





Learning the basics of cryptography with practical examples

Shab E Noor – Universidad de Granada
 Ali Ahmad – Universidad de Granada
 Vanessa Martos Núñez – Universidad de Granada
 Miguel J. Hornos Barranco – Universidad de Granada

 0000-0003-0345-4692
 0000-0001-5530-7374
 0000-0001-6442-7968
 0000-0001-5722-9816

Recepción: 03.05.2022 | Aceptado: 09.05.2022

Correspondencia a través de **ORCID**: Ali Ahmad

 **0000-0001-5530-7374**

Citar: Noor, SE, Ahmad, A, Martos Núñez, V y Hornos, MJ (2022). Learning the basics of cryptography with practical examples. *REIDOCREA*, 11(24), 274-281.

Área o categoría del conocimiento: Estudios de Ingeniería

Abstract: Cryptography is a secure technique of data communication and exchange that relies on encryption and decryption protocols. This technique is in use since many centuries. Nonetheless, in today's world, it supports data protection and privacy while ensuring the authenticity and confidentiality of the data. E-commerce, banking, military, and corporations are the prominent operators of this technology, although it is, directly or indirectly, linked to almost every single person nowadays. Symmetric and asymmetric key cryptography are the two fundamental forms of cryptography. Asymmetric key cryptography is more secure than symmetric but at the cost of greater computational complexity. The use of hash functions and digital signatures also contribute to the security of systems and the privacy of information. This article presents the basic differences between the fundamental types of cryptography as well as practical examples of encrypting information using various cipher systems, which will help to understand them. This is an introductory article that is primarily aimed at undergraduate students in the area of computer science, in order to enrich their understanding of the field.

Keywords: Digital Signature

Aprendiendo los fundamentos de criptografía con ejemplos prácticos

Resumen: La criptografía es una técnica segura de comunicación y de intercambio de datos que se basa en protocolos de cifrado y descifrado. Esta técnica se utiliza desde hace muchos siglos. No obstante, sirve para proteger los datos y la privacidad en el mundo actual, garantizando la autenticidad y la confidencialidad de los datos. El comercio electrónico, la banca, el ejército y las empresas son los principales operadores de esta tecnología, aunque hoy en día está vinculada, directa o indirectamente, a casi todas las personas. La criptografía de clave simétrica y asimétrica son las dos formas fundamentales de criptografía. La criptografía de clave asimétrica es más segura que la simétrica, pero a costa de una mayor complejidad computacional. El uso de funciones hash y firmas digitales también contribuye a la seguridad de los sistemas y a la privacidad de la información. Este artículo presenta las diferencias básicas entre los tipos fundamentales de criptografía, además de ejemplos prácticos de cifrado de información usando varios sistemas, que ayudará a comprenderlos. Se trata de un artículo introductorio que está principalmente dirigido a estudiantes de grado en el área de las ciencias de la computación, con el fin de enriquecer su comprensión del campo.

Palabras claves: Firma Digital

Introduction

The term "cryptography" consists of two Greek words: a) '*kryptos*', which means hidden secret, and b) '*graphein*', which means to write. Cryptography can be defined as a technique of scrambling ordinary text (plaintext) into encrypted form (ciphertext), and back to ordinary text for secure communication (1, 2). The conversion from plaintext to ciphertext is regarded as encryption, whereas from ciphertext to plaintext is termed as decryption, as shown in Figure 1 (3). This technique of secure information exchange is in use since centuries. For instance, Julius Caesar communicated with his generals using encrypted letters in which the letter of the alphabet written actually referred to the letter placed three positions further on the alphabet, i.e., if the written alphabet letters were UVW, they actually meant XYZ. Similarly, use of Enigma machine by Nazi Germany is another example of encrypted communication from the past (4). It is reported that of all

the global connections made through internet, cryptography provides protection to over three quarters of these connections (5).

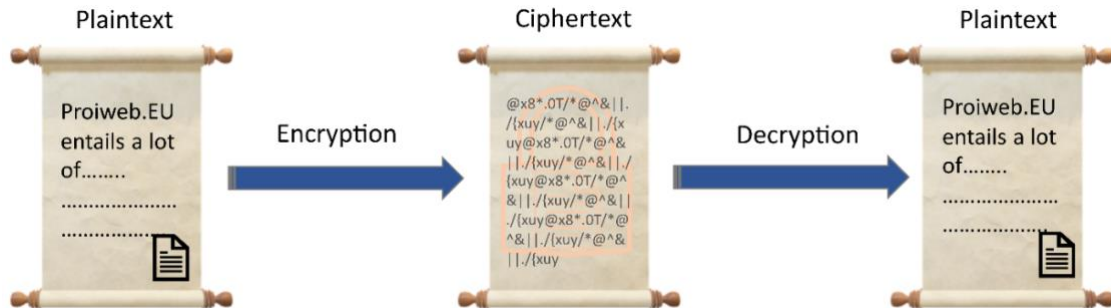


Figure 1. Representation of encryption and decryption steps in cryptography.

Cryptography supports data protection and privacy in today's world while ensuring the authenticity and confidentiality of the data. Banking, military, corporations, aviation, and e-commerce are a few of the most prominent sectors which rely on cryptography for several purposes. The four prominent principles of cryptography include confidentiality, integrity, non-repudiation, and authentication. Confidentiality refers to the accessibility of information only by the intended people. Integrity refers to the exactness and meticulousness of the information received (regarding the one sent). Likewise, non-repudiation refers to the impossibility of renouncing participation in the data exchanged by the parties involved once the transaction has been carried out. Whereas authentication in cryptography refers to the accuracy of origin (sender) and destination (receiver) (6, 7).

This introductory article is specially intended for undergraduate students in the area of computer science. Although several forms of cryptography exist today, only the fundamental forms of cryptography, i.e., symmetric key cryptography, asymmetric key cryptography, and hash functions are discussed here, followed by a series of practical examples that illustrate how different cryptographic systems operate to encrypt a certain information. Some of the challenges that cryptography will face in the future are also presented, as well as some ideas to solve them. Finally, the conclusions are outlined.

1. Symmetric Key Cryptography

Symmetric key cryptography is also sometimes referred to as shared key or secret-key cryptography. This technique uses a common (secret) key for encrypting and decrypting the information at both sender and receiver ends, as shown in Figure 2. This common key, which is self-certified, must be shared between the sender and receiver secretly. This technique is considered fast and simple, as it requires minimal resources. However, the common key can become compromised, making it easy for attacker or third party to decrypt the message and benefit from it. Therefore, this technique should be applied when a lot of data transfer is required with no strict security measures (2, 8). Numerous algorithms, including Data Encryption Standard (DES), triple DES (3DES), Advanced Encryption Method (AES), and Blowfish, have been implemented to define the symmetric key cryptography.

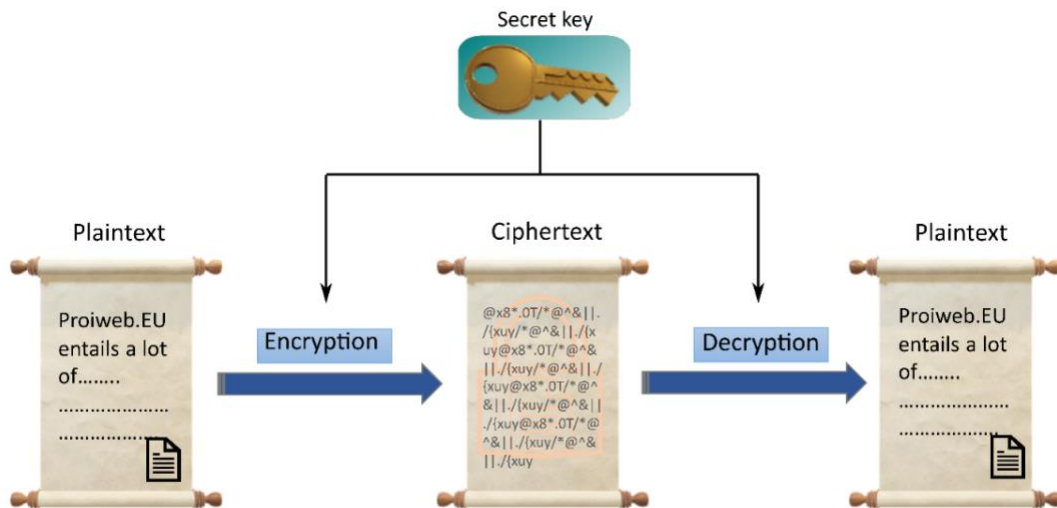


Figure 2. Representation of symmetric key cryptography.

2. Asymmetric Key Cryptography

Asymmetric key cryptography is also sometimes referred to as public key cryptography. In contrary to symmetric key cryptography, this technique uses two different keys, i.e., public key and private key. In this method, plaintext is encrypted using a public key and is decrypted back to plaintext using a private key (see Figure 3), thus there is no self-certification as in symmetric key cryptography. For keys certification, certificates and digital signatures are used. This system is considered more secure, and is thus used for highly sensitive information transfer, as those transactions related to banking, e-commerce, military, etc. Most common algorithms used in asymmetric key cryptography include Elliptic Curve Cryptosystem (ECC), Rivest Shamir Adleman (RSA), Diffie-Hellman protocol, Digital Signature Algorithm, etc. (2, 8).

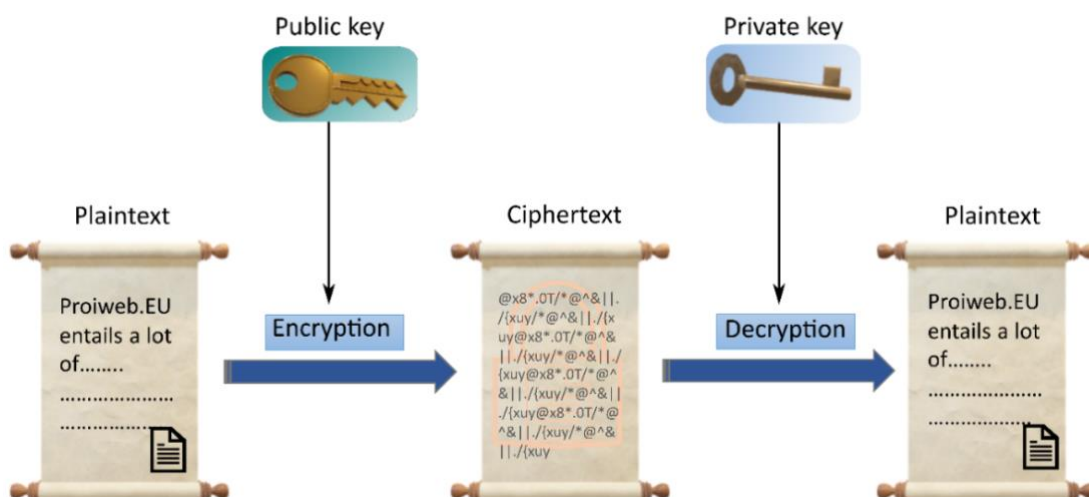


Figure 3. Representation of asymmetric key cryptography.

3. Hash Functions

Apart from symmetric and asymmetric key cryptography, hash functions also form the basis of a cryptographic system. Hash functions are also sometimes referred to as one-way hash functions because they are usually one-way irreversible functions that protect data by not letting the recovery of original message. The message received can be interpreted as unaltered and complete (ensuring its integrity) only if the sender's hash value verifies the user (Figure 4). A decent hashing system should generate unique outputs as a result of every given input. Otherwise, if two inputs produce the same output (i.e., hash value) a hash collision or clash will occur. This is due to a hash function always generated a hash value with a fixed number of bits, which depends on the algorithm in question. This technique is used for hashing certificates and passwords, among other applications. Most common algorithms used in hash functions include Message Digest (MD), Whirlpool, Blake 2, Blake 3, etc. (7, 9).

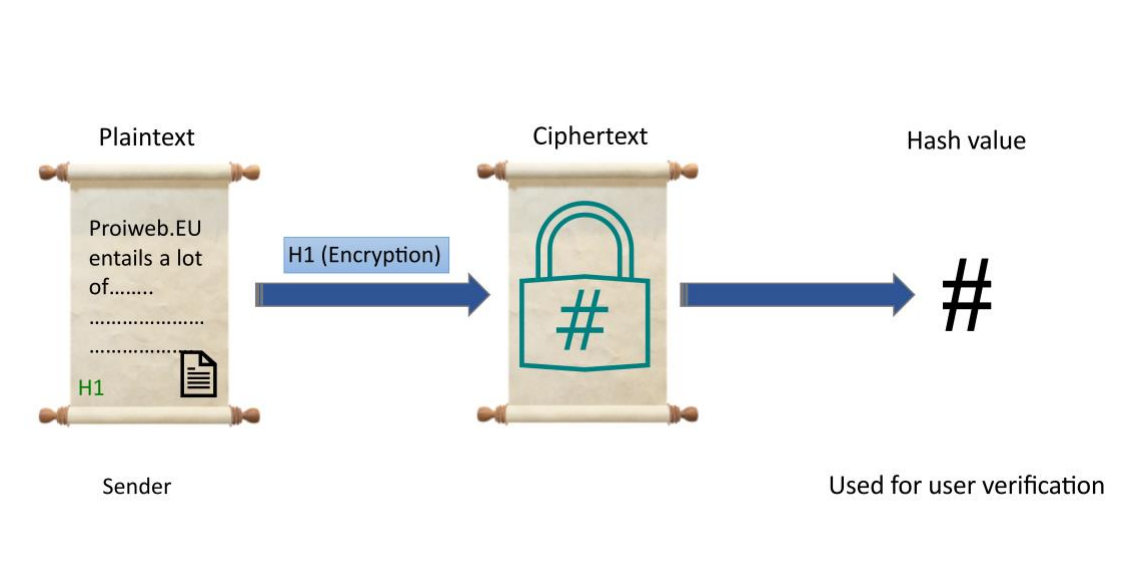


Figure 4. Representation of hash function, where the encrypted data results in a hash value that cannot be decrypted and is used for user verification.

Based on these basic forms of cryptography, numerous algorithms and cipher systems have been made. The following section presents with practical examples how some of the first encryption systems used work.

4. Practical Examples of Cryptography

Here we will see some practical examples in cryptography by encrypting a given message (e.g., “cease attack”) in the following cipher systems: Caesar, Shift, Rail Fence, Mono-alphabetic, Polybius Square, Vigenère and Cardan Grille.

A. Caesar Cipher

Caesar Cipher encoding is done by shifting the letters of alphabet to 3 places forward (10). For example, letter “a” is encrypted by letter “D”, letter “b” with “E”, and so on.

Message:	cease attack
Cipher text:	FHDVHDWDFN

B. Shift Cipher

In Shift cipher, encryption is done by shifting the letters of alphabet according to the key. Key can be a number between 0-25 (10). For example, if the key is 5, then letter “a” will be replaced by letter “F”.

Message:	cease attack
Key:	2
Cipher text:	EGCUG CVVCEM

C. Rail Fence Cipher

Rail fence cipher encoding is done by arranging the letters of the message into a zig zag pattern, and then write the cipher text from left to right and from top to bottom (11). Depth of this zig zag pattern (i.e., number of rows) depends on the value of a key. Thus, Figure 5 shows 3 rows because the key is 3.

c				e				a		
	e		s		a		t		c	
		a				t				k

Figure 5. Representation of zig zag pattern used in rail fence cipher encoding.

Message:	cease attack
Key:	3
Cipher text:	CEA ESATC ATK

D. Mono-Alphabetic Cipher

Mono-alphabetic cipher technique uses the fixed substitution of alphabet letters. Each letter of the message is mapped to a given letter of the cipher alphabet, which is defined in a fixed way, as shown in Figure 6 (10). Thus, for example, if letter “L” is set as the substitute for letter “a”, then it will be replaced by the same substitute letter every time it is repeated in the message.

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

Figure 6. Representation of substitution alphabets used in mono-alphabetic cipher.

Message:	cease attack
Cipher text:	KFLIF LPPLKX

E. Polybius Square Cipher

In Polybius square cipher, alphabet letters are arranged in a square matrix (12). For encryption, each letter of the message is replaced by a two-digit number (each one ranges from 1 to 5, due to the alphabet letters are placed in a 5 x 5 grid), using the row x column principle, as shown in Figure 7.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Figure 7. Polybius square cipher used in cryptography.

Message:	cease attack
Cipher text:	3151113451 114444113152

F. Vigenère cipher

In Vigenère cipher, key ('LOVE' in our example) is repeated according to the length of the message to be encrypted. Encoding is done by looking for the letter of the message to be encrypted at the top of the Vigenère table (shown in Figure 8) and the letter of the key in the left column. The encrypted letter is found at the intersection (10).

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

Figure 8. Representation of Vigenère square.

Message:	cease attack
Key:	LOVELOVELOV
Cipher text:	NSVWP OOXLQF

G. Cardan Grille Cipher

In Cardan grille, original message is hidden within a larger note, which seems like an innocent message. The encryption in Cardan grille cipher is done by using grid with holes, receiver need to put the grid on the note/letter and read only the letters shown through the holes (11). This can be easily understood with the following example:

Encryption:

Hello Richard,
 I hope you are doing well. I am coming home tomorrow.
 See you at 3 p.m.
 Take care.
 -Karen

Decryption:

			c		
	e			a	
Se		at			
Ta	c				
				K	

Message: cease attack

5. Challenges for cryptography in the future

Cryptography holds a vital position in all the affairs of modern life, including the use of social media platforms, online transactions, data transfer, establishing smart cities and homes, educational institutions, etc., where privacy and security are the prime concerns. Both classical models of cryptography, i.e., symmetric and asymmetric key cryptography, are useful for ensuring confidentiality, non-repudiation, integrity, and authentication. Nevertheless, both of them have their limitations and strengths. For instance, due to its lower security, Diffie-Hellman algorithm could be replaced by quantum cryptography. Quantum key distribution, Shor's algorithm for factoring, and device independent quantum cryptography are few of the most commonly employed algorithms in quantum cryptography (13). However, quantum cryptography is also susceptible to the classical bucket brigade attacks, also known as man-in-the-middle attacks, which try to intercept without authorization the communication between the sender and the receiver. The other challenge in this regard is the quantification of secrecy and confidence that are also connected to Bell's inequality (14). Similarly, the generation of large sets of prime numbers for higher encryption also remains challenging. Apart from all this, most algorithms providing higher level encryption and decryption security used in cryptography are computationally complex and expensive that limit their general use (1, 6-8).

Having a hybrid cryptosystem can increase the security while offering substantial usage simplicity. Future systems might have much more sophisticated algorithms for encryption and decryption than the current ones. Based on previous knowledge and experiences in current cryptography systems, more research and efforts are needed to preserve the security and privacy of information in all electronic transactions conducted over the internet. In an increasingly connected world this type of transaction increases exponentially, while new technologies, such as Internet of Things and Quantum Computing, are emerging. These technologies bring important opportunities and advantages, while posing new threats to the security and privacy of data, so valuable for companies lately.

Conclusion

Cryptography is a technique for secure information exchange nowadays, though it is being used since many centuries. Symmetric and asymmetric key algorithms form the basis of cryptography and are greatly effective in securing the transferred data. Symmetric cryptographic systems offer limited security but are simple and faster, whereas asymmetric cryptographic systems offer highly secure medium but hold a high computational complexity and are a bit slower. Use of digital signatures and hash functions can also be applied to maintain the security and privacy of information. However, there is further needed to devise novel algorithms that could offer rigorous protection against third party attacks. This is especially relevant if we take into account the threats that some of the new technologies that are emerging pose to security and privacy in digital information exchanges.

References

1. Arslanian H, Fischer F. The Basics of Cryptography and Encryption. *The Future of Finance*: Springer; 2019. p. 89-93.
2. Rajanbabu DT, Raj C, editors. Implementing a reliable cryptography based security tool for communication networks. *2014 International Conference on Science Engineering and Management Research (ICSEMR)*; 2014: IEEE.
3. Maqsood F, Ahmed M, Mumtaz M, Ali M. Cryptography: a comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*. 2017;8(6):442-8.
4. Bumiske C, Tatar J. *Cryptoassets: The innovative investor's guide to bitcoin and beyond*: McGraw-Hill Education New York; 2018.
5. Martin K. *Cryptography: The key to digital security, how it works, and why it matters*: WW Norton & Company; 2020.
6. Delfs H, Knebl H. *Introduction to Cryptography Principles and Applications* (2007). Springer.
7. Delfs H, Knebl H, Knebl H. *Introduction to cryptography*: Springer; 2002.
8. Chandra S, Paira S, Alam SS, Sanyal G, editors. A comparative survey of symmetric and asymmetric key cryptography. *2014 international conference on electronics, communication and computational engineering (ICECCE)*; 2014: IEEE.
9. McKenzie BJ, Harries R, Bell T. Selecting a hashing algorithm. *Software: Practice and Experience*. 1990;20(2):209-24.
10. Katz J, Lindell Y. *Introduction to modern cryptography*: CRC press; 2020.
11. Gaines HF. *Cryptanalysis: A study of ciphers and their solution*: Courier Corporation; 2014.
12. Arroyo JCT, Dum Dumaya CE, Delima AJP. Polybius Square in Cryptography: A Brief Review of Literature. *International Journal*. 2020;9(3).
13. Bhatt AP, Sharma A. Quantum cryptography for internet of things security. *Journal of Electronic Science and Technology*. 2019;17(3):213-20.
14. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Reviews of modern physics*. 2002;74(1):145.