Information Protection & Computer Security

Rajendra Kachhwaha
Email: rajendra1983@gmail.com

June 23, 2015

- **Already Covered:**

  1. Security Architecture, Security Attacks, Security Services.

  2-3.Model for Network Security,Basic terms used in Cryptography, Symmetric Cipher Model, Substitution Techniques, Transpositions Techniques.

  4.Block Cipher and Stream Ciphers,Component of Modern Block Cipher, Feistel Cipher Structure, Data Encryption Standard (DES)

  5. Numerical Problems

- Lecture 6.

  Today's Topic:

  Triple DES

  Block Cipher Modes

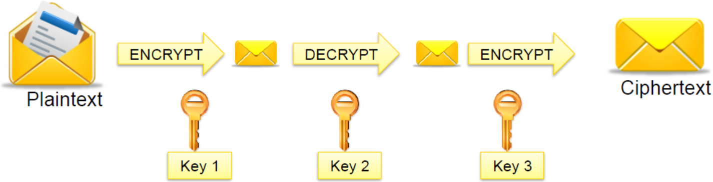
  Finite Fields

- **Triple DES:**(3DES)

  It is a block cipher that applies DES three times to each data block.

  It uses a key bundle comprising of three DES keys (K1,K2,K3), each with 56 bits.

  DES encrypts with K1, decrypts with K2, then encrypts with K3
  $C_i = E_{K3}(D_{K2}(E_{K1}(P_i)))$



  Disadvantage: very slow

- **Block Cipher Modes:**

  Defines how the block cipher algorithm is applied to the data stream.

  A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block. The block cipher modes provide confidentiality, but they do not protect against accidental modification or malicious tampering.

  Five Basic Modes

  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC) /Propagating Cipher block chaining
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

- **Initialization vector (IV):** (unique non-repeating binary sequence)

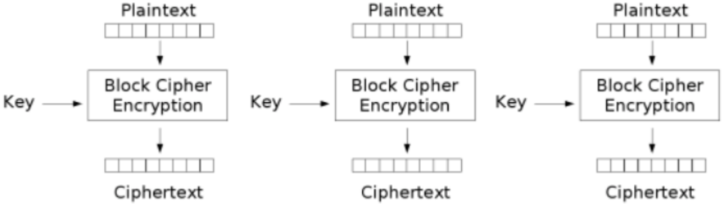
  An initialization vector (IV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertexts.

- **Padding:**

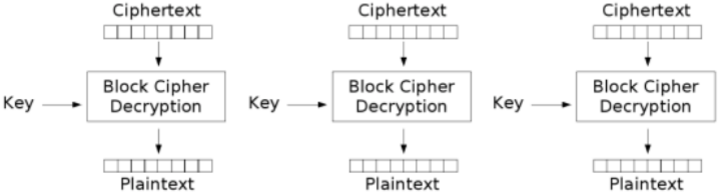
  A block cipher works on units of a fixed size (block size), but messages come in a variety of lengths. So some modes require that the final block be padded before encryption. The simplest is to add null bytes to the plaintext to bring its length up to a multiple of the block size.

Information Protection & Computer Security

Electronic code book Mode:



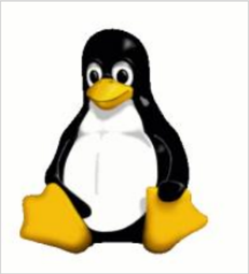
Electronic Codebook (ECB) mode encryption

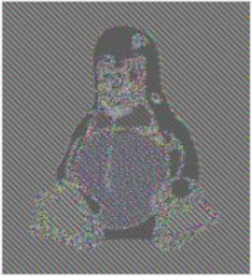


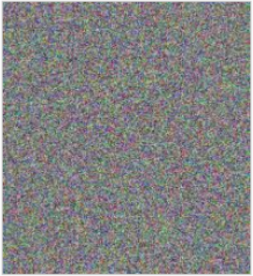
Electronic Codebook (ECB) mode decryption

- **Electronic code book Mode:**

  Example of ECB mode

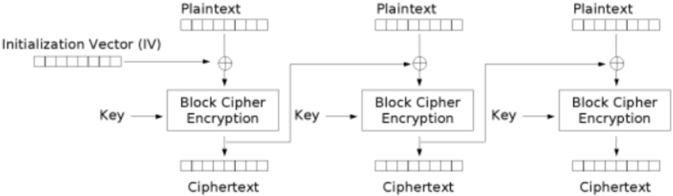

Original image


Encrypted using ECB mode


Modes other than ECB result in pseudo-randomness

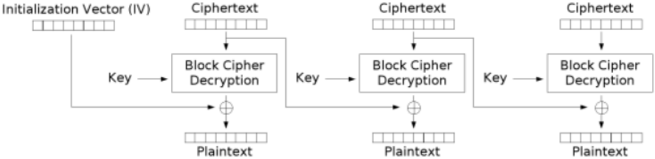
The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all.

Cipher block chaining Mode:



$$C_i = E_k(P_i \oplus C_{i-1}), C_0 = IV$$

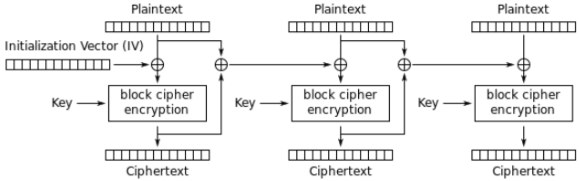
Cipher Block Chaining (CBC) mode encryption



$$P_i = D_k(C_i) \oplus C_{i-1}, C_0 = IV$$

Cipher Block Chaining (CBC) mode decryption

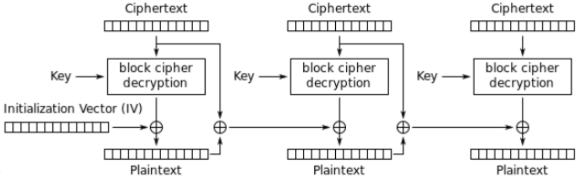
Propagating Cipher block chaining Mode:



Propagating Cipher Block Chaining (PCBC) mode encryption

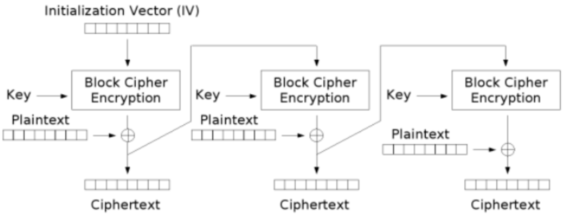
$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1}), P_0 \oplus C_0 = IV$$

$$P_i = D_K(C_i) \oplus P_{i-1} \oplus C_{i-1}, P_0 \oplus C_0 = IV$$



Propagating Cipher Block Chaining (PCBC) mode decryption

Cipher feedback mode:

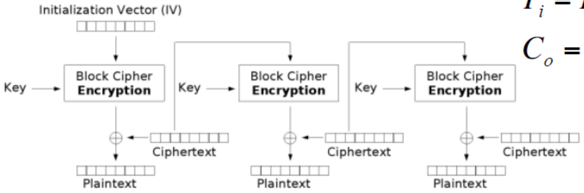


Cipher Feedback (CFB) mode encryption

$$C_i = E_k(C_{i-1}) \oplus P_i$$

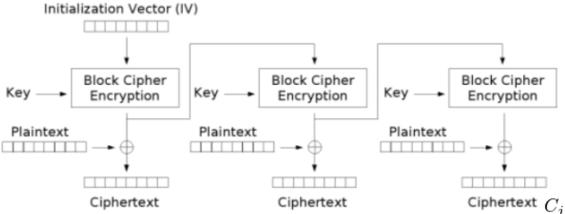
$$P_i = E_k(C_{i-1}) \oplus C_i$$

$$C_o = IV$$



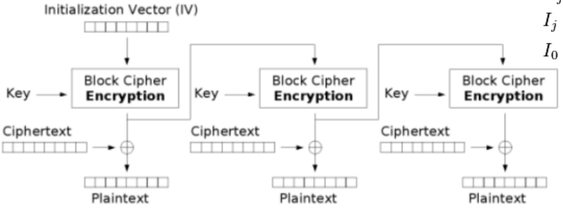
Cipher Feedback (CFB) mode decryption

Output feedback mode:



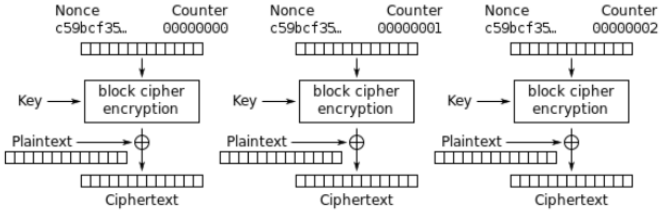
Output Feedback (OFB) mode encryption

$$C_j = P_j \oplus O_j$$
$$P_j = C_j \oplus O_j$$
$$O_j = E_K(I_j)$$
$$I_j = O_{j-1}$$
$$I_0 = \text{IV}$$

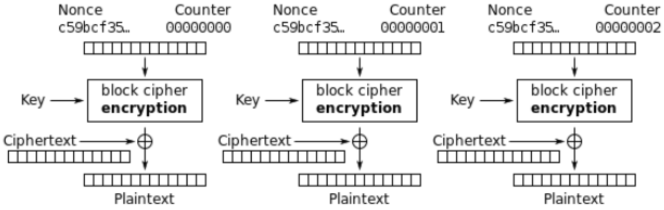


Output Feedback (OFB) mode decryption

- **Counter mode:**



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Finite Fields:

- Group, Rings and Fields
- Modular Arithmetic
- Euclidean Algorithm
- Finite fields of the form GF(p)

1. A field is a set of elements on which two arithmetic operations (addition and multiplication) have been defined.
2. Modular Arithmetic is a kind of integer arithmetic that reduces all numbers to one of a fixed set [0,1,..n-1] for some number n.

Finite Fields:

- Group:
  A group G, denoted by {G,•}, is a set of elements with a binary operation, denoted by •, that associates to each ordered pair (a,b) of elements in G an element (a • b) in G, such that the following properties are satisfies:

1. A1.Closure:If a and b belongs to G, then a • b is also in G.
2. A2.Associative: a • (b • c) = (a • b) • c for all a,b,c in G.
3. A3.Identity element: There is an element e in G such that a • e = e • a = a, for all a in G.
4. A4.Inverse element: For each a in G there is an element a' in G such that a • a' = a' • a = e.

Finite Fields:

- Abelian Group:
  A group G, is said to be abelian group if it satisfies following properties:

A1.Closure:If a and b belongs to G, then a • b is also in G.

A2.Associative: a • (b • c) = (a • b) • c for all a,b,c in G.

A3.Identity element: There is an element e in G such that
a • e = e • a = a, for all a in G.

A4.Inverse element: For each a in G there is an element a' in G such that
a • a' = a' • a = e.

A5.Commutative: a • b = b • a for all a,b in G.

Finite Fields:

- Rings:
  A ring R, denoted by {R,+,X}, is a set of elements with two binary operations, such that the following properties are satisfies:

  (A1-A5) R is an abelian group with respect to addition.

  M1.Closure under multiplication: If a and b belongs to R, then ab is also in R.

  M2.Associativity of multiplication: a(bc) = (ab)c for all a,b,c in R.

  M3.Distributive laws: a(b+c) = ab + ac for all a,b,c in R.
  (a+b)c = ac + bc for all a,b,c in R.

1. A ring is commutative if it satisfies following additional condition:
   M4.Commutativity of multiplication: ab = ba for all a,b in R.
2. An integral domain, which is a commutative ring that obeys the following properties:
   M5.Multiplicative Identity: There is an element 1 in R such that a1 = 1a = a for all a in R. M6.No zero divisors: If a, b in R and ab=0, then either a=0 or b=0.

Finite Fields:

- Fields:
  A field F, denoted by {F,+,X}, is a set of elements with two binary operations, such that all a,b,c in F satisfies following properties:

  (A1-M6) F is an integral domain; that is, F satisfies A1 through A5 and M1 through M6.

  M7. Multiplicative Inverse: For each a in F, except 0, there is an element a^{-1} in F such that
  $aa^{-1} = (a^{-1})a = 1$.