_i \oplus C_{i-1}) \text{ and } B_i = D_k(C_i) \oplus C_{i-1}$$

Flip penultimate bit of C6

Maps to M7 xor 00….10

5 maps to 101; 7 maps to 111

M6 garbled due to tampering with C6

Cipher Feedback Mode (CFB)

$$C_i = E_k(C_{i-1}) \oplus B_i \text{ and } B_i = E_k(C_{i-1}) \oplus C_i$$

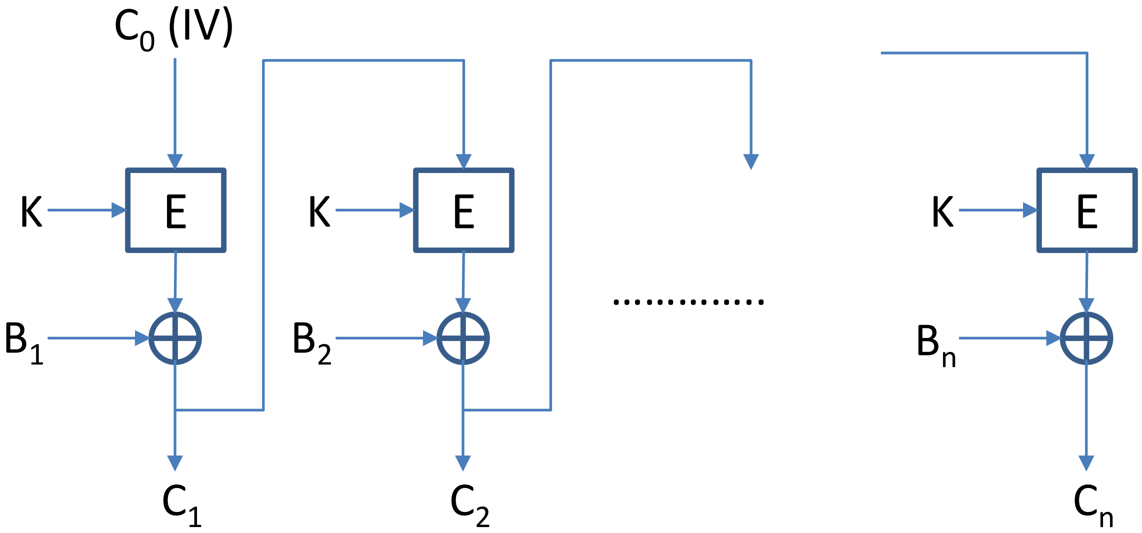
Transmit C_0 (IV, random) with ciphertext

+ Involves no decryption
    + If decryption is a slower operation, CFB better than CBC
+ Decryption can be in parallel

- Encryption needs to be in sequence

- Can modify plain text but it will garble next block

Block Diagram



Stream Ciphers

- Operate on a stream of plain/cipher text, one symbol at a time
  - Similar to one time pads (xor plain text with random bits)
- Key is not random bits. Why?
- Key (fixed bits) is input to a pseudo random generator that outputs arbitrarily long random bits

- “Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin. “ -- **John von Neumann**
- PRG(K) not truly random but goal is computationally secure
  - Attacker can’t distinguish pseudo random pad from truly random pad.
- E(K,M) = PRG(K,IV) xor M
- Example: RC4 stream cipher (has vulnerabilities)
- Block ciphers can turn into stream ciphers. How?

Output Feedback Mode (OFB)

$$V_i = E_k(V_{i-1}) \text{ and } C_i = V_i \oplus B_i \text{ and } B_i = V_i \oplus C_i$$

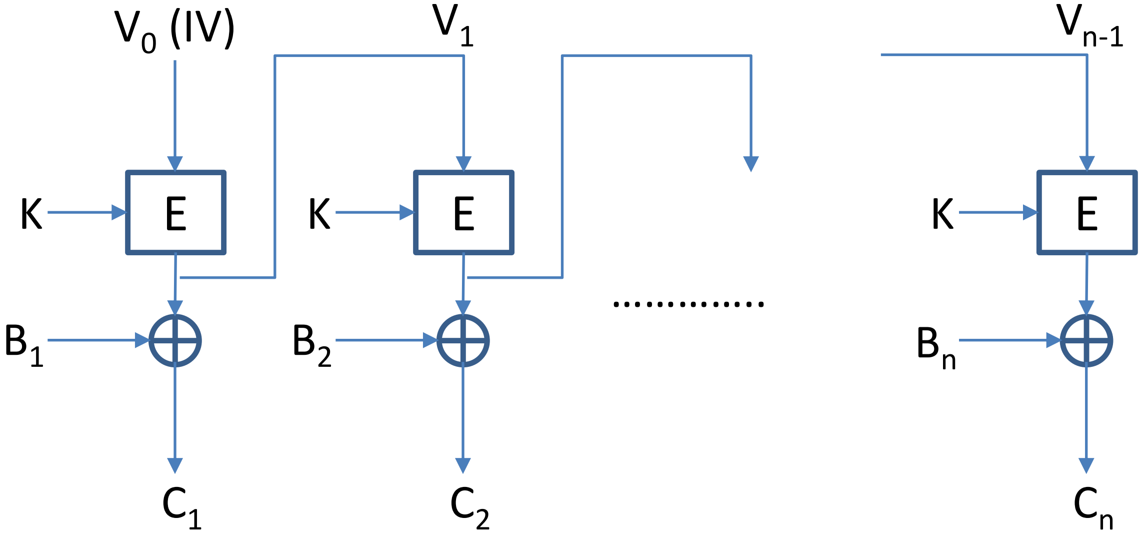
- V_i's can be generated before hand
  - Initialization vector V_0; random each time
  - Similar to a one time pad
  - Transmit IV with ciphertext

+ Tolerates losses

+ Encryption/Decryption can happen in parallel

- Can modify plaintext (no garbling also)

Block Diagram

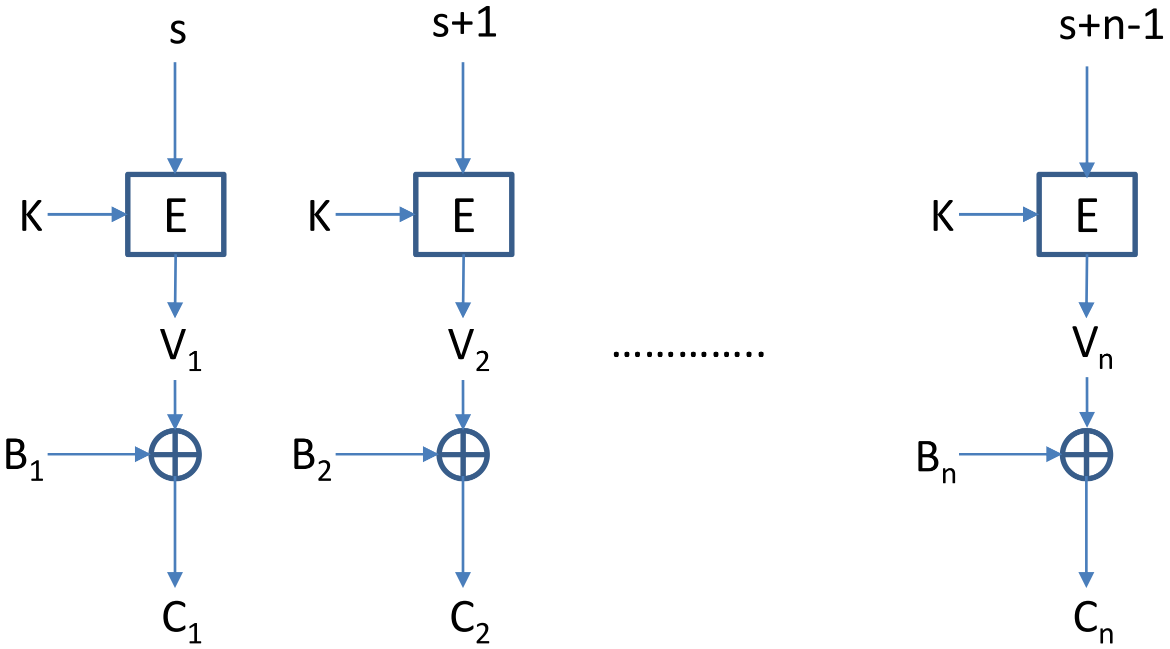


Counter Mode (CTR)

$$V_i = E_k(s+i-1),\ C_i = V_i \oplus B_i \text{ and } B_i = V_i \oplus C_i$$

- Very similar to OFB, except can decrypt at any point rather than from beginning
  - i.e. Pad (V_i) can be generated in parallel
- Gaining popularity over CBC
- s has to be random each time
- Transmit s with ciphertext

Block Diagram



Note: OFB, CTR are stream ciphers. CFB can also be converted into stream cipher, albeit its more complex

Summary

- Symmetric key algorithms like DES, AES are great, but usage as important
  - ECB highlights the drawbacks
- CBC, CFB, OFB, CTR other alternatives
  - Some positives and negatives
  - Still subject to tampering
- Integrity (to be covered) essential to protect against tampering of ciphertext