

Chapter 1 Analysis of the main encryption systems and their applicability

Capítulo 1 Análisis de los principales sistemas de cifrado y su aplicabilidad

LÓPEZ-GONZÁLEZ, Erika†*, REYES-NAVA, Adriana, ANTONIO-VELÁZQUEZ, Juan A. and CABALLERO-HERNÁNDEZ, Héctor

Tecnológico de Estudios Superiores de Jocotitlán, Carretera Toluca-Atacomulco km 44.8, Ejido de San Juan y San Agustín, Jocotitlán, Edo.

ID 1st Author: *Erika, López-González* / **ORC ID:** 0000-0001-7279-5111, **CVU CONACYT ID:** 289386

ID 1st Co-author: *Adriana, Reyes-Nava* / **ORC ID:** 0000-0002-4440-909X

ID 2nd Co-author: *Juan A., Antonio-Velázquez* / **ORC ID:** 0000-0003-3052-3171

ID 3rd Co-author: *Hector, Caballero-Hernandez* / **ORC ID:** 0000-0002-2790-833X, **CVU CONACYT ID:** 445998

DOI: 10.35429/H.2022.3.1.15

E. López, A. Reyes, J. Antonio and H. Caballero

*erika.lopez@tesjo.edu.mx

A. Ledesma (AA.). Science of Technology and Innovation. Handbooks-TII-©ECORFAN-Mexico, 2022.

Abstract

Virtual work, e-commerce, digital health, distance, or virtual education grew exponentially thanks to the confinement due to the Covid-19 pandemic. As a result, the same happened with attacks and security incidents, caused by various circumstances. Personal data is generally the main target of hackers, this includes financial institutions. In 2020 alone, 12 known cybersecurity events occurred in Mexico that included institutions such as Condusef, SAT, Banxico, the secretary of public function, among others, in the last one personal data of public officials were violated and exposed (Riquelme, 2021).

With the evolution of technology, attacks become increasingly sophisticated. However, one of the most used and effective systems to protect data is encryption that is related to computer security offers solutions to this problem since it is a discipline that addresses various techniques, applications and devices responsible for ensuring the integrity and privacy of the information of both the computer system and its users. This work seeks to explain the main encryption techniques currently used, the fundamental basis of its encryption process, the importance of the best-known standards in the computer age, the difference between symmetric encryption and asymmetric encryption, when it can be considered hybrid encryption and where they are commonly used.

Asymmetric, Encrypted, Symmetric, Systems, Integrity

Resumen

El trabajo virtual, comercio electrónico, la salud digital, la educación a distancia o virtual, crecieron exponencialmente gracias al confinamiento por la pandemia de Covid-19. Como consecuencia lo mismo sucedió con los ataques e incidentes de seguridad, provocados por diversas circunstancias. Los datos personales generalmente son el principal objetivo de los hackers, esto incluye a las entidades financieras. Tan sólo en el año 2020 ocurrieron 12 eventos de ciberseguridad conocidos en México que incluía a instituciones como Condusef, SAT, Banxico, La secretaria de función pública, entre otras, en la última se vulneraron y expusieron datos personales de los funcionarios públicos (Riquelme, 2021).

Con la evolución de la tecnología, los ataques se vuelven cada vez más sofisticados. Sin embargo, uno de los sistemas más usados y efectivos para proteger los datos es el encriptado que se relaciona con la seguridad informática ofrece soluciones a esta problemática ya que es una disciplina que aborda diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información tanto del sistema informático y sus usuarios. Este trabajo busca explicar las principales técnicas de cifrado utilizadas actualmente, la base fundamental de su proceso de cifrado, la importancia que tienen en la era informática los estándares más conocidos, la diferencia entre el cifrado simétrico y el cifrado asimétrico, en qué momento puede considerarse cifrado híbrido y dónde comúnmente son empleados.

Asimétrico, Cifrado, Simétrico, Sistemas, Integridad

1. Introduction

Various public and private institutions have suffered attacks and security incidents, putting the information of hundreds of thousands of people at risk and/or vulnerability (Gil Vera, 2017). Where those affected by the personal data breach can do little to protect their information.

Therefore, security strategies applied at the national level must be sought, as mentioned by Romero, there are different attacks that are perpetrated directly or indirectly in the financial sector, in public or private institutions by organized crime organizations, this makes it important to increase security in the various sectors of the country to avoid risks (Romero, 2018), especially economic that can cause a high impact, this is a task that not only concerns the ICT infrastructures that support the different business processes. It is an activity that involves everyone, including industrial control systems. Therefore, it must seek to address threats to national, local and personal security that guarantee the stability, integrity, availability and control of information.

The study of security depends on the origins or sources of threats to systems. (Haro, 2011) In the field of logical security, information is protected within its own environment with the use of security tools, and can be defined as a set of operations and techniques aimed at protecting information against destruction, modification, improper disclosure. gives or simply delays in its gestation; That is, it applies barriers and procedures that safeguard access to data and only access them, the people authorized to do so. Depending on the application required for the processing of information or the means by which it is transmitted, so will be the services to be covered and/or the objectives of all security services.

The goals of logical security are to restrict access to data, programs, or files, to ensure that users can work with confidence that they won't modify information or resources that don't belong to them. Ensure the correct use of information resources with the appropriate procedures and if the information is transmitted it is received guaranteeing security. Some of the objectives of security are to guarantee some services, table 1.

Table 1 Security Objectives

Objective	Service
Keep information secret, for everyone except those who have access authorization.	Confidentiality
Ensure that the data has not been altered in any way, and if it was correctly altered by the right person	Integrity
Have the information at the required and authorized time	Availability
Check the source of the message.	Authentication
Verify the identity of a participating entity.	Identification
Be able to relate a message to an entity.	Company digital
Approval of certain information by a trusted entity.	Certificate
Prevent the denial of previous agreements or actions. Not being able to deny actions	Non-repudiation
Being able to hide the identity of an entity involved in some process	Anonymity

Source: Own Work

One of the sciences responsible for safeguarding security is cryptology whose main objective is to offer security to data, hiding information, using different techniques. This is derived from cryptography, which is responsible for studying the algorithms, protocols and systems that are used to protect information and provide security to communications and entities that need it. Currently, cryptography is the only method capable of ensuring the correct use and protection of data, guaranteeing confidentiality, availability, integrity and authentication of data. Therefore, it is important to know the operation of the various encryption systems that will be described below.

2. Basis of encryption systems

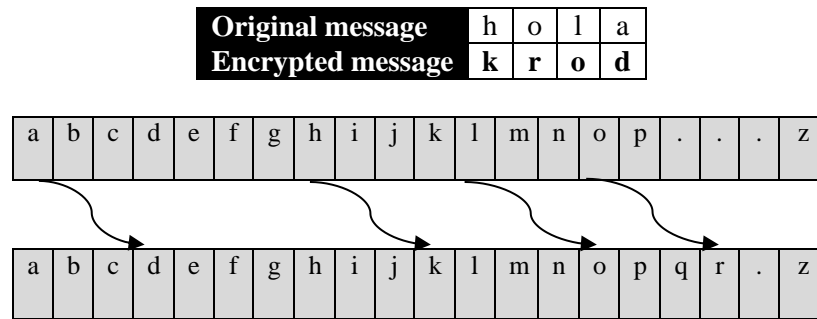
2.1 Replacement

The substitution technique is used as a base process in various systems of cryptography, where its main objective is only to replace an occupied character, by another, it is often done by a character that belongs to the same system used; either numeric or alphanumeric, depending on the encryption system, however it takes different variants, currently it is used by standards such as DES, AES.

An example of the operation of substitution encryption can be seen in Figure 1 that describes one of the oldest forms of cipher and consists of replacing one character with another of the alphabet considering a number as a key (k), this key will indicate how many characters will have to be advanced in the previously ordered alphabet. In this example, the key k is 3 so for each letter of the message will advance 3 positions of the alphabet, finding a different character from the original. If the word "hello" is considered taken from the alphabet that already has a defined order as shown in figure 1 shaded part, the letter h is replaced by the d, having traveled the 3 positions indicated by the key; for example, the letter o is replaced by the r, the letter l by the letter o, and a for d; thus having a surrogate encrypted message; Then the word hello of the original message is replaced by the letters krod which would be the encrypted message by substitution, as marked in Figure 1.

In the example of figure 1, the decryption will consist of placing the encrypted message and now instead of advancing the 3 positions of the value of k (key), in the array of the alphabet, those same positions will be regressed, in such a way that the original characters of the message are located, if the value of **k** is not correct the original message can not be deciphered.

Figure 1 Substitution Encryption



Source: Own Work

It is important to mention that cipher systems occupy this principle, but considering other elements or characteristics, for example, with bits, or hexadecimal numbers and will be described later with encryption standards.

2.2 Transposition

Transposition encryption consists of hiding the original message, but placing the characters in different positions or order, there are different techniques and ways to perform it, usually a key is used, for example, the transposition by columns with key works as shown in table 2. This technique basically consists of choosing a word that will be the key to encrypt the message, in the example the key is "secret", and of course the message, which in this case is "hello as you are today". The operation is described in the following steps:

1. First it will be necessary to place in an array the keyword "secret", considering a character by position of the array, as shown in Table 2,
2. The letters of the key are numbered according to the order in which they appear in the alphabet. In case a letter is repeated, it will be assigned the number following the first, as is the case with the letter e in the example.
3. Once the key values have been assigned, the message to be encrypted is written by placing letter by letter at the same height of the calve occupying one cell at a time and according to the length of the key, if the message is long it will continue in the next row, until all the columns are completed (according to the key) and finish writing the message.
4. If the characters in the message are not enough, some other character known as "*" is added.
5. To obtain the encrypted message, the letters will be written considering the columns according to the consecutive order of numbers, that is, first all the characters that seem in the column numbered with 1, then those of column 2, and so on, you have to obtain the encrypted message, as seen in the example, table2. In this case column 1 corresponds to the letter a and is marked with red, column 2 is c, etc. So the encrypted message is "oa*I hoo syaeohmsct*".

Table 2 Substitution encryption

Key	s	e	c	r	e	t	a
Position and/or order	6	3	2	5	4	7	1
Original message	h	o	l	a	c	o	*
	m	o	e	s	t	a	*
	s	h	o	y	*	*	*
Encrypted message	oa*I hoo syaeohmsct*						

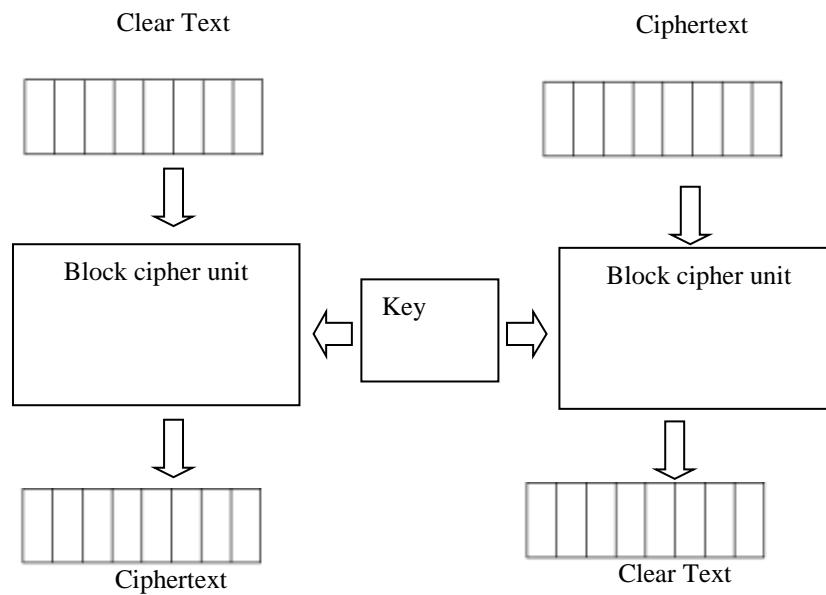
Source: Own Work

The decryption process is reversed, that is, it is necessary to know the key and having the length of the encrypted message you can know the appropriate rows to the table to build the array. Starting by placing the characters in the column with the number 1, the same for the 2, so on, until you get all the columns and find the original message, which will be read by rows

3. Symmetric encryption

This symmetric encryption uses a key to encrypt and with the same key the original message is decrypted, normally it works in blocks of data, binary or hexadecimal. Generally, in the encryption algorithm, does divide the clear text into blocks of equal length, operating on each of these considered as a unit, as can be seen in figure 2. It is important to consider that the encryption process, like the decryption process, is the same. The block length is preset by the encryption algorithm such as the DES or IDEA standard.

Figure 2 Block Cipher



Source: Own Work

3.1 DES Y Triple DES

DES (Data Encryption Standard), is the most studied and widely used data encryption standard, developed by Horst Feistel of IBM, published in March 1975 (Hernández Díaz, 2016). This algorithm works with 64-bit blocks and keys of the same length, described in the following steps, which are also shown in Figure 3:

Data processing

1. To develop the standard encryption process, this is made up of 19 stages, in the first and last, processes called transposition known as initial permutation (IP) and inverse permutation (IP-1) respectively, which are observed in the table 3. This is that the bits are reordered considering the positions marked by each table.

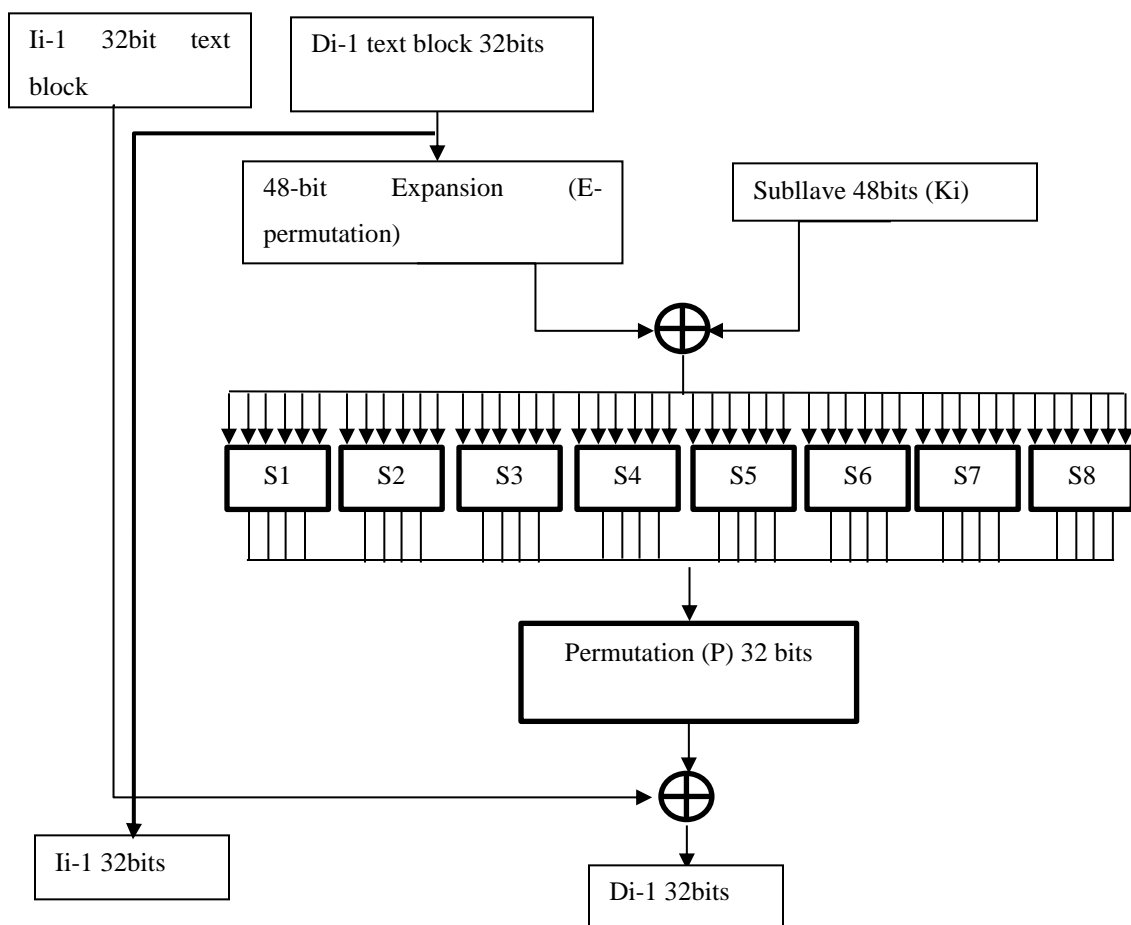
Table 3 Initial permutation (IP) Reverse permutation (IP-1)

58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	28	30	22	14	6	39	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5	34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7	33	1	41	9	49	17	57	25

Source: Own Work

2. Subsequently, the information is processed in 64-bit blocks, which will be subdivided into 2 32-bit blocks, so that one 32-bit block will take the left part (I) and the other, the right part (R). This process will be carried out in 16 intermediate stages, considering for the first stage of the 16 the first data right block to which the party function is applied, figure 3, which is used in the 16 stages.
3. The Fiestel function figure 3, expands and reduces the processed data block (right), all this based on permutation tables and substitution boxes, that is, it is composed of an expansion permutation (E), which converts the right block of 32 bits into one of 48 bits and is observed in table 4. For the expansion it is necessary, as indicated in the standard table, to repeat 16 bits, which are already marked in it. Subsequently, an exclusive-or is performed with the data block and the subkey block, the respective K_i value. The result will be a 48-bit data block; then it is necessary to reduce the result of the x-o again to a 32-bit block, eight 6x4-bit boxes are used (S-Box established by the standard). For this, groups of 6 bits must be condensed, the 1st and 6th bits of the block are taken and they form a 2-bit number called m. This value will indicate the row in the corresponding substitution table S (j), with the 2nd to 5th bits another number called n is formed, with four bits that will indicate the column of S (j) so that the intersection between these two numbers in the S boxes they will indicate the number by which the previous group of 6 bits will be replaced in bits, thus reducing the value of the bits, which is observed in Table 5. Considering that the maximum value for the rows is a binary number of 2 digits, where the largest value would be 3, and the maximum number for the columns would be a binary number of 4 that would be represented as greater than 15. This intermediate phase is completed with a permutation (P) that is shown in the second part of table 4 (Publication F. I., 1999), obtaining a processed right block that for the next round will take the place of the left. The resulting 32-bit blocks will swap positions until the required 16 rounds are obtained. As indicated in the general figure 4.

Figure 3 Fiestel function



Source: Own Work

Table 4 Expansion Function (E) and Permutation Function (P)

32	1	2	3	4	5	4	5	16	7	20	21	29	12	28	17
6	7	8	9	8	9	10	11	1	15	23	26	5	18	31	10
12	13	12	13	14	15	16	17	2	8	24	14	32	27	3	9
16	17	18	19	20	21	20	21	19	13	30	6	22	11	4	25
22	23	24	25	24	25	26	27								
28	29	28	29	30	31	32	1								

*Source: Own Work***Table 5** Replacement boxes S

Row	Column															S-boxes	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14		15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	12	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Source: Eown Work

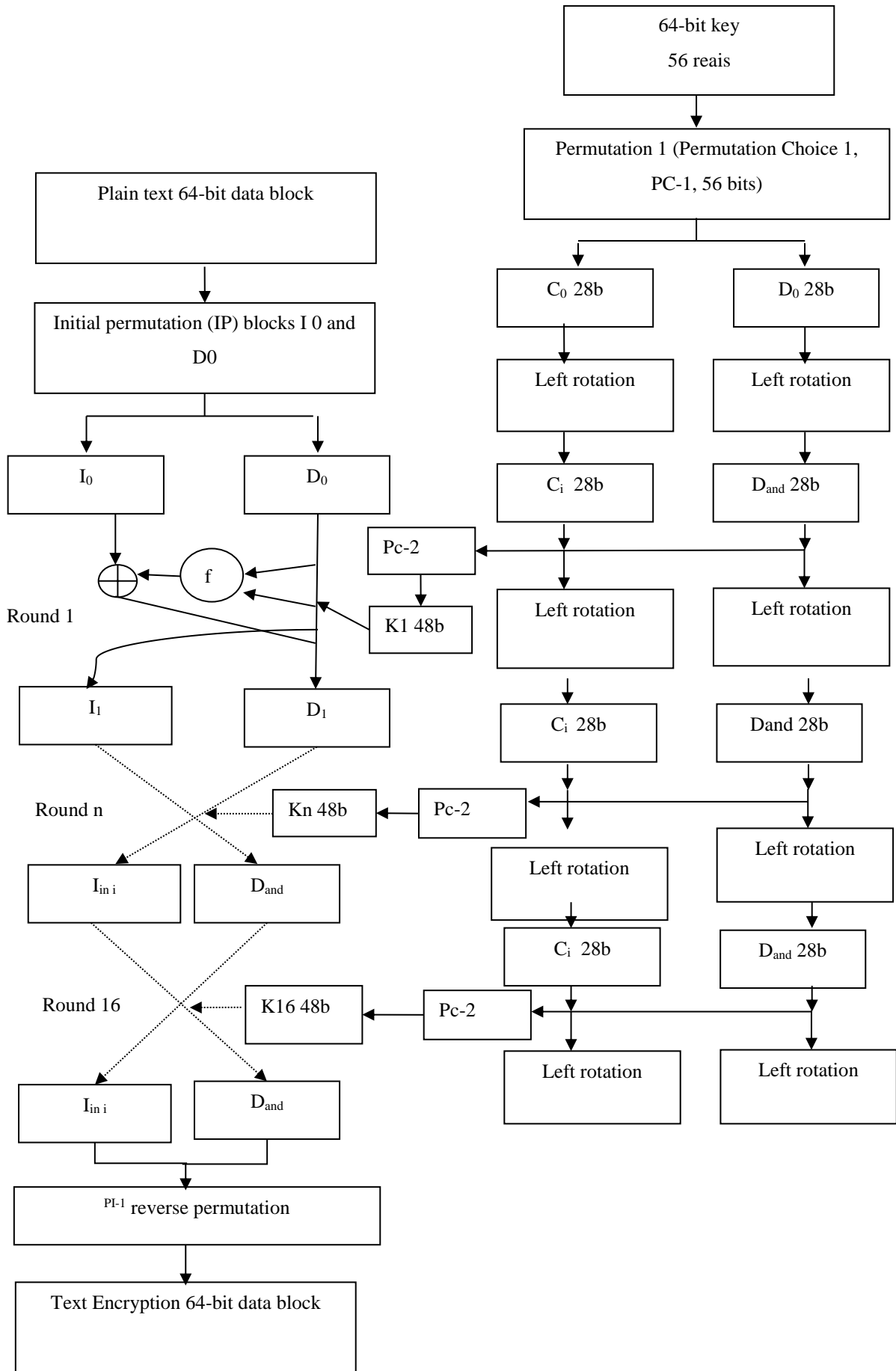
4. In the penultimate stage, the exchange of left and right blocks of 32 bits each is carried out, as shown on the left of figure 4.

Working the keys

1. First for key processing: initially the key block is 64 bits, however, it is reduced in the process to 56 bits that guarantee the effectiveness of encryption, that is, the least significant bits of each byte are eliminated.
2. 16 different subkeys of 48 bits each, obtained from the original 56-bit key, are processed. To obtain the first subkey, an initial permutation (PC-1) is performed, which is shown in Table 6 First Part
3. The subkey is divided into 28-bit blocks which are rotated to the left a certain number of bits depending on the round, for this a table of shift bits provided by the standard is used, table 7.

- Subsequently, the permuted choice is made (PC-2) as a reference to table 6 part 2, of the two halves already rotated; the process is cycled from the rotation of bits to obtain the 16 necessary subkeys, (Sánchez Arriazu, 1999).

Figure 4 DES encryption diagram



Source: Own work

Table 6 Permutation (PC-1) and Permutation (PC-2)

57	49	41	33	25	17	9	1	14	17	11	24	1	5	3	28
28	50	42	34	26	18	10	2	15	6	21	10	23	19	12	4
29	51	43	35	27	19	11	3	26	8	16	7	27	20	13	2
60	52	44	36	63	55	47	39	41	52	31	37	47	55	30	40
31	23	15	7	62	54	46	38	51	45	33	48	44	49	39	56
30	22	14	6	61	53	45	37	34	53	46	42	50	36	29	32
29	21	13	5	28	20	12	4								

Source: Own Work

Table 7 Offset bits according to round

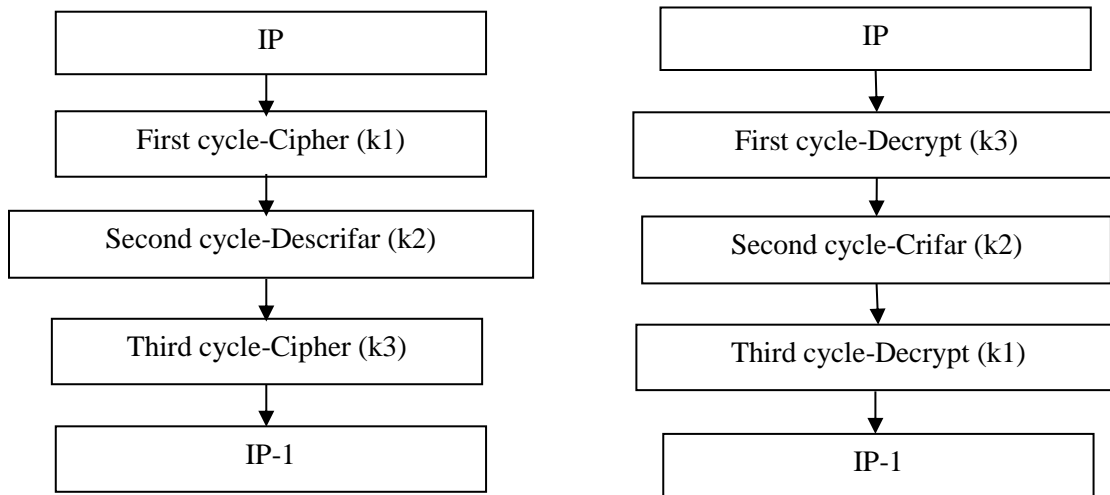
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Source: Own Work

The decryption process uses the same algorithm that is used to encrypt, only the keys are used in the reverse order, although this standard has already been violated by brute force, it is still used in its Triple DES version.

The Triple DES algorithm consists of applying, as its name indicates, 3 DES cycles. To encrypt, use the CDC process (Encrypt-Decrypt-Encrypt) and to decrypt DCD (Decrypt-Encrypt-Decrypt). There is another less used variant which consists of CCC (Encrypt-Encrypt-Encrypt) for encryption and DDD (Decrypt-Decrypt-Decrypt) for decryption. In the algorithm described in the standard (Publication, 1999) 3 different keys are used (k1-k2-k3), which means that an effective 168-bit key called 3DDEA is used. You can also use 2 different keys (k1-k2), where the key effectiveness would be 112 known as 2TDEA. The technique known as 3TDEA can be seen in Figure 5, where you can see from the first to the last stage described in the previous DES.

Figure 5 Encryption and decryption Triple DES



Source: Own Work


3.2 Advanced Encryption Standard (AES)

The Advanced Encryption Standard officially adopted by the United States National Institute of Standards and Technology (NIST) in October 2000, also known as Rijnda, an acronym formed by the surnames of its authors Joan Deamen and Vincent Rijmen (Diaz, 2012). This encryption system works on data blocks in a 4x4 arrangement with 128 bits in hexadecimal notation, the keys can be 128, 192 and 256. The higher the key, the more secure it will be. Figure 6 shows an example of how the data is stored on the left and the key on the right of the aforementioned image, both represented by tables.

Figure 6 AES Data Block

Flat text				Encryption key			
52	78	A1	11	21	56	89	C2
89	B2	C3	33	41	87	34	F3
22	34	67	F1	59	E4	6D	1C
D2	55	9B	1C	44	6A	2B	11

Hexadecimal notation

Example **0101 0010**


5hex 2hex

Source: Own Work

AES works with substitution and permutation processes in 4 transformation operations called: SubBytes, ShiftRows, MixColumns, and AddRoundKey, applied in 10 rounds, for data encryption shown in Figure 9, general diagram of AES.

The first operation that is applied in AES, is SubBytes which consists of replacing each byte with another according to the S-Box box (provided by the standard) considering row by column, example shown in table 8, where the unit of the hexadecimal number will determine the column and the ten of the hexadecimal number determine the row, being that the intersection of both numbers will be the one taken in the new data set, example for the number 52 of the plain text of figure 6, this would be replaced by 00.

Table 8 Substitution table SubBytes

HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	TO	D4	A2	OF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	1F	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Source: Own Work

In ShiftRows one byte is rotated to the left according to the row of the array, where row 0 has no rotation, row 1 rotates 1 byte, row 2 rotates two bytes and the third row 3 bytes to the left, figure 7.

Figure 7 AES ShiftRows

DATA to process ShiftRows				DATA processed ShiftRows			
66	32	45	23	66	32	45	23
04	If	89	Of	If	89	Of	04
E5	DC	5F	DF	5F	DF	E5	DC
81	A1	FD	FC	FC	81	A1	FD

Source: Own Work

MixColumns will multiply the 4 bytes of each column by a given matrix, using a linear transformation, obtaining new data for the matrix.

While AddRoundKey does an x-or with column0 of the datablock and column0 of the key, column1 of the datablock with column1 of the key and so on with the 3 columns, figure 8.

These four operations are carried out in the 9 intermediate rounds, while for the last one only SubBytes, ShiftRows and AddRoundKey will be used, an encryption process consulted in the official publication ((Publication F. I., 2001)).

Figure 8 AES AddRoundKey

66	x-or	Ago	=	9C
04		A0		A4
E5		17		F2
81		FE		7F

DATA (column1-3)			KEY (column1-3)		
32	45	23	47	8F	AA
If	89	Of	5F	DC	Ff
DC	5F	DF	E2	A1	D9
A1	FD	FC	D6	C7	E3

Source: Own Work

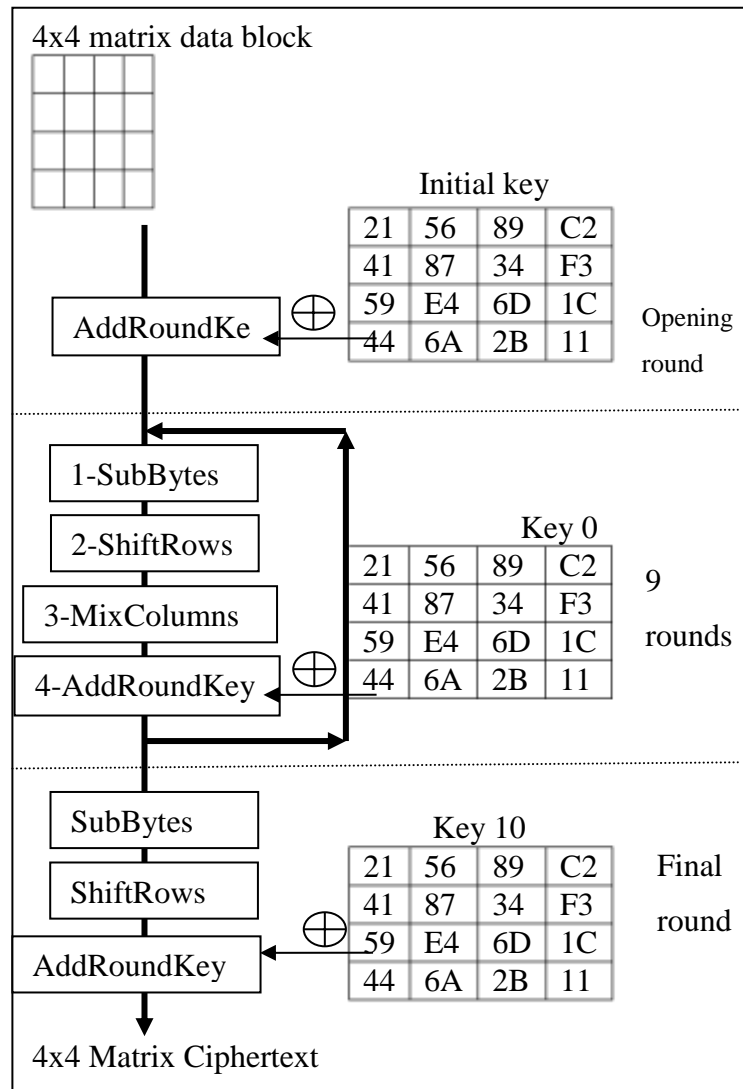
For the generation of subkeys in AES, the original key block is considered and the fourth column from the left or the first from the right, marked in the key table of figure 6, is processed. This consists of rotating the first byte downwards, with the rotated bit.

The SubBytes transformation function (Boxes-S, table 8) is applied to the entire column, that is, new data will be obtained, according to the substitution of table S. Subsequently, a logical operation is performed on this column x-or with column 1 from the left of the original key, in the same way another x-or will be applied with the first column of a constant matrix (Rcon of the standard), assigned one for each subkey, in this way the first column is processed.

The complete key is made up of a 4x4 matrix. In the previous iteration, only the first column of the subkey was worked. For the second column of the subkey, an X-OR will be applied with the second column of the previous key and the first column of the already processed subkey.

Then, for the third column, the third column of the previous key will be taken with the second column of the subkey already processed, performing an X-OR. Finally the fourth column of the subkey will be obtained from the X-OR operation of the fourth column of the previous key and the third column of the subkey already preceded of course. The iterations from the generation of the first column are repetitive, which allows generating the necessary 10 subkeys in AES.

Figure 9 AES cipher diagram



Source: Own Work

4. Asymmetric encryption

This type of encryption works using a key to encrypt and another key to decrypt, generally each user who wishes to work with this technique must have two keys one that is public, and that any other user can use to transmit a message; and a private one that is only known by the owner and is used to recover the original encrypted messages, by asymmetric encryption

4.1 RSA

In 1978, Ronald Rivest, Len Adleman and Adi Shamir proposed the first (probably the best known) public-key cryptographic system. RSA, whose name derives from the initials of each of the authors. It is a cryptographic system that complies with the Diffie–Hellman conditions. Its security is based on the factorization of composite numbers as a product of primes. It also allows the exchange of secret keys and mathematically signing.

RSA work with modular arithmetic using the notation "mod" where the number you want to rescue is the residue of a division. The public key (n) equation 1, is obtained by multiplying 2 prime numbers large enough to guarantee its security, named p and q , it is convenient to clarify that p and q are not public. An F -value, equation 2, is also obtained. From F , a number e is selected, where e and F are relative primes, that is, they have no divisors in common and that their greatest common divisor is one. Finally, a number d that satisfies equation 3 and that is the inverse (multiplicative) of e modulo F , (R. Rivest, 1978).

$$n = p * q \quad (1)$$

$$F = (p - 1) * (q - 1) \quad (2)$$

$$e * d \text{ mod } F = 1 \quad (3)$$

To encrypt, s emust use e and n , considering the plaintext M equation 3.

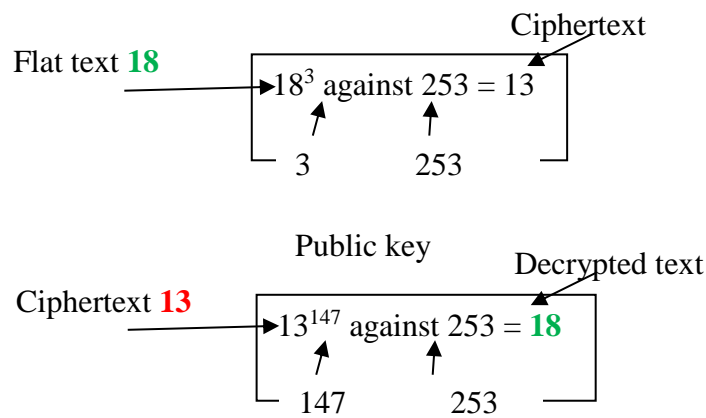
$$C = (M^e) \text{ mod } n \quad (4)$$

To decrypt, consider the value d, the ciphertext value and use equation 5.

$$M = (C^d) \text{ mod } n \quad (5)$$

To better observe this process of encryption with RSA, Figure 8 exemplifies encryption, using the equations.

Figure 8 RSA Encryption Process



Source: Own Work

5. Other forms of encryption

5.1 Hybrid encryption

A hybrid cipher uses both symmetric encryption and asymmetric encryption. That is, a hybrid encryption scheme, an encryption mechanism that can be built from a key encryption scheme or KEM (Key Encapsulation Mechanism) based on a public key scheme, i.e. asymmetric encryption is used to encrypt the key available to encrypt the data in a data encryption scheme or DEM (Data Encapsulation Mechanism) based on a private key scheme.

5.2 Quantum cryptography

"Quantum cryptography solves the problems of encrypting messages to hide information, as well as key distribution, where each bit can be in a discrete and alternate state at the same time; The fundamental unit of storage is the quantum bit, each of which can have multiple states simultaneously at a given instant, reducing the execution time of some algorithms from thousands of OS to just seconds. Quantum cryptography is based on the interactions of the sub-atomic world, and has elements such as the quantum bit, quantum gates, confusing states, quantum teleportation, quantum parallelism, and quantum computing (Molina Vilchis, Silva Ortigoza, & Bracho Molina, 2007)."

Therefore, we must consider that this is a paradigm that must be studied in depth because the most recognized research centers already have and/or are working on quantum computers, hence the weakness of the numbers used in the encryption processes, meaning that in order to crack a key used to encrypt data, less time and effort will be spent with quantum computers, so it is important to start working on quantum encryption and cryptography.

6. Discussion

It is clear that there are many symmetric encryption algorithms, such as: DES, 3DES, AES, IDEA, RC4, among others. Currently several institutions use AES combined with other ciphers. Also, in asymmetric cryptography there is variety such as: Diffie-Hellman, RSA, ElGamal Cipher, Elliptic curve cryptography, Merkle-Hellman cryptosystem, which can also be combined with symmetric encryption to ensure security or privacy. Table 9 describes some advantages and disadvantages of the systems.

Table 9 Comparison of encryption systems

Systems by type		
Type of encryption	Advantages	Disadvantages
Symmetric encryption	<ul style="list-style-type: none"> – Fast encryption – Easy to set up – Easy to understand – Suitable for encrypting big data – Only one key is memorized 	<ul style="list-style-type: none"> – Same key to encrypt as to decrypt – Key exchange is not secure – If the key is shared several times, non-repudiation is not guaranteed
Asymmetric encryption	<ul style="list-style-type: none"> – No keys are shared – Keys must be larger than symmetric keys – Support digital signatures – Ensures recipient authentication 	<ul style="list-style-type: none"> – Must have experience with encryption – If the private key is lost, it will never be recovered – Time consuming
Analyzed encryption systems		
Some	<ul style="list-style-type: none"> – Security of 2^{64} 	<ul style="list-style-type: none"> – Obsolete – Shared key
Triple DES	<ul style="list-style-type: none"> – Security of 2^{128} and 2^{192} since it accepts 2 keys of 64 or 3 also of 64 	<ul style="list-style-type: none"> – May become sluggish – Shared key
AES	<ul style="list-style-type: none"> – Accepts 128, 192, 256-bit keys, minimum security of 2^{128} 	<ul style="list-style-type: none"> – Shared key – Relatively fast
RSA	<ul style="list-style-type: none"> – Can be combined with asymmetric and forms a hybrid cipher 	<ul style="list-style-type: none"> – Slow – Using a random number system for encryption

Source: Own Work

Now, it is important to consider that encryption systems are not only used to protect information. There are also forms of attack such as ransomware, which is a type of cyberattack through malicious software that encrypts files preventing the legitimate user from accessing them, generating a kind of computer hijacking. This type of attack is very common and has great effects, as Ruiz and Jairo comment. Therefore, it is important to document yourself and know both the advantages and risks of encryption systems (Pinzón Ruiz, 2021).

7. Conclusions

Encryption is intended to hide information using cryptographic techniques to prevent it from being readable by those who are not authorized to see it. Encryption is a solution for storing and transmitting sensitive information, since it allows you to control access to information; Restricts unauthorized dissemination in case of loss or theft.

We recommend that you use symmetric encryption when you want to send a fast encrypted message. Asymmetric encryption can be used when you have the public key verified, which complies with a security standard such as OpenPGP of your recipient. It is often complemented by digital signatures to avoid taking risks.

Asymmetric encryption is considered to be more secure since there is no sharing of keys, the public key is already publicly available. With symmetrical encryption, you have to share the password in one way or another, so there is a risk of leakage and you can potentially compromise the encrypted message. In addition to this, the decryption key must be strong enough to prevent unauthorized access to the information that is protected; if this key is lost the information will not be accessible; in the event of a failure of the physical storage device, the information may not be recovered, even if it is encrypted or not.

Finally, it is concluded that symmetric, asymmetric or hybrid data encryption is used depending on the needs of the computer system, the objective is to comply with the characteristics of computer security, which includes protecting the integrity and privacy of the information stored, in process or transaction. Unquestionably, cryptography and the various encryption systems complement computer security and are a preventive measure for data processing and information protection.

Acknowledgement

We are grateful to the Tecnológico de Estudios Superiores de Jocotitlan for the support given in carrying out this research project.

References

- Díaz, L. P. (2012). Algoritmo de encriptación híbrido: cifrado simétrico AES (Advanced Encryption Standard) en combinación con curva elíptica. México. IPN, ESIME. <https://tesis.ipn.mx/handle/123456789/17679?show=full>
- Gil Vera, V. D. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. (I. 0122-1701, Ed.) *Scientia Et Technica [en línea]* 22(2), 193-197. Obtenido de <https://www.redalyc.org/>, <https://www.redalyc.org/pdf/280/28010209.pdf>
- Haro, R. (2011). La Seguridad Informática. C. A. <https://www.redalyc.org/pdf/5826/582663867004.pdf>
- Hernández Díaz, E. A. (2016). Cifrado de audio por medio del algoritmo Triple DES-96. México: IPN, CIDETEC. <https://n9.cl/dimaa>
<https://tesis.ipn.mx/bitstream/handle/123456789/20140/Cifrado%20de%20audio%20por%20medio%20del%20algoritmo%20Triple-DES-96.pdf?sequence=1&isAllowed=y>
- Molina Vilchis, M. A., Silva Ortigoza, R., & Bracho Molina, E. (2007). Criptografía Cuántica: Un Nuevo Paradigma. *Polibits*, núm. 36, Instituto Politécnico Nacional, México, 30-35. <https://www.redalyc.org/articulo.oa?id=402640449006>
- Pinzón Ruiz, J. J. (2021). *Análisis del impacto de los ataques de Ransomware en las organizaciones colombianas como base de conocimiento para la determinación de nuevos mecanismos de protección y minimización de riesgos cibernéticos*. <https://repository.unad.edu.co/handle/10596/50093>
- Publication, F. I. (1999). “FIPS PUB 46-3”. <https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf>
- Publication, F. I. (2001). Advanced Encryption Standard (AES). “FIPS PUB 197”. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>
- R. Rivest, A. S. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, Vol. 21 (2). <https://people.csail.mit.edu/rivest/Rsapaper.pdf>
- Riquelme, R. (2021). 2020 en 12 hackeos o incidentes de seguridad en México. *El economista*. <https://www.economista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html>
- Romero, G. J. (2018). Conceptualización De Una Estrategia De Ciberseguridad Para La Seguridad Nacional De México. *Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM*, XXVIII (2), 1-26. <https://www.redalyc.org/articulo.oa?id=65458498003>
- Sánchez Arriazu, J. (1999). *Descripción del algoritmo DES, (Data Encryption Standard)*. México. <https://docplayer.es/9888866-Descripcion-del-algoritmo-des-data-encryption-standard.html>