Week 3

Lecture 1

Modern Symmetric key Ciphers

Lecture 2

Finite Field mathematics,

Workshop 3: Workshop based on Lectures in Week2

Quiz 3

Modern Symmetric key Ciphers

COMP90043

Lecture 1

15/08/2020

Udaya Parampalli

Modern Symmetric key Cryptography

Lecture 1

1.1 Modern Symmetric Ciphers

- Model and Design Principles
- Stream Ciphers and Block Ciphers

1.2 One-Time Pad Encryption

- Vernam Cipher
- One-Time Pad
- Perfect Secrecy

1.3 Fiestel Cipher

- Motivation and General ideas
- Cipher Terms and Structure
- Data Encryption Standard
- A worksheet

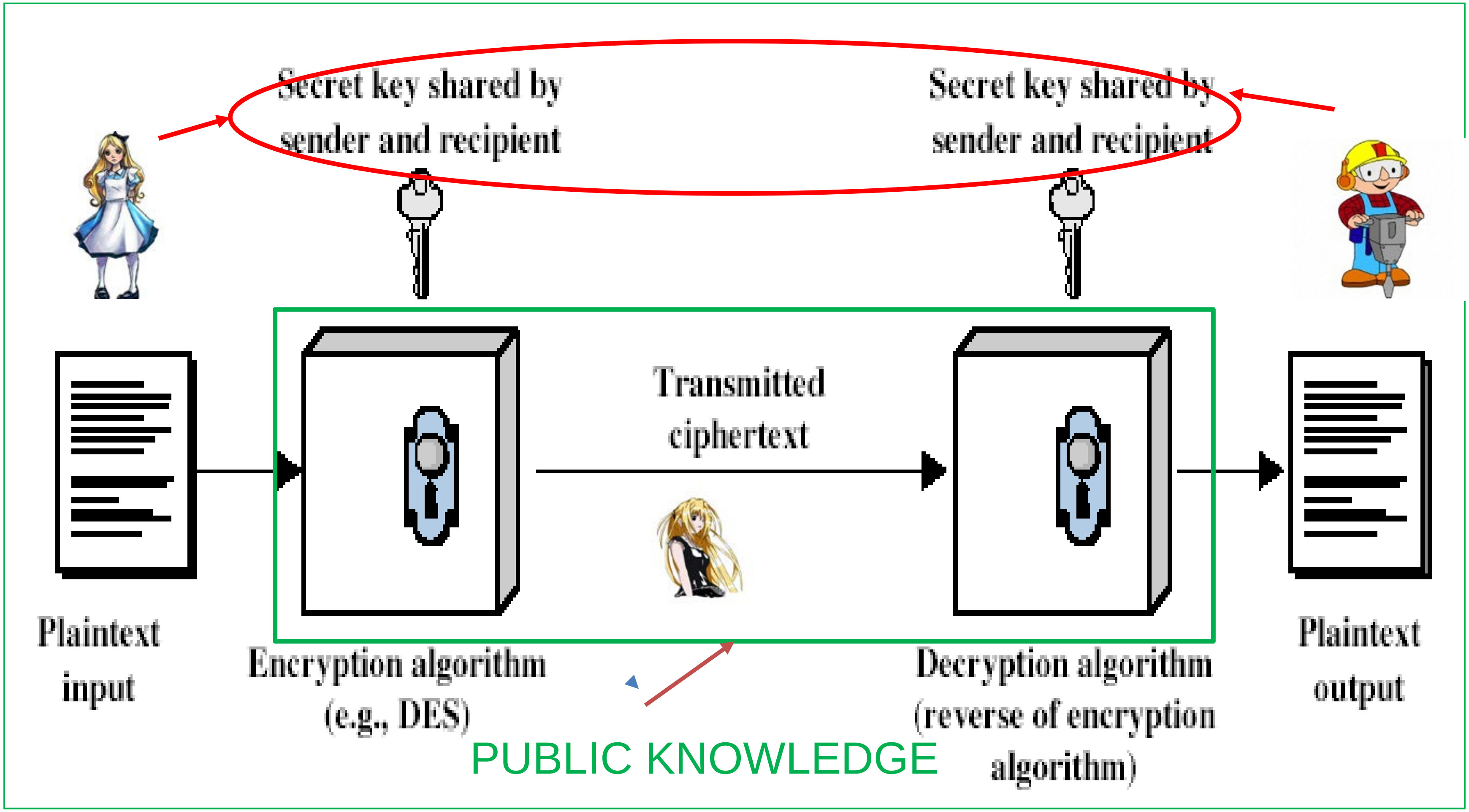
1.4 Modes of Block Ciphers

- Codebook Mode
- Cipher Block Chain
- Stream Cipher modes

Udaya Parampalli

Recap: Symmetric Key Cyptosystems

Modified From:Stallings Figure 2.1:



Recap (Week 2)

- 1.1 Symmetric Cipher Models
- Basic Terminology
- Model and Logical View
- Basic Requirements and Kerckhoffs'sprinciple

- 1.2 Security
  - Characterization of Symmetric key Encryption
  - Attacks on Symmetric key Encryption

- 1.3 Classical Ciphers
  - Substitution CiphersCaesar and Affine Ciphers
  - Monoalphabetic Substitution Ciphers

  - Transposition CiphersRail fence cipher
  - Row Transposition Cipher

- 1.4 Cryptanalysis of Classical Ciphers
  - Caesar Cipher
  - Affine Cipher
  - Monoalphabetic Substitution Ciphers

- 1.5 Complex Ciphers
- Polyalphabetic CiphersVigenèreCipher

Numbers, gcd, primes,
Extended GCD algorithm
Inverse mod n
Euler Phi function

Udaya Parampalli

1.1 Modern Symmetric Ciphers

COMP90043

Lecture 1

Udaya Parampalli

Design Principles

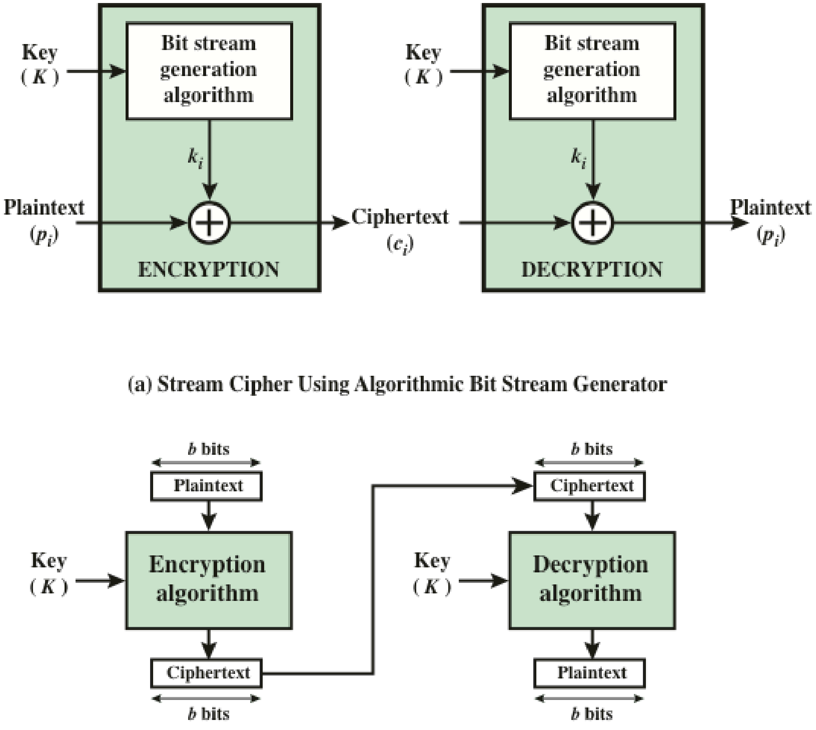
- These are two major kinds of ciphers, which differ in the way the plaintexts are encrypted.

- **Block Cipher**: A block cipher takes a fixed length plain text message block (for example, 64 or 128 bits) and a key, and produces a cipher text block of the same length as the original message.
  - DES (56), Triple-DES (168), IDEA (128), Blowfish() and AES (128)

- **Stream Cipher**: Takes a key of fixed size and generates a key stream in a pseudo random fashion with large period; this key stream is then combined with the plain text message stream on a bit by bit basis to form a cipher text stream.

  - RC4, A5, BlueTooth cipher etc.

Stream and Block Ciphers



(a) Stream Cipher Using Algorithmic Bit Stream Generator

(b) Block Cipher

Figure 4.1 Stream Cipher and Block Cipher

From:Stallings Figure 4.1:

- Unit of stream operation can be “bit by bit” or “byte by byte” or “symbol by smbol”, it encrypts one unit of plain text stream at a time. Useful for processing stream-based data such as voice, connection-oriented traffic etc.

- Unit of operation is always of block of information, generally n-bit blocks. Useful in many situations of data traffic.

.

1.2 One Time Pad Encryption

COMP90043

Lecture 1

Vernam Cipher

- We looked at Vegenere Cipher, a simple polyalphabetic substitution cipher.
- ith plaintext symbol is handled by Caesar cipher with key: $k_{(i \bmod d)}$

- The idea is very simple, a key is a multiple letter word: $K = k_1\ k_2 \ldots k_d$
- $P = p_1\ p_2 \ldots p_d\ p_{d+1}\ p_{d+2} \ldots p_{2d} \ldots$
- $C = c_1\ c_2 \ldots c_d\ c_{d+1}\ c_{d+2} \ldots c_{2d} \ldots$
- Encryption: E(K,P) = C, where $c_i = p_i + k_i \bmod 26$
- Decrypton: D(K,C) = P, where $p_i = c_i - k_i \bmod 26$
- Here we extend the size of the key to be equal to the message (d = n). The resulting cipher is Vernam.
- The scheme can be defined over any alphabet (mod m).
- It is also called as One-Time-Pad.

One-Time Pad Definition

- Defined over binary messages.
- Let ⊕ denote exclusive or symbol. Let [0,1] be binary alphabet.
  - $0 \oplus 0 = 1 \oplus 1 = 0;$
  - $0 \oplus 1 = 1 \oplus 0 = 1.$
- We will extend the operation naturally (point wise) to any sequence over [0.1].
- If A, B, C are vectors, is point-wise vector XOR then

  $A \oplus B = C$; then $B = A \oplus C$; $A \oplus A = 0$; $B \oplus B = 0$, $C+C= 0$
- Suppose Alice wishes to send a message   M = 0110111 to Bob and they have previously established a shared secret key:K =1011011.
  The cipher text is formed by exclusive-oring the message with the key:

  $$C = M \oplus K = 1101100.$$

  Decryption is trivial: the message could be obtained by the same process, i.e. by addition of K to C.

  $$M = C \oplus K = 0110111.$$

One-Time Pad Properties

- An extension of Vernam Cipher for binary messages.
- Here the key is as long as the message.
- For each message you need a distinct random key.
- Encryption and Decryption operation are exactly same, XOR with the key.

Perfect Secrecy

- What does it mean for an encryption scheme to be perfectly secure?

- Let us look at the approach taken by Shannon to answer this question.

- An encryption scheme has the property of **unconditional security** if the cipher text generated by the algorithm does not reveal sufficient information to break the scheme, even with access to an unlimited amount of computational power.
- In other words, the adversary cannot not obtain any knowledge to reverse the encryption by watching any amount of cipher text without access to the key. Shannon in his seminal paper* in 1949 showed that one-time pad encryption is perfectly secure.

* C.E. Shannon. Communication in presence of noise. IEEE, 37:10{21, 1949.

Probability Basics

- Let S be a sample of space of events.
- $S = \{x_1, x_2, x_3, \ldots, x_n\}$
- An event A is a subset of S, probability of A satisfies:
- $0 \leq P(A) \leq 1.$
- $P(S) = 1$, $P(\emptyset) = 0$.
- If $E \subset F$, $E, F \in S$, then $P(E) \leq P(F)$
- $P(E) + P(E^c) = 1$, where $E^c = S \setminus E$.

- Conditional Probability: If $A, B \in S$ are any events in S and $P(B) = 0$, then the conditional probability relative to the event B is given by
- $P(A \mid B) = P(A \cap B) / P(B)$

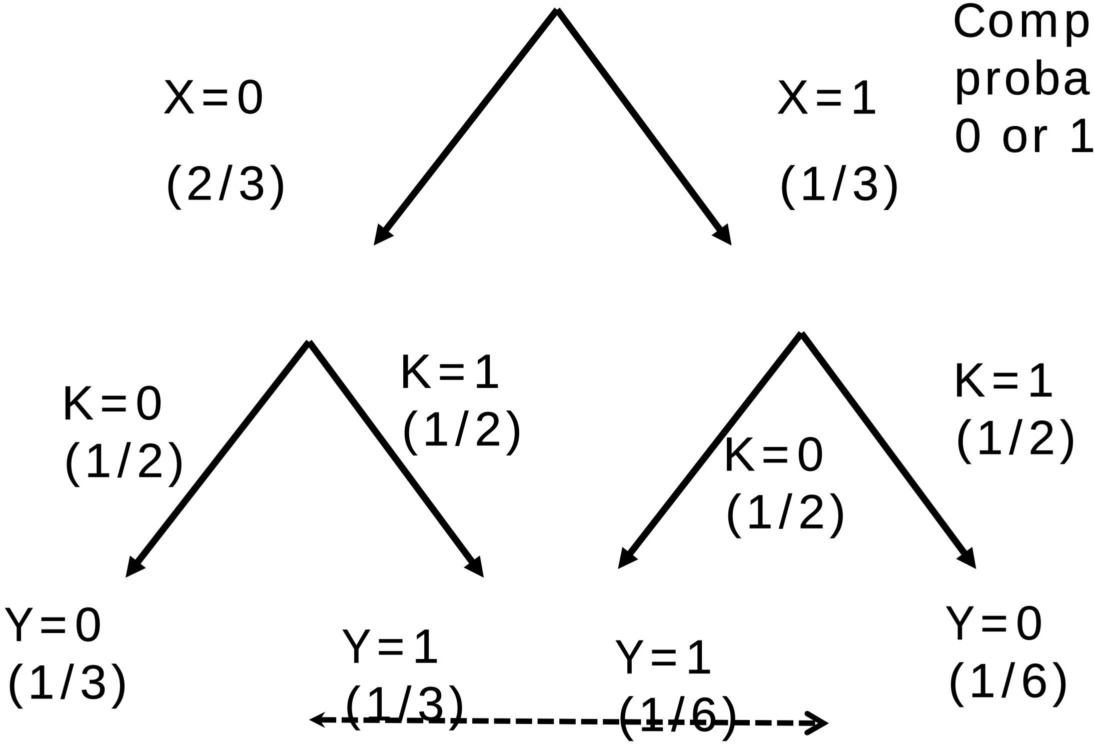
Perfect Secrecy

- Let x: input, y: output
- Perfect Security implies: $P_{X|Y}(x|y) = P_X(x)$
- The one-time pad offers perfect secrecy. Let us make it more precise what this means.
- Let us assume that the message space is binary (0 or 1) and key space is also binary. Assume that A chooses message 0 quarter of the time, i.e Probability that the message is 0 is equal to 1/4, P(M=0) = 1/4.
  Perfect secrecy means knowing this fact, any adversary (E) should not get more information by observing the cipher message ($C = M \oplus K$).
  i.e. The condition probability, P(M = 0 | C =1) should not be different from apriori probability P(M=0).
- This means that seeing the cipher text C does not increase the adversary's knowledge about the message

Another example

- Let message space be 0 or 1, i.e X = 0 or 1.
- Assume that the Adversary a priori knows that probability that (X = 0) is 2/3.
- i.e, P(X=0) = 2/3, then P(X=1)= 1/3.
- Suppose Y =1 was observed at the output of the cipher.
- We want to prove P(X=0|Y=1) = P(X=0).
- **This equivalent to : Seeing the cipher text does not increase the adversaries knowledge about the underlying message**.

Graph of one bit encryption



X=0

(2/3)

X=1

(1/3)

Computation of probabilities: message is 0 or 1

K=0
(1/2)

K=1
(1/2)

K=0
(1/2)

K=1
(1/2)

Key is chosen randomly

Y=0
(1/3)

Y=1
(1/3)

Y=1
(1/6)

Y=0
(1/6)

P(Y=1)= 1/3+1/6=1/2

$$P(X=0|Y=1) = P(X=0 \ \Lambda \ Y=1) / \ P(Y=1) \ = ((2/3)(1/2)) / (1/2) = 2/3 = P(X=0)$$

General Result

- When X and Y are long sequences of 1’s and 0’s of length n.
- Theorem: $P(X=m|Y=c)= P(X=m)$.
- Proof depends critically on the fact that K is generated according to uniform distribution,
- i.e, $P(K=k_1) =1/2^n$,

Implications

- In practice, messages may be biased; could be observed by the adversaries.
- Requirement: Encryption transformation should distribute messages to cipher space fairly uniformly irrespective of known apriory statistics of the messages.
- One-time pad analysis tells us that if we choose a random secret key pad at least the size as the message, we can achieve the perfect secrecy.
- Basically, the random key, which is as long as the message, hides the message completely leading to the perfect “confusion” to the adversary by perfectly “diffusing” the statistical structure of the plain text to the entire ciphertext.
- However, one-time pad is not practical.

Two-time pad is Dangerous

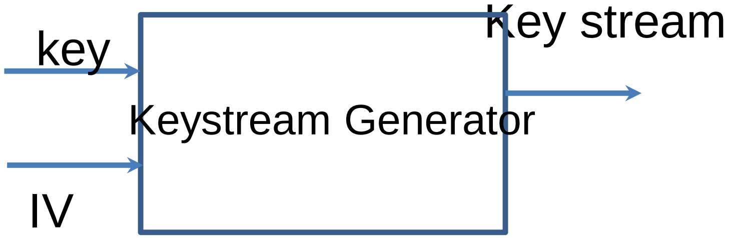
- One-time pad is not practical. It demands a key as long as the message.
- What happens if we reuse the one-time pad used in the encryption?
- $C_1 = M_1 \oplus K$; $C_2 = M_2 \oplus K$; then
- $C_1 \oplus C_2 = M_1 \oplus M_2 \oplus K \oplus K = M_1 \oplus M_2$.
- Even though $M_1 \oplus M_2$ may not direct meaning, it still leaks information about both M_1 and M_2 . Also, in a cryptanalysis setting if one of the messages M_1 or M_2 is available to the adversary, then he/she can get the other.
- This attack implies that you need a new key for every message.
- The idea is used in attacking Vegenere cipher (same key-pad is added many times).
- This type of analysis helped Allied in World Wars in 20th Century. Germans made this mistake in the war times!. Turing led Allied team made use of such vulnerability during initial key broadcast by Germans, which eventually helped to crack the master key used for the day.

Stream Ciphers

- How to we define a practically useful One-Time pads?

- An idea is to generate a long stream based on a short key and use it as a keystream in One-Time pad scheme. The resulting cipher is “stream Cipher”.

- Stream cipher in general takes a key and a random nonce (Initial Vector(IV))as input and outputs a keystream of arbitrary size. The keystream is then xored with the plaintext to obtain a ciphertext.

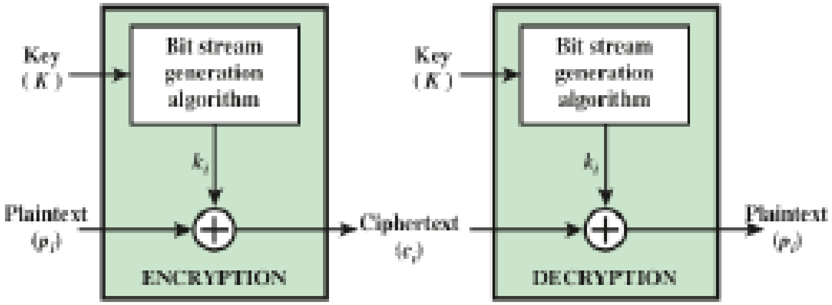


key

IV

Keystream Generator

Key stream



Modified From:Stallings Figure 4.1a:

Modern Stream Ciphers

- Stream ciphers are extensively employed in modern communication networks.
- They are of the algorithm of choice in Light Weight Cryptographic applications.
- eSTREAM: ECRYPT Stream Cipher Project: An European stream cipher project in the last decade gave impetus to the development of the subject.
- They are every where: BlueTooth, Phones, browsers etc.
- We will revisit this idea when we study Block Ciphers in Stream Cipher mode.

1.3 Modern Block Ciphers

COMP90043

Lecture 1

Block Ciphers

- Encrypts blocks of n characters/bits of plain text simultaneously outputting blocks of cipher texts.
- Same key is used for many different message blocks.
- Fundamental building blocks for many cryptographical functions.
- Examples include hash functions, preudorandom generators, message authentication codes etc.
- **Confusion and diffusion principles:**
- **Diffusion** dissipates statistical structure of plaintext over bulk of ciphertext.
- **Confusion** makes relationship between ciphertext and key as complex as possible.
- Generally diffusion is created by permutations and confusion is created by substitution.

Product Ciphers and Fiestel Ciphers

- A **product cipher** combines two or more transformations so that resulting cipher is more secure than the individual components by making use of confusion and diffusion principles.
- A **substitution-permutation cipher** is a product cipher made up of number of stages each involving substitution and permutation. The operations of substitution and permutation are responsible for effecting the confusion and diffusion respectively.
- An **iterated block cipher** is a block cipher involving sequential repetition of an iterated function called a round function.
- The parameters of iterated block ciphers are r: number of rounds; n: block length; k: bit-size of key, K from which r subkeys (round keys) k_i's are derived.
- **Fiestel Cipher** is an example of an iterated block cipher.

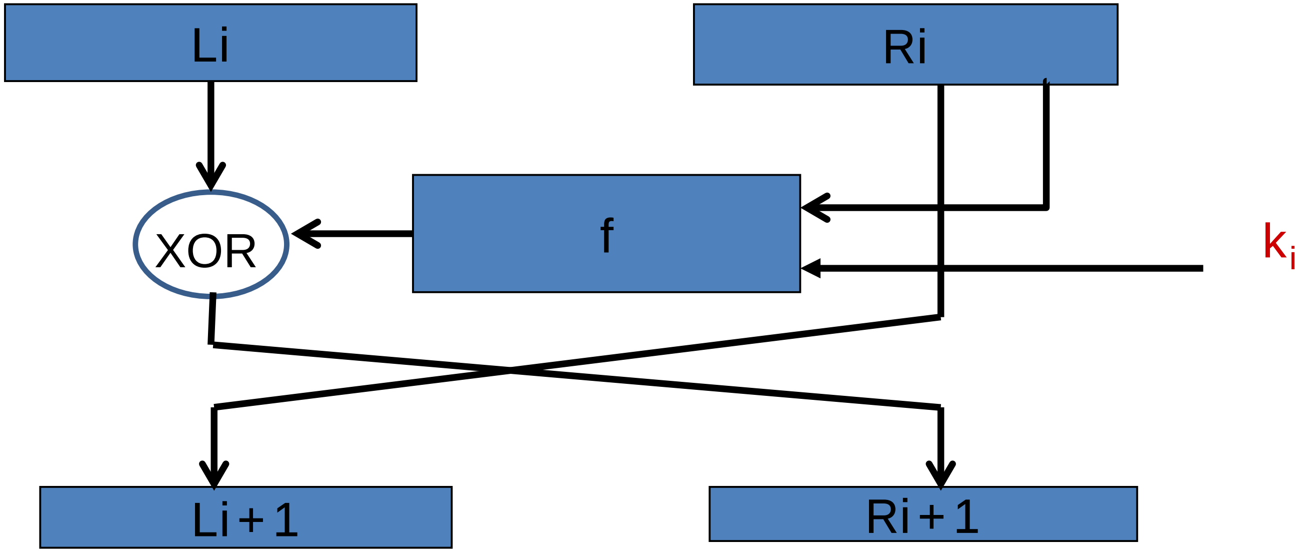
Fiestel Block Cipher

- **Fiestel** ciphers are iterative ciphers; they repeat a given operation several times in rounds.
- Each round will have the following distinct operations:
- **Substitution**: Each plaintext bit or group of bits in a block are replaced with a corresponding cipher text bit or group of bits.
- **Permutation**: A certain perimutation is effected to each transformed ciphertext bits.
- The above round operations are repeated certain number of rounds.

Fiestel Block Cipher, cont.

For such a cipher, the input key is used to produce round keys $k_1, k_2, \ldots, k_r$. The message is initially divided into two parts, namely left and right halves, L and R.

For each of r rounds, the following operations are executed.



After r rounds, the final left and right haves are swapped and concatenated to form the cipher text.

The design of a good function f is partly ``ART'' and partly ``SCIENCE''.

Data Encryption Standard (DES)

- IBM's 1974 submission for a standard.
  A Fiestel cipher
  Block size: n = 64,
  keysize = k = 56 bits.

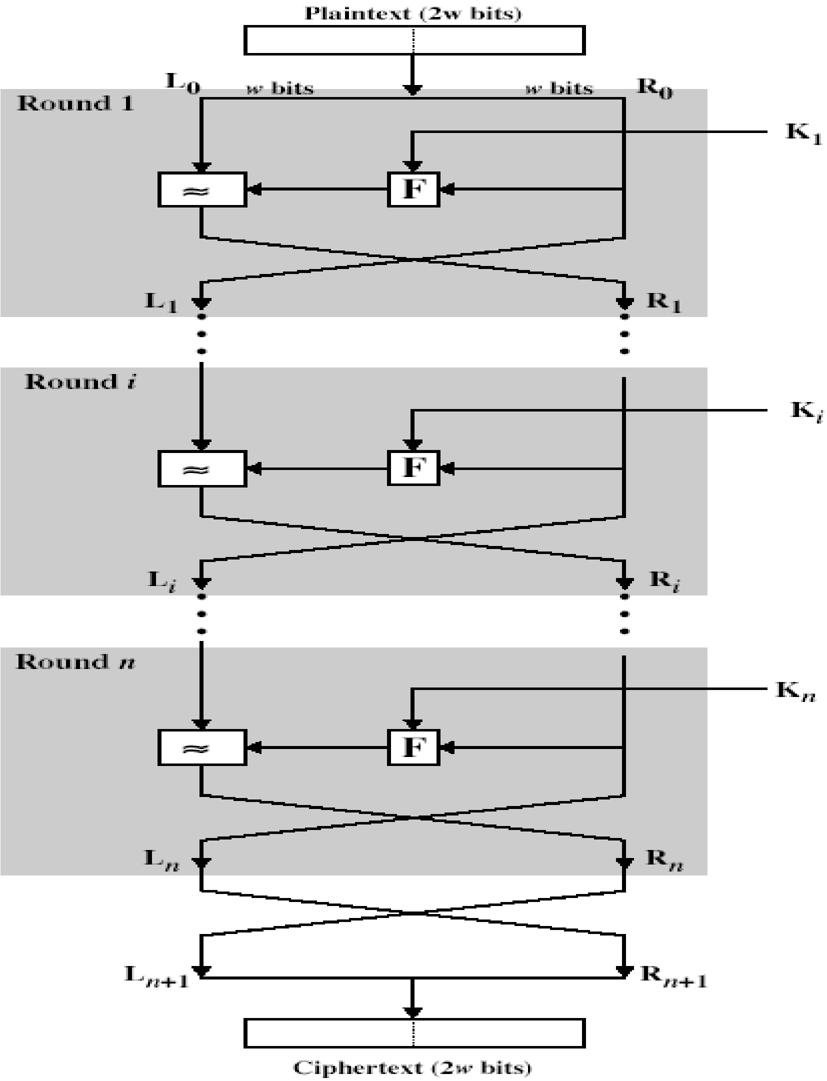
  The key is specified with 64 bits containing 8 bits of parity.
  Number of rounds = 16.

  Strengthening DES:
  DESX: Apart from 56 bit key K, choose two new 64 bit keys K_I and K_O, then we encrypt

  $C = K\_O \oplus DES(K, M \oplus K\_I)$

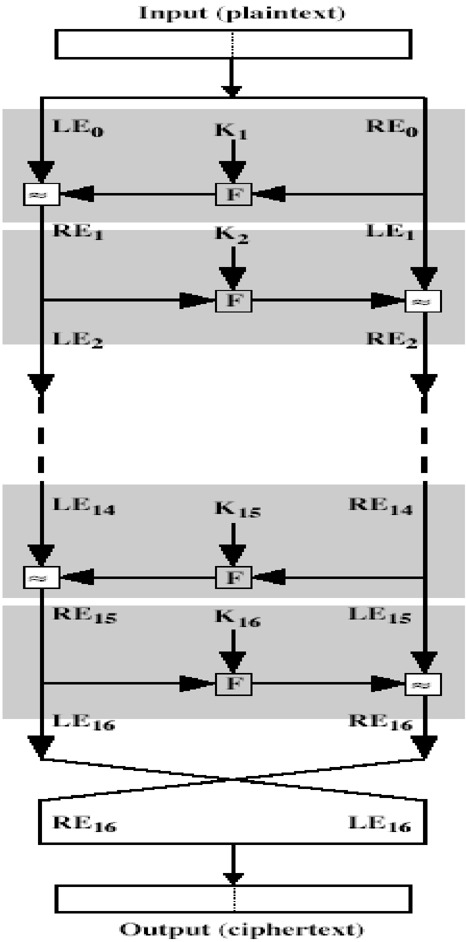
  This method increases effective key length to 199-t, where t is a quantity related to adversaries' cryptanalytic assumptions where the adversary is able to collect 2^t matching input-output pairs.
- Read the textbook for more details on DES.

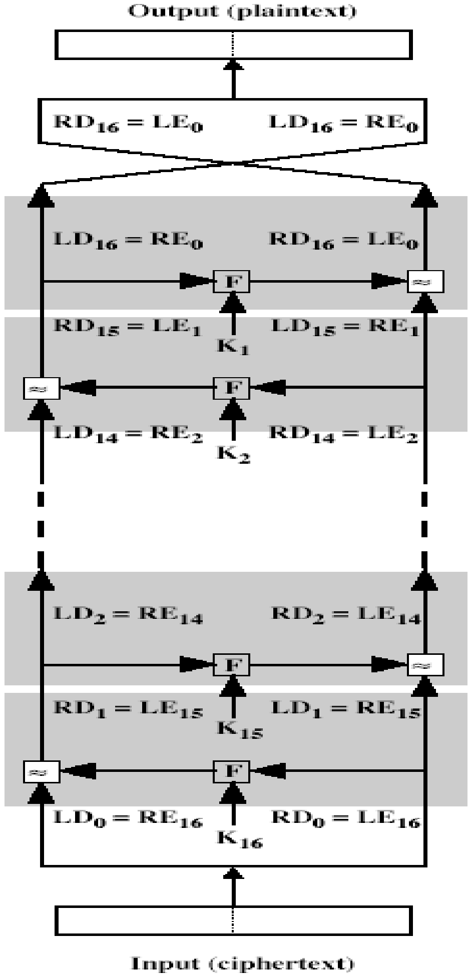
Feistel Cipher Structure



From:William Stallings 5th Edition:

Feistel Cipher Decryption





From:William Stallings 5th Edition:

Strengths, properties and attacks on DES

- Each bit of cipher text depends on all bits of the key and all bits of the plain text.
- No statistical relationship between plain and cipher visible.
- Altering a key bit or a plain text bit should alter each cipher bit with probability close to half.
- Altering a cipher bit should result in unpredictable change in plain text block.

Cryptanalysis of DES

- Empirically it is found that DES is safe.

- Exhaustive search -- Brute force. 2^{56} computations.

Differential cryptanalysis

- Chosen plain text attack,

- Not realistic -complexity 2^{47} computations.

Linear cryptanalysis

- Complexity : 2^{43} computations.
- The main drawback is limited key space.

- The new standard for encryption now is AES which has key space >= 2^{128}.

Advanced Encryption Standard (AES)

- DES is not recommended as it has small key space and have known theoretical attacks.
- Financial Systems still use a modification of DES such as Triple-DES, which also has significant drawbacks (Slow and have small block size)
- So, NIST worked with crypto community to develop to develop an Advanced Encryption Standard (AES) in 1997.
- In October 2000, NIST accepted Rijndael as the AES in Oct-2000.
- It is proposed by cryptographic researchers: Dr. Joan Daemen and Dr.Vincent Rijmen.

AES Algorithm

- Stallings discusses AES algorithm in detail.
- It is not a Fiestel cipher, but still iterative.
- Main design requirements:
  - Should withstand all known attacks
  - It should have flexible implementation, to be able to run on varieties of platforms and CPUs.
  - It should have a simple design features.

How do you make Encryption more complex?

- One can increase block size n and also look for different functions for encryption.
- In practice, data comes in many forms. W ecan modify the function for different modes.
- These practical modes are developed by people working on using encryption. More on Chapter 7 of the textbook

1.4 Modes of Block Ciphers

COMP90043

Lecture 1

Udaya Parampalli

Modes of Operations

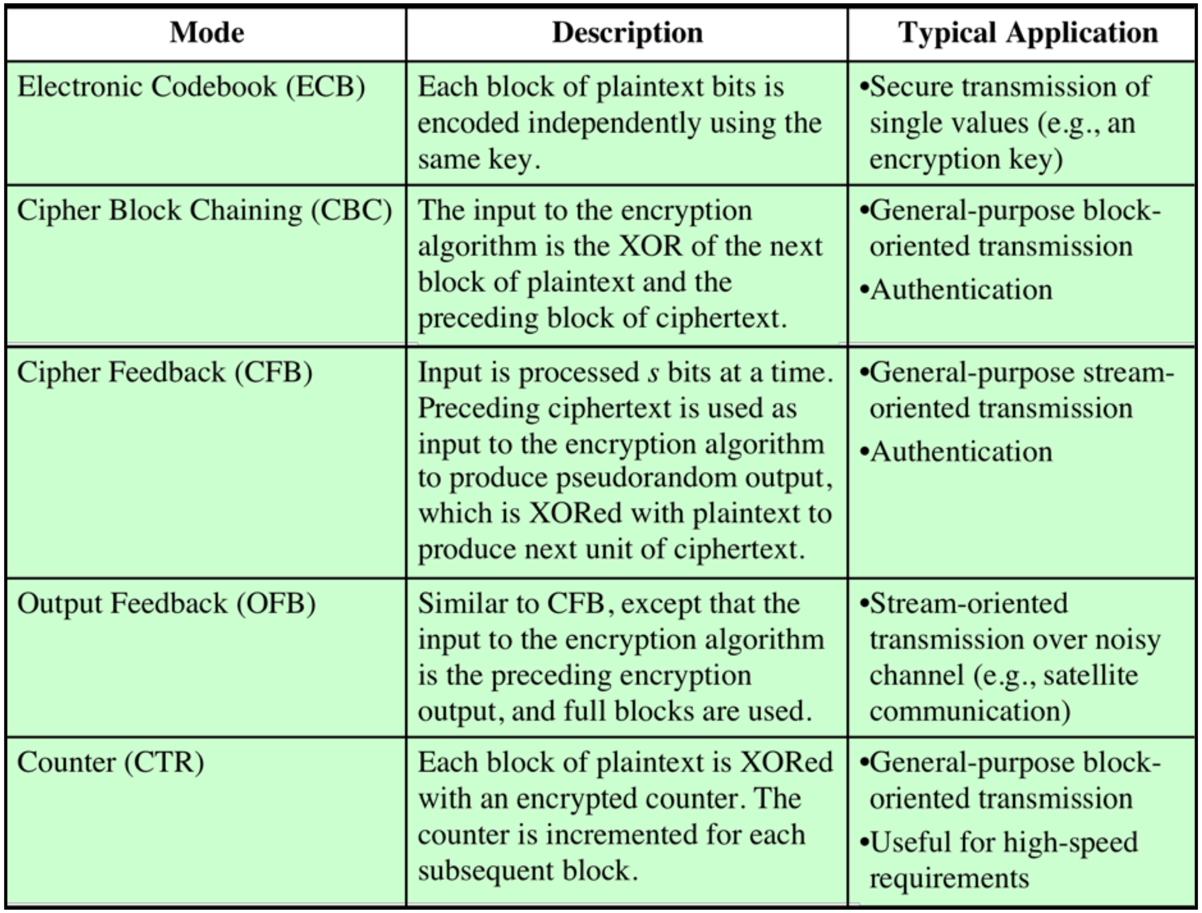
- NIST defined five basic modes of usage of block cipher.
- They are generic: can be use with any block cipher.
- Five modes:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

Uses both Encrypt and Decrypt functions

Uses only Encrypt functions

Used like a stream cipher

Mode of Operations



Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

From:Stallings Table 7.1:

You will learn more from the textbook.

Week 3

Lecture 1

Modern Symmetric key Ciphers

Lecture 2

Finite Field mathematics,

Workshop 3: Workshop based on Lectures in Week2

Quiz 3