German University in Cairo
Faculty of Media Engineering and Technology
Mervat Abu-Elkheir
Mohamed Abdelrazik
Ahmad Helmy

CSEN1001: Computer and Network Security

Spring Term 2019

Tutorial 3

Combination and Permutation

Link for an online tutorial:
http://www.mathsisfun.com/combinatorics/combinations-permutations.html

Problem 1 - Permutation without Repetition

There are 5 seats around a table and 5 people to be seated at the table. In how many ways can they seat themselves?

Answer

Sitting 5 people at the table is a sequential problem. Assigning the first person to the first chair, there are 5 possible ways to do this. Then assigning a person to the second chair, there are 4 possible ways to do this, because one person has already been assigned. And so on, until there remains one free chair and one person to be seated. Therefore, the number of ways to seat the 5 people at the table is equal to the number of permutations of 5 objects (without repetition). If we denote it by P_5, then:

$$P_5 = 5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$$

Problem 2 - Permutation with Repetition

A byte is a number consisting of 8 bits that can be equal either to 0 or to 1. How many different permutations of a byte are there?

Answer

Each bit in a byte could be zero or one, i.e. there are 2 options for each bit. Therefore, the number of ways to choose the 8 digits is equal to:

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8 = 256$$

Problem 3 - Confusion and Diffusion

In modern encryption techniques, what is the difference between confusion and diffusion?

Answer

- Diffusion: dissipating the statistical structure of plaintext over bulk of cipher text (relationship between letters of text).

- Confusion: making the relationship between plaintext and cipher text as complex as possible.

Problem 4

Given the following ciphers, do they have the properties of diffusion?

a) Vigenère Cipher

b) A cipher that was able to encrypt AJKOW to NFJPX and ABKOW to KSIMY using the same key.

Answer

a) The Vigenère cipher is a stream cipher, in order for diffusion to happen we must have some sort of transpositions/permutations. Therefore, only a block cipher can have the two properties.

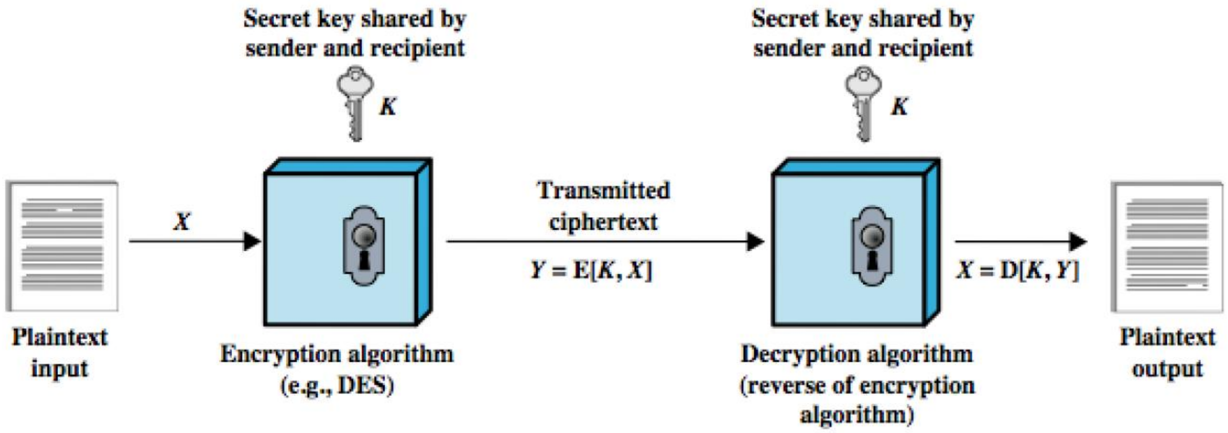
b) It should be noted that by changing a single symbol (in this case the J was replaced by B), the resulting cipher was dramatically different, therefore diffusion occurred here. However, there's a clear relation between the ciphertext and the plaintext, this relation makes the confusion property unsatisfied.

Problem 5 - Symmetric Cryptography

Illustrate with a figure what is meant by symmetric cryptography.

Answer

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text.

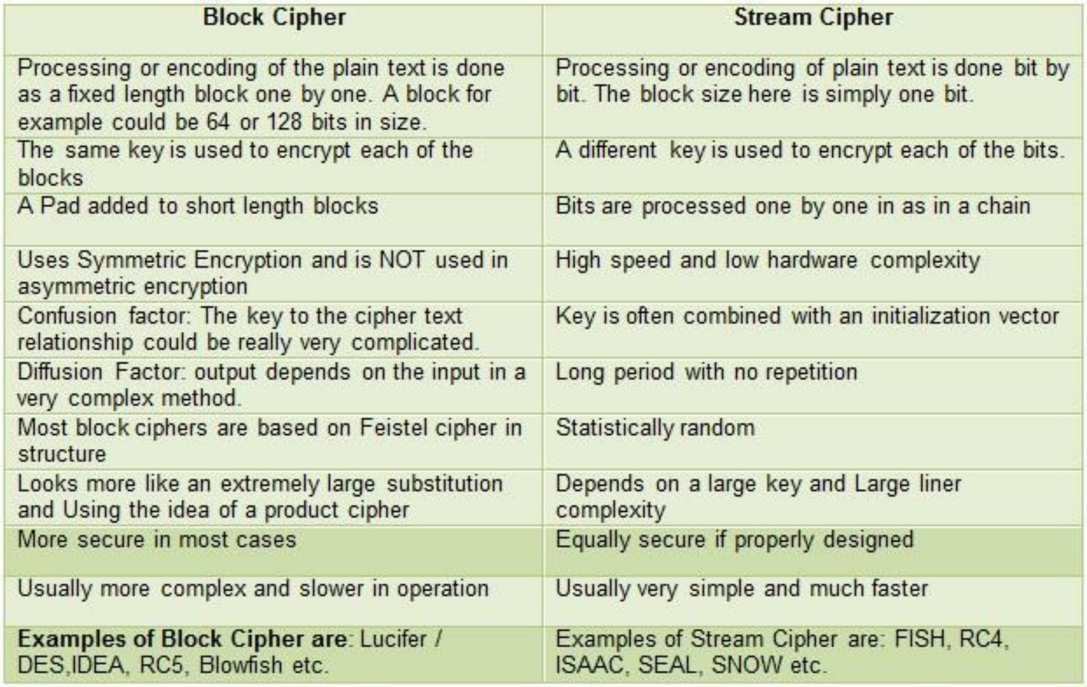

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Problem 6 - Block and Stream Ciphers

Compare between block cipher and stream cipher.

Answer

Below are the key comparison and differences between Block Cipher and Stream Cipher in a tabular form that makes it easier to remember, compare and understand.



Block Cipher	Stream Cipher
Processing or encoding of the plain text is done as a fixed length block one by one. A block for example could be 64 or 128 bits in size.	Processing or encoding of plain text is done bit by bit. The block size here is simply one bit.
The same key is used to encrypt each of the blocks	A different key is used to encrypt each of the bits.
A Pad added to short length blocks	Bits are processed one by one in as in a chain
Uses Symmetric Encryption and is NOT used in asymmetric encryption	High speed and low hardware complexity
Confusion factor: The key to the cipher text relationship could be really very complicated.	Key is often combined with an initialization vector
Diffusion Factor: output depends on the input in a very complex method.	Long period with no repetition
Most block ciphers are based on Feistel cipher in structure	Statistically random
Looks more like an extremely large substitution and Using the idea of a product cipher	Depends on a large key and Large liner complexity
More secure in most cases	Equally secure if properly designed
Usually more complex and slower in operation	Usually very simple and much faster
Examples of Block Cipher are: Lucifer / DES,IDEA, RC5, Blowfish etc.	Examples of Stream Cipher are: FISH, RC4, ISAAC, SEAL, SNOW etc.

Problem 7

What is meant by S-box?

Answer

S-box stands for Substitution box. "In general, an S-box takes some number of input bits, m, and transforms them into some number of output bits, n, where n is not necessarily equal to m." quoted from http://en.wikipedia.org/wiki/S-box