CHAPTER II ENCRYPTION

Learning Outcor..es:

At the end of the lesson, you are expected to:

1. Discuss the brief history of Encryption
2. Define Encryption
3. List the different application of Encryption
4. Define and simulate Conventional Encryption
5. Differentiate Cryptography and Cryptanalysis
6. Enumerate type of attack on encrypted message
7. Discuss Steganography
8. Identify and explain the different steganography technique
9. Differentiate Substitution and Transposition Technique
10. List and Describe Classical Encryption Technique
11. Simulate the steps involve Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher.
12. Explain Modern Encryption Technique.
13. Define Block Cipher
14. Compare and contrast Stream cipher and Block Cipher

Learning Content:

2.1. Brief History of Encryption
2.2. Conventional Encryption
- Steganography
- Classical Encryption Techniques
2.3 Modern Encryption Techniques
- Symmetric Block Cipher
- DES (Data Encryption Standard)

Start your lesson here.

2.1. HISTORY OF CRYPTOGRAPHY

The word cryptography stems from the two Greek words “Krypto’s and grafein” meaning “hidden” and “to write” respectively. Indeed, the most basic cryptographic problem, which dates back millennia, considers the task of using “hidden writing” to secure, or conceal communication between two parties [1]. Cryptography, the use of codes and ciphers to protect confidential data, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption [2].

The development of cryptography has been paralleled by the development of cryptanalysis — the "breaking" of codes and ciphers”. Until the 1960s, secure cryptography was largely the preserve of governments.

Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to the original form through decryption. In general, the longer the key is, the more difficult it is to crack the code. This holds true because deciphering an encrypted message by brute force would require the attacker to try every possible key. To put this in context, each binary unit of information, or bit, has a value of 0 or 1. An 8-bit key would then have 256 or 2^8 possible keys. A 56-bit key would have 2^56, or 72 quadrillion, possible keys to try and decipher the message. With modern technology, cyphers using keys with these lengths are becoming easier to decipher. DES, an early US Government approved cypher, has an effective key length of 56 bits, and test messages using that cypher have been broken by brute force key search. However, as technology advances, so does the quality of encryption. Since World War II, one of the most notable advances in the study of cryptography is the introduction of the asymmetric key cyphers (sometimes termed public-key cyphers). These are algorithms which use two mathematically related keys for encryption of the same message. Some of these algorithms permit publication of one of the keys, due to it being extremely difficult to determine one key simply from knowledge of the other.

Beginning around 1990, the use of the Internet for commercial purposes and the introduction of commercial transactions over the Internet called for a widespread standard for encryption. Before the introduction of the Advanced Encryption Standard (AES), information sent over the Internet, such as financial data, was encrypted if at all, most commonly using the Data Encryption Standard (DES). This had been approved by NBS (a US Government agency) for its security, after public call for, and a competition among, candidates for such a cypher algorithm. DES was approved for a short period, but saw extended use due to complex wrangles over the use by the public of high-quality encryption. DES was finally replaced by the AES after another public competition organized by the NBS successor agency, NIST. Around the late 1990s to early 2000s, the use of public-key algorithms became a more common approach for encryption, and soon a hybrid of the two schemes became the most accepted way for e-commerce operations to proceed.

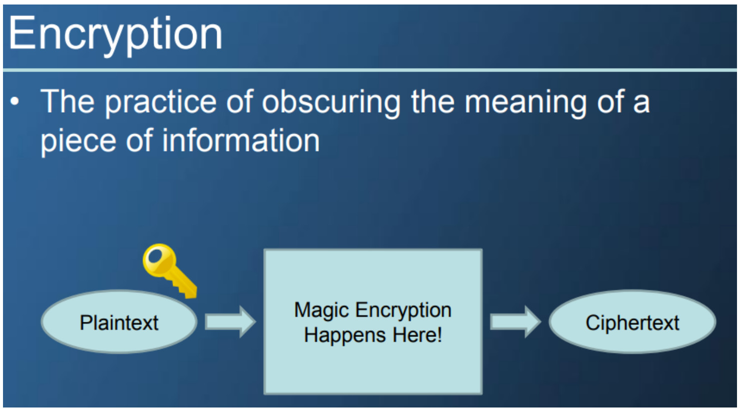
Additionally, the creation of a new protocol known as the Secure Socket Layer, or SSL, led the way for online transactions to take place. Transactions ranging from purchasing goods to online bill pay and banking used SSL. Furthermore, as wireless Internet connections became more common among households, the need for encryption grew, as a level of security was needed in these everyday situations.

Claude E. Shannon is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs, and during his time there, he produced an article entitled "A mathematical theory of cryptography". This article was written in 1945 and eventually was published in the Bell System Technical Journal in 1949. It is commonly accepted that this paper was the starting point for development of modern cryptography. Shannon was inspired during the war to address the problems of cryptography [because] secrecy systems furnish an interesting application of communication theory". Shannon identified the two main goals of cryptography: secrecy and authenticity. His focus was on exploring secrecy and thirty-five years later, G.J. Simmons would address the issue of authenticity. Shannon wrote a further article entitled "A mathematical theory of communication" which highlights one of the most significant aspects of his work: cryptography's transition from art to science.

In his works, Shannon described the two basic types of systems for secrecy. The first are those designed with the intent to protect against hackers and attackers who have infinite resources with which to decode a message (theoretical secrecy, now unconditional security), and the second are those designed to protect against hackers and attacks with finite resources with which to decode a message (practical secrecy, now computational security) [1].

ENCRYPTION

ENCRYPTION is defined as the process of hiding by converting the information or data into unreadable form or a code with the aim to prevent unauthorized access. The illustration on figure below shows how encryption process is conducted [4].



Encryption

- The practice of obscuring the meaning of a piece of information

Plaintext

Magic Encryption Happens Here!

Ciphertext

Figure 1. Encryption Process

Consider two parties, Alice and Bob. Alice wants to privately send messages (called plaintexts) to Bob over an insecure channel. By an insecure channel, we here refer to an "open" and tappable channel; in particular, Alice and Bob would like their privacy to be maintained even in face of an adversary Eve (for eavesdropper) who listens to all messages sent on the channel. How can this be achieved?

Additional Information:

Plaintext: With the advent of computing, the term *plaintext* expanded beyond human-readable documents to mean any data, including binary files, in a form that can be viewed or used without requiring a key or other decryption device. Information—a message, document, file, etc.—if to be communicated or stored in encrypted form is referred to as plaintext. [Source: https://en.wikipedia.org/wiki/Plaintext]

Ciphertext: In cryptography, **ciphertext** or **cyphertext** is the result of encryption performed on plaintext using an algorithm, called a cipher.[1] Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with codetext because the latter is a result of a code, not a cipher. [Source: https://en.wikipedia.org/wiki/Ciphertext]

A possible solution before starting their communication, Alice and Bob agree on a "secret code" that they will later use to communicate. A secret code consists of a key, an algorithm Enc to encrypt (scramble) plaintext messages into ciphertexts and an algorithm Dec to decrypt (or descramble) ciphertexts into plaintext messages. Both the encryption and decryption algorithms require the key to perform their task. Alice can now use the key to encrypt a message, and then send the ciphertext to Bob. Bob, upon receiving a ciphertext, uses the key to decrypt the ciphertext and retrieve the original message [1].

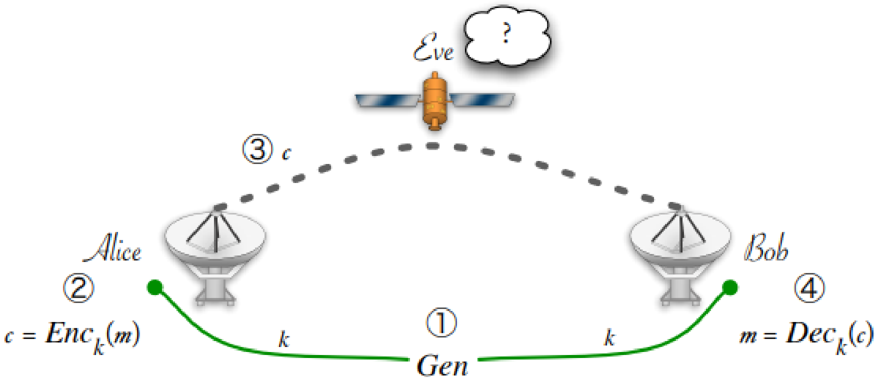


Figure 1. Illustration of the steps involved in private-key encryption

The figure above shows the illustration involved in private-key encryption. First, a key k must be generated by the Gen algorithm and privately given to Alice and Bob. In the picture, this is illustrated with a green "land-line." Later, Alice encodes the message m into a ciphertext c and sends it over the insecure channel—in this case, over the airwaves. Bob receives the encoded message and decodes it using the key k to recover the original message m. The eavesdropper Eve does not learn anything about m except perhaps its length [1].

APPLICATION OF ENCRYPTION

Application of Encryption is a data-security solution that, at the application level, encrypts sensitive data, so only authorized parties can read it. When encryption occurs at this level, data is encrypted across multiple (including disk, file and database) layers. This application layer encryption approach increases security by reducing the number of potential attack vectors. Another advantage to application encryption is that, since it encrypts specific fields at the application layer, organizations can secure sensitive data before storing it in database.

Time Stamping

Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allow the sender to get a message receipted by another party without revealing any information about the message to the other party.

Time stamping is very similar to sending a registered letter through the U.S. mail, but provides an additional level of proof. It can prove that a recipient received a specific document. Possible applications include patent applications, copyright archives, and contracts. Time stamping is a critical application that will help make the transition to electronic legal documents possible.

Electronic Money

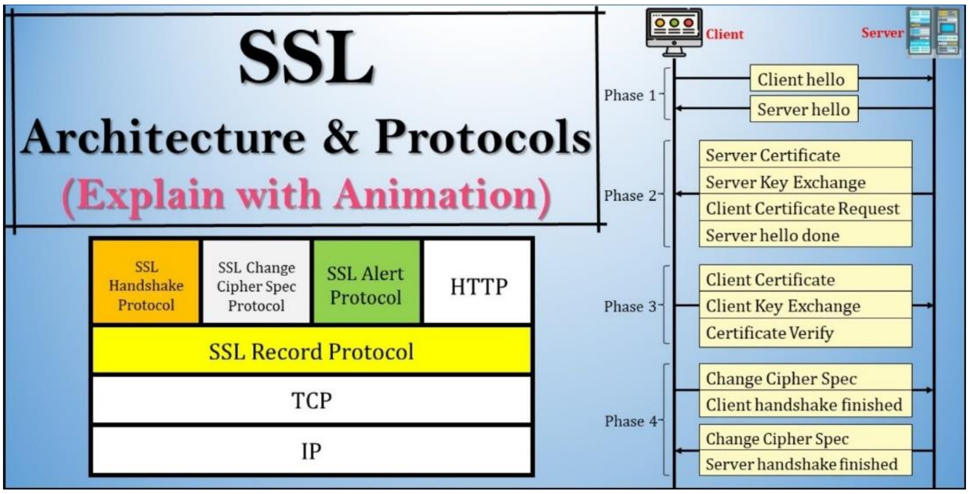
The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving. It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. There are both hardware and software implementations.

Anonymous applications do not reveal the identity of the customer and are based on blind signature schemes. (Digicash's Ecash) Identified spending schemes reveal the identity of the customer and are based on more general forms of signature schemes. Anonymous schemes are the electronic analog of cash, while identified schemes are the electronic analog of a debit or credit card. There are also some hybrid approaches where payments can be anonymous with respect to the merchant but not the bank (CyberCash credit card transactions) ; or anonymous to everyone, but traceable (a sequence of purchases can be related, but not linked directly to the spender's identity).

Encryption is used in electronic money schemes to protect conventional transaction data like account numbers and transaction amounts, digital signatures can replace handwritten signatures or a credit-card authorizations, and public-key encryption can provide confidentiality. There are several systems that cover this range of applications, from transactions mimicking conventional paper transactions with values of several dollars and up, to various micropayment schemes that batch extremely low-cost transactions into amounts that will bear the overhead of encryption and clearing the bank.

Secure Network Communications

Secure Socket Layer (SSL)



Netscape has developed a public-key protocol called Secure Socket Layer (SSL) for providing data security layered between TCP/IP (the foundation of Internet-based communications) and application protocols (such as HTTP, Telnet, NNTP, or FTP). SSL supports data encryption, server authentication, message integrity, and client authentication for TCP/IP connections.

The SSL Handshake Protocol authenticates each end of the connection (server and client), with the second or client authentication being optional. In phase 1, the client requests the server's certificate and its cipher preferences. When the client receives this information, it generates a master key and encrypts it with the server's public key, then sends the encrypted master key to the server. The server decrypts the master key with its private key, then authenticates itself to the client by returning a message encrypted with the master key. Following data is encrypted with keys derived from the master key. Phase 2, client authentication, is optional. The server challenges the client, and the client responds by returning the client's digital signature on the challenge with its public-key certificate [6].

2.2. CONVENTIONAL ENCRYPTION

CONVENTIONAL ENCRYPTION - Conventional encryption, also referred to as symmetric encryption or single-key encryption, was the only types of encryptions in use prior to the development of public key encryption

Symmetric Encryption - is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information.

Conventional Encryption Model

The following figure illustrates the conventional encryption process. The original intelligible message, referred to as plaintext, is converted into apparently random nonsense, referred to as ciphertext, the encryption process consists of an algorithm and a key

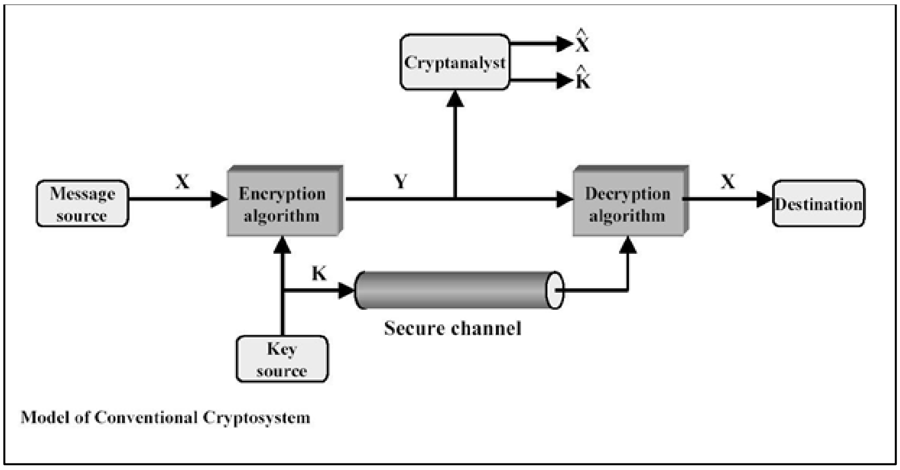


Figure 2. Conventional Encryption Model

Conventional Encryption Model

- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y.
- We can write this as
  - $Y = E_K(X)$
- This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K.
- The intended receiver, in possession of the key, is able to invert the transformation:
  - $X = D_K(Y)$
- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithm.

Cryptography

Cryptographic systems are generally classified along three independent dimensions:

1. The type of operation used for transforming plaintext to ciphertext:

   substitution, transposition

2. The number of keys used:

   one key, two keys

3. The way in which the plaintext is processed:

   block cipher, stream cipher

Cryptanalysis

- The process of attempting to discover X or K or both is known as cryptanalysis
- The strategy used by the cryptanalyst depends on the nature of the encryption scheme and information available to the analyst.

Type of attack on encrypted message

- Ciphertext only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack

STEGANOGRAPHY

A plaintext message is hidden in something.

- **Character marking**
  - Selected letters of printed or type written are over written in pencil.
  - The marks are ordinarily not visible unless the paper held at an angle to bright light.
- **Invisible ink**
- **Pin punctures**
  - Small pin punctures on selected letter are ordinarily not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon**
  - Used between lines typed with a black ribbon, the result of typing with the correction tape are visible only under a strong light

CLASSICAL ENCRYPTION TECHNIQUES

Substitution Techniques

- ◈ A substitution technique is one in which the letters of plaintext are replaced by other letters or by number of symbols.

Youtube Search: **Cryptography 101 – Substitution Ciphers**
Source: https://www.youtube.com/watch?v=1P8Xpxm76e8

Types of Substitution Techniques

1. Caesar Cipher

- ◈ The earliest known use of a substitution cipher, the simplest and also known as "Shift Cipher" that shifts the letters of alphabet against another alphabet to create a secret message. It was named after Julius Caesar, a roman emperor. The substitution technique was used in order to communicate secretly with his army.

- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.
  For example:
  Plaintext: meet me after the party
  Ciphertext: PHHW PH DIWHU WKH SDUWB

Plaintext	m	e	e	t		M	e		a	f	T	E	r		t	h	e		p	a	r	t	Y
Ciphertext	P	H	H	W		P	H		D	I	W	H	U		W	K	H		S	D	U	W	B

Table 1. Ceasar Cipher Substitution

Plain	A	B	C	D	e	f	g	h	i	j	k	l	M	n	o	p	Q	R	S	t	u	v	w	x	y	z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Note that the alphabet is wrapped around, so that the letter following Z is A.

TRY ME! Applying the Ceasar Cipher substitution technique, determine the following hidden message by substituting Ciphertext to plaintext using Table 1.

1. LVX-FFVLFW = __ __ __ - __ __ __ __ __ __

2. VWXGB KDUG = __ __ __ __ __ __ __ __ __

3. NHHS VDIH = __ __ __ __ __ __ __ __

2. Monoalphabetic Cipher

- The Monoalphabetic cipher, can have random value of key space alphabet unlike ceasar cipher, it was fix into three space.
- Monoalphabetic ciphers is a weak cipher and is easy to break because they reflect the frequency data of the original alphabet.

Table 2. Monoalphabetic Cipher

Plain	a	b	C	d	e	f	g	h	i	j	k	l	M	n	o	p	Q	R	S	t	u	v	w	x	y	z
Cipher	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Applying the Monoalphabetic Cipher technique, convert the following plaintext into its Ciphertext using Table 2.

1. LOVE = __ __ __ __

2. FORGIVE = __ __ __ __ __ __ __

3. PEACE = __ __ __ __ __

3. Playfair Cipher

- The best-known multiple-letter encryption cipher is the playfair, which treats diagram in the plaintext as single units and translates these units into cipher diagram.
- The playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword.

Youtube Search: **Playfair Cipher**
Source: https: https://www.youtube.com/watch?v=-KjFbTK1Ilw

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Figure 3. Playfair Cipher

Playfair Cipher Rules:

◈ Plaintext is encrypted **two letters at a time**, according to the following rules:

Rule No.1. Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x and a letter with **no pair** will have a filler of x, so that **BALLOON** would be enciphered as **BA LX OX NX**. The rule is being carefully discussed in details bellow:

Plaintext: BALLOON
Step 1: Divide the plaintext into 2 letters per pair.
BA LL OO N
Step 2: Based on Rule #1, repeating letters on the same pair will have filler of letter "X". On the example, the repeating letters in pair are letters **"L"** and **"O",** while the letter with no pair is the letter **"N".**
BA LL OO N
BA L**X** O**X** N**X**

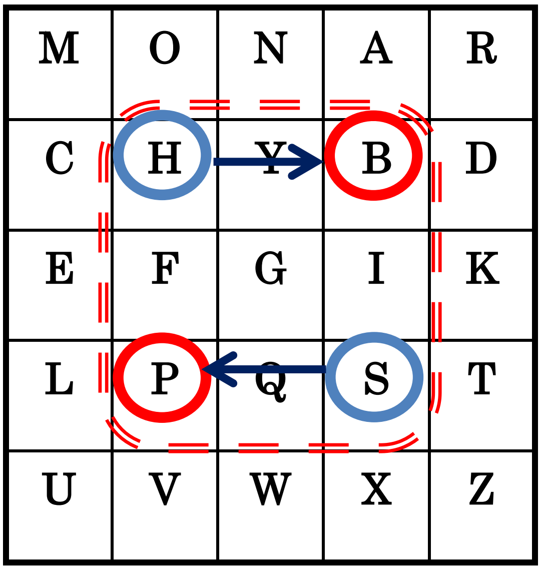
Rule No. 2. (Rules on the same ROW). Plaintext letters that fall in the same row of the matrix are replaced by the letter to the right. For example, letters **"MN"** is encrypted as **"OA".** Moreover, the letter that falls on the last column of the row of the matrix will be replaced by wrapping around on the same row. For letters "**AR",** is encrypted **"RM".**

Example no. 1: Proceed to Figure 3 and **locate** for letter **M** and **N.** Following the rule number 2, the letters are replaced with the letter to the right. The letter to the right M is O, and the letter to the right of N is A. Such that MN = OA.

Example no. 2: To find the value of **"AR"** based on figure 3. The letter to the right of **"A"** is replaced with letter **"R",** while letter **"R"** is replaced by wrapping around the row with letter **"M".** Such that AR = RM.

Rule No. 3. (Rules on the same COLUMN). Plaintext letters that fall in the same column are replaced by the letter beneath/ below. For example, letters **"YQ"** is encrypted as **"GW".** Moreover, the letter that falls on the last row of the column of the matrix will be replaced by wrapping around on the same column. For letters **"QW",** is encrypted **"WN".**

Rule No. 4. (Forming BOX). Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, **"HS"** becomes **"BP".** Moreover, "**RG**" becomes "**NK**" and "**DM**" becomes "**CR**".



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

To encrypt the plaintext: **BALLOON**, following the Playfair cipher rules, the conversion process is illustrated below.

Plaintext	Rules	Result
BALLOON	**Apply Rule no. 1**	BA LX OX NX
BA LX OX NX	**Apply Rule no 2, 3 and 4**	IB SU AV AW
Plaintext -------→ **BALLOON = IBSUAVAW** ←------Ciphertext		

TRY ME! Applying the Playfair Cipher substitution technique, determine the ciphertext of the following plaintext using the 5 by 5 matrix on Figure 3.

Plaintext **Ciphertext** **Rules Used**

1. THRIVE = ___________________________ ____________________

2. PERSEVERE = ___________________________ ____________________

3. INSPIRE = ___________________________ ____________________

4. COLLABORATE = ___________________________ ____________________

5. DREAM = ___________________________ ____________________

TRY ME! Applying the Playfair Cipher substitution technique, determine the following hidden message by substituting Ciphertext to plaintext using Figure 3 doing the reverse step.

Ciphertext **Plaintext**

1. NFCTHOILHNVZ = ___________________________________

2. TLNBTLMNYQ = ___________________________________

MODERN ENCRYPTION TECHNIQUES

Block Cipher

- In fact, all symmetric block encryption in current use is based on a structure referred to as a Feistel block cipher
- For that reason, it is important to know the design principles of Feistel cipher

Stream Ciphers and Block Ciphers

- A stream cipher is one that encrypts a digital data stream one bit or one byte at a time
- A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher block of equal length.

Block Cipher Vs. Stream Cipher

- Process messages
- Block (64bits or more) vs a bit or a byte
- Many current ciphers are block ciphers
- Block ciphers look like an extremely large substitution
- Ideal block cipher would need a key of $n*2^n$ size for a n-bit block cipher
- Based on Feistel Cipher Structure

Youtube Search: **Cryptography Lesson #1 – Block Ciphers**

Source: https://www.youtube.com/watch?v=-Gk9kaFoBxU

How does a stream cipher work? (AKIO TV)

Source: https://www.youtube.com/watch?v=rAFNmO-4CIA

Feistel Cipher Structure

From the year 1960 to 1971, a group from IBM led by Horst Feistel [5] had initiated a research project named it as "Lucifer" for computer cryptography and became the first ever known block cipher operating 64 bits per block using 128 bit key size this algorithm was also known as "Feistel Cipher". Another effort was again initiated by IBM in 1973, to produce a commercial encryption scheme and named it as DES (Data Encryption Standard). This was led by Walter Tuchman. The DES is actually an improved version of the project Lucifer which was noted as resistant to cryptanalysis. The DES was adopted as federal standard and was used by U.S. government communication in 1976. With a very strong internal structure of DES, it was used for over 20 years.

Confusion and Diffusion

▣ Cipher needs to completely obscure statistical properties of the original message

Diffusion

- ◈ Makes relationship between plaintext and ciphertext as complex as possible
- ◈ Is obtained by substitution and a following function

Confusion

- ◈ Makes relationship between ciphertext and key as complex as possible

SYMMETRIC BLOCK CIPHER

✓ DATA ENCRYPTION STANDARD (DES)

An encryption standard

The mid-1970s saw two major public advances. First was the publication of the draft Data Encryption Standard in the U.S. *Federal Register* on 17 March 1975. The proposed DES cipher was submitted by a research group at IBM, at the invitation of the National Bureau of Standards (now NIST), in an effort to develop secure electronic communication facilities for businesses such as banks and other large financial organizations. After advice and modification by the NSA, acting behind the scenes, it was adopted and published as a Federal Information Processing Standard Publication in 1977 (currently at FIPS 46-3). DES was the first publicly accessible cipher to be 'blessed' by a national agency such as the NSA. The release of its specification by NBS stimulated an explosion of public and academic interest in cryptography.

The aging DES was officially replaced by the Advanced Encryption Standard (AES) in 2001 when NIST announced FIPS 197. After an open competition, NIST selected Rijndael, submitted by two Belgian cryptographers, to be the AES. DES, and more secure variants of it (such as Triple DES), are still used today, having been incorporated into many national and organizational standards. However, its 56-bit key-size has been shown to be insufficient to guard against brute force attacks (one such attack, undertaken by the cyber civil-rights group Electronic Frontier Foundation in 1997, succeeded in 56 hours.[33]) As a result, use of straight DES encryption is now without doubt insecure for use in new cryptosystem designs, and messages protected by older cryptosystems using DES, and indeed all messages sent since 1976 using DES, are also at risk. Regardless of DES' inherent quality, the DES key size (56-bits) was thought to be too small by some even in 1976, perhaps most publicly by Whitfield Diffie. There was suspicion that government organizations even then had sufficient computing power to break DES messages; clearly others have achieved this capability. [1]

Assessment Task

Group Composition:	Leader: Members:	Date:	
Course/Yr./Section:		Score:	

GROUP ACTIVITY: The students are expected to form a group with five students each group. There will be one selected leader whose role is to assign each student on the group a specific task to finish including himself/herself.

TASK # 1. WHO IS HORST FEISTEL?

NAME:________________________________

DATE OF BIRTH:_______________________

PLACE OF BIRTH:_____________________

NATIONALITY: _______________________

FIELD OF SPECIALIZATION:_______________

Insert His Image here

COMPANY & WORK EXPERIENCES and Year:____

____
____
____
____

NOTABLE WORK/CREATION:____

EXPLAIN CLEARLY WHY HIS WORK IS REMARKABLE.

____
____
____
____
____
____
____
____
____

TASK # 2. COMPARE AND CONTRAST. Create a **VENN DIAGRAM** for **Block Cipher** and **stream cipher** showing their similarities and differences on the box below.

TASK #3. Programming Challenge. Using any Programming Language, create a program for **Stream Cipher** computation that will accept any length of same size for the value of both Plaintext and Key in binary digit and perform XOR calculation. (***Note***: Need to watch the link given for stream cipher tutorial.)

Write your Code here.	Insert Screenshot of the Program.

REFERENCE:

[1] Rafael Pass and Abhi Shelat, "A Course in Cryptography",2010, Available at: http://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf

[2] Wikipedia, "HISTORY OF CRYPTOGRAPHY", Available at: https://en.wikipedia.org/wiki/History_of_cryptography

[3] Computer Science & Information Technology

Proceeding from the Fourth International Conference on Computer Science and Information Technology (CoSIT 2017) Geneva, Switzerland, March 25-26, 2017.

[4] Encryption 101, https://www.phoenix.gov/itssite/Documents/kb-encryption-101.pdf

[5] M. Rhee, Internet Security, Cryptographic principles, algorithms and principles, John Wiley & Sons, Ltd ISBN 0-470-85285-2, 2003.

[6] Cryptography in Everyday Life, https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html