IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

The Study of Secure Communication using Cryptography Algorithms

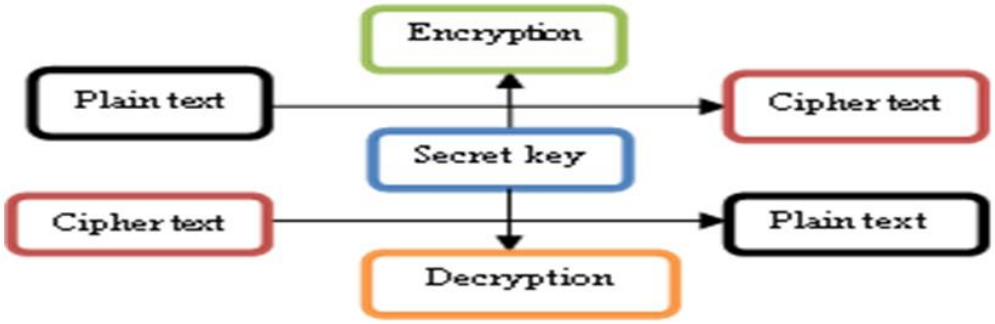
Nidhi[1], Parmila Kumari[2*], Parveen Kumar[3], Geeta Rani[4]
Department of Mathematics, Arya P.G. College Panipat, Haryana, India[1]
Department of Mathematics, C. R. A. College, Sonipat, Haryana, India[2]
Department of Mathematics, Tau Devi Lal Govt. College for Women, Murthal, Sonipat, Haryana, India[3]
Department of Commerce, Tau Devi Lal Government College for Women, Murthal, Sonipat, Haryana, India[4]

Abstract: *Network and internet applications are growing in popularity daily. Security and safety procedures are needed for sensitive information. By transforming data from its original form into an unreadable one, encryption algorithms offer the required defence against attacks by data intruders. Now a days, username/password authentication makes up the majority of web authentication. Data security can be achieved via a method known as cryptography. In the past, military data was kept secure using cryptography to safeguard national security. After the advent of communication tools, the range of uses for cryptography has significantly increased today; cryptography is primarily necessary to ensure that data are safeguarded against penetrations and to prevent the practise of spying. The state of the art for several different cryptographic methods used in networking applications is discussed in this paper with help of examples.*

Keywords: Network security, cryptography, symmetric encryption, asymmetric encryption

I. INTRODUCTION

Computer and network security is still being defined because it is a young and rapidly evolving field of technology. One may claim that a network security analyst needs to be capable of studying security from the business viewpoint in order to implement recent security acts, as well as from the technical standpoint in order to comprehend and choose the most suitable security solution. The first focus of network security was on algorithmic components like encryption and hashing methods. Even though these ideas evolve often, computer networks cannot be protected by these abilities alone. Courses that focused on the most recent assaults took place as crackers toiled away at networks and systems. Several experts now contend that in addition to learning how to safeguard networks, individuals must also develop cracker-like thinking skills [15-16] .Making wise judgements is aided by having the following background knowledge in security: Attack detection, encryption methods, network architecture, protocol analysis, access control list, and vulnerability. Cryptography is used for network security. In cryptography [9], plaintext or clear text is data that can be read and understood without the need of any additional security measures. Encryption is the process of concealing the content of plaintext by concealing its appearance. Data known as cypher text is produced when plaintext is encrypted. We employ encryption to safeguard data so that it is concealed from anybody to whom it is not projected, including those who are able to view the encrypted data. Decryption refers to the process of converting encrypted text back to plain text. Three different kinds of algorithms are used in cryptography.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Hash function, symmetric and asymmetric key algorithms, etc. The security of data users is greatly influenced by cryptographic methods. There is little chance of deciphering the original plaintext from the cypher text due to the algorithm's high complexity. Security is increased by complexity. Plain text is converted into cypher text via the process of encryption (secure data). As indicated in figure, decryption is the act of undoing encryption, which transforms encrypted text into plain text (1).

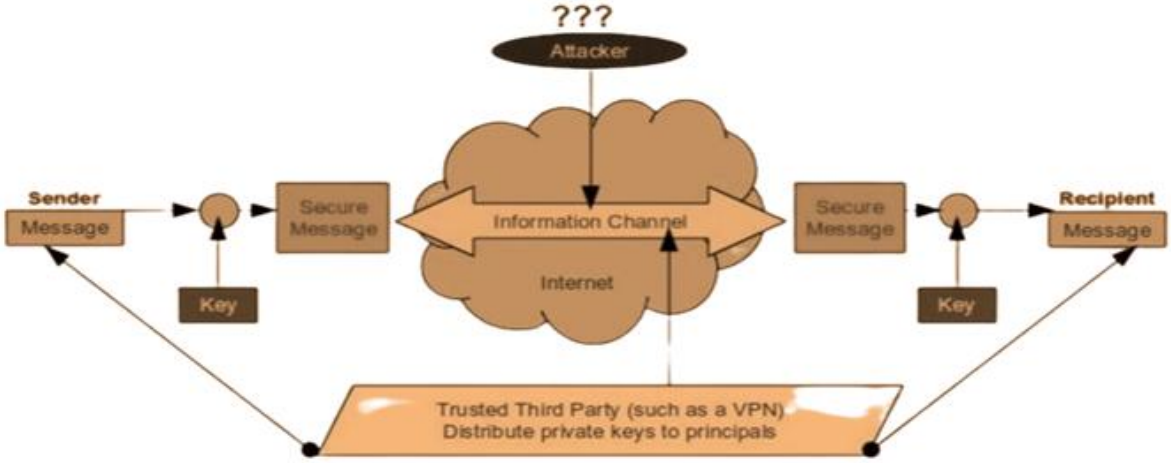
II. LITERARY SURVEY

Nowadays, cryptography is used practically everywhere in the world of electronics. Although the broad applications of cryptography have just recently begun, its traditional applications have a lengthy history. The research dates back to ancient civilizations, and historical evidence of the use of cryptography techniques is discovered, which connects to contemporary electronic cryptography. Throughout the earliest stages of civilization, people in the Egypt, Greece, and Rome regions communicated via cryptography. The earliest known form of cryptography was used in ancient Egypt on hidden hieroglyphics cut into stone around 1900 B.C. (2000 B.C. [5]), to conceal the meanings from those who did not know them and for fun. The "Scytale" of Sparta [5], which is allegedly employed by the Spartan military, is a better kind of cryptography that was used in ancient Greece as science, language, and writing skills advanced. Using wound tape and sticks, this cryptography's concept was created [6]. Another early substitution cypher was the Caesar shift cypher, which was utilised in ancient Rome. It was a mono alphabetic encryption that was created by moving the alphabets about. One of the first Hebrew cyphers is called "Atbash". Two different types of cyphers, Kauitiliyam and Mulavediya, were used in ancient India, according to the 2000-year-old Kamasutra of Vatsyayana. Mulavediya cypher was created by employing a pair of letters and their opposites, and Kautiliyam cypher was created using phonetic relationships, such as switching vowels and consonants [7]. According to the Muslim scholar Ibn al-Nadim [2], there were two secret scripts used in Persia under the Sasanian kings: h-dabrya for official correspondence and rz-saharya for secret messages with foreign nations. These traditional encryption techniques, often known as transposition cyphers, primarily relied on the rearranging of alphabets, the substitution of alphabet locations, or the replacement of other alphabets from various languages. Examples are "HOW ARE YOU?" and "WHO ERA UOY?". "How are you?" might be coded as "ERZ DUH BRX?" by inserting "D" in the first position once more or by replacing "A" with "D" and replacing the other alphabets in the same order. The necessity for a new name was recognised as cryptographic technology advanced alongside scientific knowledge. According to D. Kahn, Arabs are where contemporary cryptography got its start. By listing all conceivable Arabic words with and without vowels in Al-"Book Khalil's of Cryptographic Communications," mathematical notions like permutations and combinations were first used. According to a recently found manuscript, the Arab mathematician and polymath Al-Kindi employed frequency analysis to create encrypted text and produced a book on cryptography named "Rislah fiIstikharaj al-Mu'amma" in the ninth century. These cyphers are still employed in puzzle creation [3]. Each letter in the plaintext is given more than one substitution in Al-work, Qalqashandi's which is based on earlier work by Ibn al-Durayhim and contains the first explicitly stated work on poly alphabetic cypher [8].Leon Battista Alberti likely created the first cypher machine, an automatic cypher machine that utilised a wheel. Later Blaise de Vigenère created the most intriguing cypher, the Vigenère cypher, a poly alphabetic cypher that utilised a Caesar cypher modification [4]. Up until the early 20th century, several complex cypher machines were developed. German engineer Arthur Scherbius created the Enigma machine at the close of World War I in order to safeguard military, diplomatic, and economic communication. During World War Two, German forces used the Enigma machine to transmit vital information among the Nazi warriors. At the time, it was among the best rotor machines available [4]. Modern cryptography makes substantial use of mathematics, including elements of information theory, computational complexity, statistics, abstract algebra, and finite mathematics in general. This is due to the development of electronic machines like computers. These days, a lot of computer cyphers are classified according to their binary bit sequences. With the advent of public key cryptography in the 1970s, a new form of cryptography utilising integer modulo n was created ([11], [12]). The digital signature is the most recent addition to the area of cryptography. Diffie-Hellman first discussed the concept of a digital signature in a paper titled "New Horizons in Cryptography" [10].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

III. MODEL FOR NETWORK SECURITY

The system security model is shown in Figure.



Via some kind of Internet administration, a message is to be passed from one group to the next. The responsibility of appropriating the secret information to the sender and recipient while keeping it secret from any competitors may fall to an outsider. The supporting should be taken into account while developing a safe system.

1. Confidentiality: This refers to the fact that the data is not examined by a person who is not verified.
2. Integrity: This is a guarantee that the sender did not alter or modify the information after it was sent to the collector.

There are two components to any security method.

- A modification to the data that will be delivered that affects security. The key should be used to scramble the message in order to confuse the enemy.
- The message is scrambled before transmission and uncrashed upon receipt using an encryption enter that is used in combination with the modification. When it is essential or desirable to protect the data transmission from an adversary who may pose a threat to classification, realness, etc., security considerations become a key consideration.

IV. GOALS OF CRYPTOGRAPHIC SYSTEM

Any encryption system must guarantee a few qualities that help maintain the confidentiality of communication; these features are known as the cryptographic system's objectives. a group of such objectives are specific, however they may be divided into the following five categories:

- Privacy or Confidentiality: This function makes sure that only the intended user may read the secret message.
- Authentication: Before using the cryptographic system, the sender and receiver's identities must be confirmed.
- Non-repudiation: By using this feature, you can be sure that just the recipient is providing feedback and that the message's sender is the one who actually sent it. It was impossible for either the sender or the recipient to deny sending the letter.

V. LIST OF ESSENTIAL TERMS AND THEORIES

The terminology used in the cryptography model will be briefly explained in this section.

5.1 Cryptography

The prefix "crypt-" denotes "hidden" or "vault," while the suffix "-graphy" denotes "writing". The study and use of methods for secure communication in the face of "adversaries" is known as cryptography or cryptology (the third parties). In a broader sense, cryptography involves destroying the communication in a manner that makes it impossible for outsiders or the general public to access private messages [1]. By using codes, cryptography is a technique for encrypting data and communications so that only the intended audience can read and comprehend it.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Three different kinds of cryptography exist.

1. Symmetric
2. Asymmetric

5.2 Symmetric Key Encryption

This form of encryption uses a single key that is shared by the sender and the recipient. Also known as secret-key encryption. Either block cypher or stream cypher techniques might be used to implement it. Although stream cypher does character-by-character encoding, block cypher performs plain text encryption block-by-block. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two instances of symmetric key encryption.

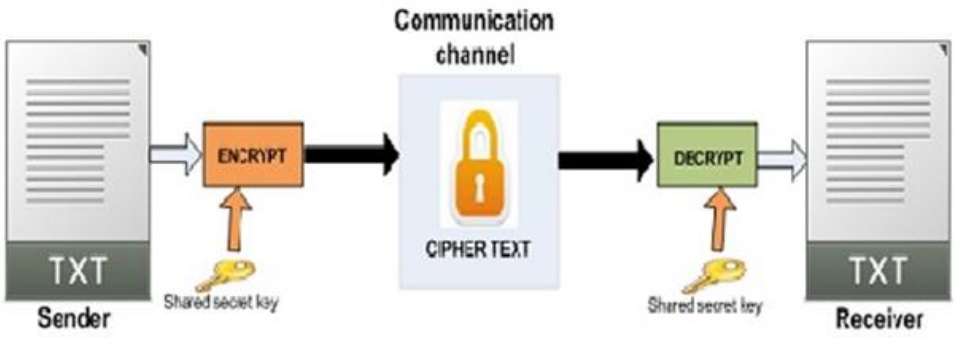


Fig. 2. Symmetric Cryptography

5.3 Asymmetric Key Encryption

A difficult job in symmetric key communication is ensuring that the key is securely sent to each receiver and sender without being compromised. Asymmetric key encryption was created to address the drawback of symmetric key types. Two keys are utilised in this case for the cryptography procedure. Everyone has access to the public key used for encryption, whereas the user-only private key is used for decryption. Sharing of keys is no longer necessary as a result. Also called public-key encryption. Asymmetric key encryption uses techniques like Deffie-Hellman, DSA (Digital Signature Algorithm), ElGamal, and others.

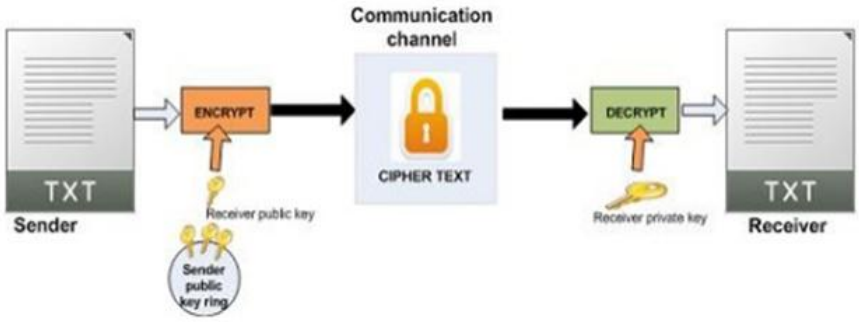


Fig. 3. Asymmetric cryptography.

In order to convert plaintext into cypher text, an algorithm known as a cypher is employed. This technique is known as encryption or enciphers (encode), and it works by turning readable and intelligible data into "worthless" data.

$$C = E_K(P) \quad (1)$$

E_K denotes the encryption algorithm that uses key K.

Decryption, or the process of turning "meaningless" data into readable data, is the reverse of ciphering and is known as deciphering (decoding), which is the procedure that recovers the cypher text.

$$P = D_{(K^{-1})}C \quad (2)$$

Caesar cypher is a widely used, simplified cypher algorithm that converts each character of plaintext into a numerical value. It adds the key value to the numerical value of each character of plaintext, and then divides the remaining

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

characters into cypher text characters using a modular value, where the modular value is the maximum numerical value plus one [13]. The Caesar cipher's mathematical model is

At encryption side: $E_n(x)= (x + n) \bmod p$ (3)

At decryption side: $E_n(x)= (x - n) \bmod p$ (4)

Table 1: Caesar Table

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Example 1:

Let the plaintext message is "PARVEEN KUMAR" and the key value=12, and use the simplest symmetric encryption algorithm, which called "Caesar cipher",

Plaintext	Encryption Process	Cipher Text
P→15	(15+12)mod 26	1→B
A→0	(0+12)mod 26	12→M
R→17	(17+12)mod 26	3→D
V→21	(21+12)mod 26	7→H
E→4	(4+12)mod 26	16→Q
E→4	(4+12)mod 26	16→Q
N→13	(13+12)mod 26	25→Z
K→10	(10+12)mod 26	22→W
U→20	(20+12)mod 26	6→G
M→12	(12+12)mod 26	24→Y
A→0	(0+12)mod 26	12→M
R→17	(17+12)mod 26	3→D

The cipher text which arrives to the receiver is “BMDHQQZWGYMD “, and the cipher text is entered into decryption process in the receiver to decrypt the text as follow:

Cipher Text	Decryption Process	Plaintext
B→1	(1-12)mod 26	15→P
M→12	(12-12)mod 26	0→A
D→3	(3-12)mod 26	17→R
H→7	(7-12)mod 26	21→V
Q→16	(16-12)mod 26	4→E
Q→16	(16-12)mod 26	4→E
Z→25	(25-12)mod 26	13→N
W→22	(22-12)mod 26	10→K
G→6	(6-12)mod 26	20→U
Y→24	(24-12)mod 26	12→M
M→12	(12-12)mod 26	0→A
D→3	(3-12)mod 26	17→R

More benefits come with symmetric encryption than asymmetric encryption. First off, because data encryption and decryption don't take much time, it is speedier. Second, secret key creation is simpler than asymmetric encryption. It does, however, have significant drawbacks, such as key distribution and sharing of the secret key between the sender and the recipient, as well as the incompleteness of symmetric key encryption for particular applications, such as

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

authentication [14]. Let's use the RSA model as an example of asymmetric encryption to better understand it. The basic phases of the RSA model are:

5.4 Steps for the RSA Model

- Each user produces a public/private key pair by randomly choosing two big primes, p and q.
- Calculating the modular value n = p×q
- Calculating φ(n) = (p-1) × (q-1), φ is the Euler's function
- Randomly selecting the public encryption key e, where e is a prime relative to φ(n) and 1 < e < φ(n).
- Finding the secret decryption key d , by solving the following equation:
  e×d=1 mod φ(n), and 0 ≤ d ≤ n.
- Sharing their public encryption key, which is P_k = (e, n).
  P_r= (d, n) is the secret private decryption key.
- The sender employs an encryption mathematical equation at the encryption side.
  C= p^e mod n.
- The receiver employs a decryption mathematical equation at the decryption side.
  P= c^d mod n.

Example 2:

Let a part of the plaintext message be " PARVEEN KUMAR ", thenthe RSA key generation process is:

- Select two prime numbers: p = 3 & q=11
- Computing n = p×q=3×11=33
- Computing Φ (n) = (p-1) × (q-1) =2X10=20.
- Selecting e: gcd (e, 20) =1, choose e=7.
- Determining d:d×e=1 mod 20 and d×7=1mod 20 we take d=3 that is, (3×7)mod 20 =1 so d=3, publishing public key P_k = (7,33)
- Keeping private key secret P_r = (3,33)

The encryption process and decryption process then is applied to previously calculated parameters as follows

Plaintext	Encryption Process
P→15	15^7 mod 33 = 27
A→0	0^7 mod 33 = 0
R→17	17^7 mod 33 = 8
V→21	21^7 mod 33 = 21
E→4	4^7 mod 33 = 16
E→4	4^7 mod 33 = 16
N→13	13^7 mod 33 = 7
K→10	10^7 mod 33 = 10
U→20	20^7 mod 33 = 26
M→12	12^7 mod 33 = 12
A→0	0^7 mod 33 = 0
R→17	17^7 mod 33 = 8

The cipher text will arrive the receiver, and at the receiver the cipher text will be entered into decryption process to decrypt the text as follows:

Decryption Process	Plaintext
27^3 mod 33 = 15	15→P
00^3 mod 33 = 0	00→A
08^3 mod 33 = 17	17→R
21^3 mod 33 = 21	21→V

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

16^3 mod 33 = 4	04→E
16^3 mod 33 = 4	04→E
07^3 mod 33 = 13	13→N
10^3 mod 33 = 10	10→K
26^3 mod 33 = 20	20→U
12^3 mod 33 = 12	12→M
00^3 mod 33 = 0	00→A
08^3 mod 33 = 17	17→R

VI. CONCLUSION

Modern security protocols use cryptography to encrypt data to keep it safe from prying eyes and enable secure two-way communication. In this paper, we studied a brief history of cryptography, terminology relating to cryptography, and how cryptography functions to protect data from being compromised or altered while being sent. We also discuss about the objectives and forms of it. We may infer that cryptography has become a crucial method to protect our private information because of the need of secure communication and the rise in use of cryptographic systems. In the future, we intend to expand our performance study findings and design new symmetrical and asymmetrical strategies.

REFERENCES

[1]. Aparajita and Rana, A. (2003) Steneography- The Art of Hiding Information: A comparison from Cryptography, International Journal of Innovative Research in Science, Engineering and Technology, 2(5), 1308-1312.

[2]. Bosworth, C. E. (1992) CODES- Encyclopaedia Iranica. https://iranicaonline.org/articles/codes-romuz-sg

[3]. Broemeling L. D. (2011) An Account of Early Statistical Inference in Arab Cryptology, The American Statistician, 65(4), pp. 255-257. DOI: https://doi.org/10.1198/tas.2011.10191

[4]. Bruen A. A. and Forcinito M. A. (2004) CRYPTOGRAPHY, INFORMATION THEORY, AND ERROR CORRECTION: A Handbook for the 21st Century, John Wiley & Sons Inc., New Jerseypp. 21.

[5]. C. Paar, C. and Pelzl J. (2010) Understanding Cryptography: A Textbook for Students and Practitioners, Springer, Hedelberg Dordrecht London New York.

[6]. Damico, T. M. (2009) A Brief History of Cryptography, INQUIRES, 1(11), .

[7]. Kahn, D. (1967) THE CODEBREAKERS: The Story of Secret Writing, SCRIBNER, Ney York.

[8]. B. Lennon (2018) Passwords: Philology, Security, Authentication, Harvard University Press, Cambridge, pp. 21.

[9]. Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S. Shebani, "Communication Cryptography",2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.

[10]. Qadir A. M. and Varol N. (2019) A Review Paper on Cryptography, In Proceedings of 2019 th International Symposium on Digital Forensics Security (ISDFS), IEEE, Barcelos, Portugal. DOI: 10.1109/ISDFS.2019.8757514.

[11]. Stein, W. (2017) Elementary Number Theory: Primes, Congruences and Secrets, Springer, New York.

[12]. Stinson, D. R. (2005) Cryptography: Theory and Practice Third Edition (Discrete Mathematics and its Applications), Chapman and Hall/CRC, London.

[13]. Stallings, W. : "Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA.

[14]. Thomas, K. : The Myth Of The Skytale ". Taylor Francis, (1998), Vol (33), pp: 244-260.

[15]. Computer Network Defense Course (CNDC), Army Reserve Readiness Training Center, Fort McCoy WI, http:/arrtc.mccoy.army.mil, Jan. 2004.

[16]. "How to improve JavaScript cryptography." : http://hellais.wordpress.com/2011/12/27/how-to improve-java script-cryptography/.