

A Review on Cryptography

¹Gyanvendra Pratap Singh, ²Garima Gupta

¹Assistant Professor, ²M.Sc Mathematics (IV Sem)
Department of Mathematics and Statistics
Deen Dayal Upadhyaya Gorakhpur University
Gorakhpur-273009, (U.P.)-INDIA
Email:gpsingh.singh700@gmil.com¹,

Abstract- In the era of digitalization, use of internet is our part of life. The Internet merges with our lives and grown explosively over the last several decades. Data security is the main trouble for everyone on the internet. Data security ensures that our data is only accessible by sender and receiver. Cryptography prevents our data from being accessed by any third party and person. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography is a technique to encrypt the data by using some algorithms and prevent it or made it indecipherable to the unauthorized parties unless it is decrypted by the receiver using the same algorithms which is used by the sender. In this paper we study the various type of algorithms to encrypt and prevent the message by using cryptography.

Keywords: Cryptography, Network security, Algorithms, Encryption, Decryption, Cipher, Data security.

1- INTRODUCTION

Cryptography is the key to secure our messages. Generally Cryptography protects our private messages from third parties or the public. Cryptography comes from the Greek word “crypto” which means hiding and “Graphy” means writing i.e., secret writing. Nowadays, however, the privacy of individuals and organizations is provided through cryptography at a high level, making sure that information is sent securely in a way so that the authorized receiver can access this information [1].

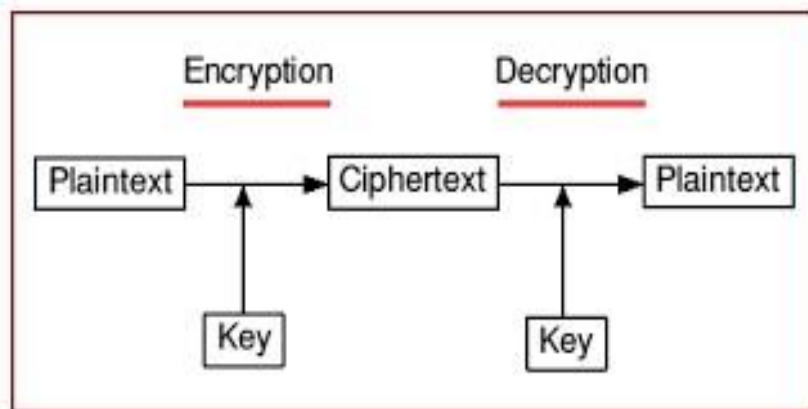


Figure 1: Procedure of Cryptography

The historical background of cryptography is that the first known evidence of the using cryptography was found in an engraving sculpted around 1900 BC in Egypt on the tomb of the nobleman Khnumhotep II. However, the science of cryptography was initiated by Arabs since 600s. Cryptography becomes vital in the twentieth century where it played a crucial role in the World War I and II. [2]

2- LITERATURE REVIEW

Tayal et al. [3] mentioned that the world generates a large amount of data daily. This large amount of data is generated by the emergence of ecommerce applications and social networks, organizations across the world. And for the security of the data transmission is the most extreme basic issue in guaranteeing safe transmission. But somehow it attracts a lot cyber - attacks. So we have to protect computer and network security.

Rawat et al. [4] referred as there is a drastic growth in the exchange of information through the emergence of new media age. They are growing and shift their offline schedule to online. Because of online schedule there is data and information

sharing through the internet and it leads to the e-crime or cyberterrorism. So we have to secure our information and data from the cyberattacks.

Jyothi et al. [5] referred as for the data transmission through the wireless network, cryptography is being used. Network security is one of the main concerns as the world transitions into the digital world. For safe communication we use encryption techniques such as cryptography, digital signatures, watermarking, steganography and other applications. Cryptography is a technique of encryption used to protect the network.

Khalifa et al. [6] referred as for the growth of technologies communication plays an important role in this age. For making the communications more prevalent we need to involved electronics security. Therefore a mechanism is needed for security and privacy of information. Whether the communication is wired or wireless. The method of transforming the original information into the unreadable format is called encryption and decryption and the study of encryption and decryption is called cryptography.

Hellman et al. [7] introduce the importance of cryptography in the military and diplomatic communities. It is also to attract much commercial attention. It is also the study of rapid computerization of information storage, transmission and spying.

Nagaraj et al. [8] referred as for the transactions, e- payments in secure commerce and payment application need security for communications. And we protect the sensitive information by using fundamental tool of encryption. They proposed a new method on the basis of Euler's Totient theorem to produce a set of numbers that encrypt the data.

Qadir et al. [9] pointed out that our lives merges with internet and it is growing explosively, data security is the main trouble for anyone. Data security ensures that our data is accessible by sender and receiver and for this level of security we have to use some algorithms. Cryptography is the technique to protect our data.

Varol et al. [10] referred as security against cyber-attacks is necessary for the world. In this, they study about the cyber-attacks and analysis output models. For the security scenario they apply statistical calculation methods to the analysis and give a new model.

Jirwan et al. [11] referred as data communication is mainly depends upon digital data communications. And our first priority is data security. For providing the security we have to use cryptography techniques. They define the different type of cryptography such as symmetric and asymmetric.

Sharma et al. [12] referred as nowadays data security become crucial aspect in every sector. Various methods and algorithm have been used to protect it. There are many of companies stores business and individual information on computer. The information stored is highly confidential and not for public.

They define the cryptography algorithm which is based on block cipher concept.

Garg et al. [13] referred as the procedure of cryptography is to secure data communication in the presence of third party. For secure data transmission over network cryptography is used by selected some algorithms which fulfil the conditions of integrity protection, conventional message authentications and digital signatures, PN numbers are used for encryption.

Agrawal et al. [14] referred as network security is increasing at full speed and become major challenging issue. The security threats and attacks on internet are more strenuous to detect. For security of the system encryption plays an important role. For the shared data many techniques are required to protect. They define four encrypt techniques AES, DES, 3DES and E-DES algorithms.

Preneel et al. [15] referred as the state of the art of cryptographic code of behaviour as posted for securing computing networks. For securing a large scale network, the easy way to design a efficient cryptographic algorithms. They define key words cryptographic algorithms, network security, block ciphers stream cipher.

Panda et al. [16] studied for wireless sensor network which is consists of autonomous sensor nodes attached to one or more base station. Identify the suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy. Symmetric cryptography schemes do not scale well while public key cryptography schemes are widely used.

3- HISTORICAL BACKGROUND OF CRYPTOGRAPHY

It was probably thought that earliest thought of Cryptography was in Egyptian town of Menet Khufu. Cryptography probably begin around 2000 B.C. in Egypt, where hieroglyphics were used to decorate the tombs of deceased rulers and kings. Which is used on the tomb of nobleman KHNUMHOTEP II.

Some evidence of use of cryptography has been seen in early civilizations. "Arthshashtra" a classical work on statecraft scripted by Kautalya, define the espionage service in India and mentions giving assignments to spies in "secret writing".

World War I is the second largest military conflict in history. The Zimmerman Telegram was a telegram from Germany to Mexico containing essential war information about The Great War - World War I. It included the Germans' plans for unrestricted submarine warfare, as well as a proposal asking Mexico to ally with the Germans and invade the US.

3.1- CIPHER TECHNOLOGIES USED IN WORLD WAR I

The Vigen`ere disk, code books and different methods of transposition ciphers were widely used ciphers in World War I. These ciphers were hundreds of year old and had solutions.

The Vigen`ere disk consists of 2 rings of the alphabet that spin on a central axis. The smaller ring was inside the larger one and it would be rotated on the centre. Both rings are divided into 24 equal parts and each part containing a symbol. In the large ring there was all uppercase letters in the Latin alphabet (except H, J K U W and Y) in the proper order, as well as the number 1 to 4.

In the small ring there was all lowercase letters (except j, u and w) in a random order, as well as the `&` symbol. There are some missing letters are not part of the Italian alphabet.



Figure 2: Vigen`ere disk

Because of the radio communication, cryptography was used widely in the World War II. But by the radio, messages could be intercepted, so secret information had to be transmitted in secret codes. There are complex machines that turned ordinary text in secret codes. A German machine called Enigma and an American device known as SIGABA are used in World War II

4- CONCEPT OF CRYPTOGRAPHY

The basic concept of cryptography is information about all type of cipher or data transformation safely to unauthorized person. Two of the most common uses of cryptography would be using it to transmit data through an insecure channel, such as the internet, or ensuring that unauthorized people do not understand what they are looking at in a scenario in which they have accessed the information. [17]

In Cryptographic system some terminologies are used, **“Plain Text”**- the original data or message we have to send. **“Encryption”**- the process of converting from plain text to cipher text is known as encryption. **“Decryption”**- the reverse process of changing from cipher text to plain text is known as decryption. **“Ciphers”**- codes or policy of hidden the message are known as ciphers. **“Cipher Text”** - when a Plain Text message transform into a secret form by using suitable scheme or algorithm, the resulting message is known as Cipher Text. **“Crypto System”**- Hardware or software implementation of cryptography that transform a message to the cipher text and back to the plain text is known as crypto system. **“Crypto Analysis”**- crypt analysis is technique of decoding cipher text into plain text without knowing how they are initially converted from plane text to cipher text. In other word crypt analysis is an art of breaking the secret code. **“Encipher”**- art of transforming data into an unreadable format. **“Decipher”**- art of transforming data into a readable format. **“Key”**- security sequence of bites and instruction that govern the art of encryption and decryption.

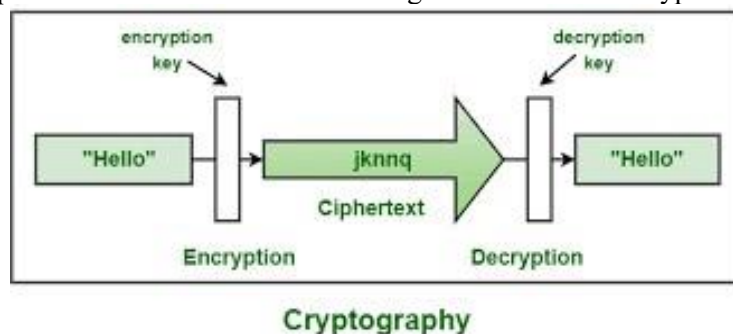


Figure 3: Cryptography

Basically there are two type of cryptography one is symmetric key cryptography or private key cryptography and second one is asymmetric key cryptography or public key cryptography.

5- PRIVATE KEY CRYPTOGRAPHY

Private key cryptography is also known as secret key cryptography or symmetric key cryptography. In this cryptography one key is used for both encryption and decryption.



Figure 4: Private Key Cryptography

6- PUBLIC KEY CRYPTOGRAPHY

Under the system of pair of keys are used to encrypt or decrypt the information. A public key is used for encryption and a private key is used for decryption.

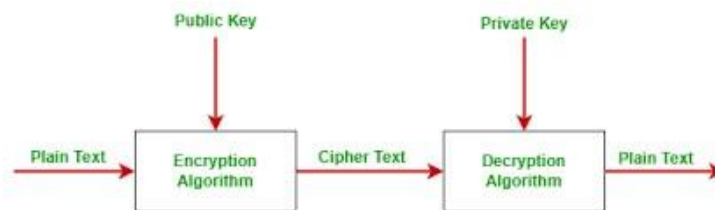


Figure 5: Public Key Cryptography

Public key and private key are different. Even if the public key is known by everyone but the private key is known by anyone.

7- CATEGORIES OF CLASSICAL CIPHERS

7.1 Substitutions Ciphers

7.1.1 Mono-alphabetic

1. Additive cipher- In this cipher the plain text consists of lower cases letter and the cipher text consist of uppercase letter. The secret key K is an integer between 0 to 25.

Encryption: $C \equiv (P + K)(mod26)$

Decryption: $P \equiv (C - K)(mod26)$

2. Shift Cipher- Additive ciphers are called shift Cipher.

3. Caesar Cipher- The Caesar involves replacing each letter of the alphabet with letter standing three places further down the alphabet. The Caesar cipher used a key K=3 in additive Cipher.

Encryption: $C \equiv (P + 3)(mod26)$

Decryption: $P \equiv (C - 3)(mod26)$

4. Affine Cipher- In this cipher, for encrypt the message we use the formula,

$Y = (ax + b)(mod26)$

Where x is numerically equivalent to the corresponding letter and $gcd(a,26)=1$, $a = 1,3,5,7,9,11,15,17,19,21,23,25...$

$b \in 0,1,2,3,4...25$.

Decryption Formula is

$$Y - b \equiv ax \pmod{26}$$

$$x \equiv a^{-1}(Y - b) \pmod{26}$$

7.1.2- Poly-alphabetic

1. Auto Key Cipher-It is a polyalphabetic substitution cipher. It is related to the Vigenere cipher but it uses a different method of generating the key.
2. Playfair Cipher-The secret key in this cipher is made of 25 alphabets letter arranged in 5x5 matrix. Usually the letter I & J counted as 1 letter.
- 3.Hill Cipher- In this cipher the plain text is divided into equal size of blocks. The blocks are encrypted once at a time in such a way that each character in the block contributes to the encryption of the other character in the block.

$$C \equiv KP \pmod{26} \tag{1}$$

$$\begin{bmatrix} C1 \\ C2 \\ C3 \end{bmatrix} \equiv \begin{bmatrix} K11 & K12 & K13 \\ K21 & K22 & K23 \\ K31 & K32 & K33 \end{bmatrix} \begin{bmatrix} P1 \\ P2 \\ P3 \end{bmatrix} \pmod{26} \tag{2}$$

Here the key in a Hill Cipher is a square matrix and also the key matrix must be a non singular matrix.

For decryption we use the formula

$$P \equiv (K^{-1}C) \pmod{26} \tag{3}$$

4. Vigenere Cipher- Vigenere Cipher used a different step to create the key stream for encryption and decryption as follows

$$C_i \equiv (P_i + K_i) \pmod{26}$$

$$P_i \equiv (C_i - k_i) \pmod{26}$$

Where $P_i = P_1, P_2, P_3, \dots$

$K = (K_1, K_2, \dots)(K_1, k_2, \dots) \dots C = C_1, C_2, \dots$

5. Vernam Cipher- In this Cipher we use following encryption and decryption formula

For encryption-

$$C_i \equiv (P_i + K_i) \pmod{26}$$

For decryption-

$$P_i \equiv (C_i - K_i) \pmod{26}$$

7.2- Transposition Ciphers

1. Rail Ferner Cipher- In this Cipher the plain text is written downward in the successive range of an imaginary fence then move up we get to the bottom. Write down a plain text message as a sequence of diagonal then read the plain text written in above.
2. Simple Columnar with multiple round- The cipher is to use some basic idea of Rail cipher. In this cipher the permutation of key is given.

8- CATEGORIES OF PUBLIC KEY

8.1- Diffie-Hellman key exchange

It is not a encryption algorithm. It is used to exchange the secret key. We will use asymmetric encryption to exchange the secret key. The algorithm says that consider a prime number q and select α such that it must be the primitive root of q and $\alpha \leq q$

'a' is primitive root of q if

$$a \pmod q$$

$$a^2 \pmod q$$

$$a^3 \pmod q \dots$$

gives result $\{1, 2, 3, \dots, q - 1\}$

i.e. values should not be repeated & we should have all values in the set from 1 to q-1.

1) Discrete logarithms

2) key exchange protocols

3) man in the middle attack

8.2- Elgamal Cryptographic System

As with Diffie Hellman, the global elements of Elgamal are a prime number q and α . A Public key pair is define as-
Key Generation-

Select large prime number (p)

Select decryption key/ private key(D)

select second part of encryption key or public key(E_1)

Third part of encryption key or public key (E_2). $E_2 = E_1 \text{ mod } P$

Public key= (E_1, E_2, P) , Private key= D

Encryption-

Select random integer (R)

$$C_1 = E_1^R \text{ mod } P$$

$$C_2 = (PT * E_2^R) \text{ mod } P$$

$$C.T = (C_1, C_2)$$

Decryption-

$$PT = [C_2 * (C_1^D)^{-1}] \text{ mod } P$$

8.3- Elliptic Curve Cryptography

It is asymmetric/ public key cryptosystem, it has small key size and high security. It makes use of elliptic curves. Elliptic curves are defined by some mathematical function, cubic function

eg. $Y^2 = X^3 + aX + b$

- 1) RSA
- 2) Abelian Groups
- 3) Elliptic curves over Real numbers
- 4) Elliptic curves over Z_p
- 5) Elliptic curves over $GF(2^m)$

8.4- Pseudorandom number Generation based on an asymmetric cipher.

A Symmetric block cipher produces an apparently random output, it can be the basic of a pseudorandom number generator. Similarly, an asymmetric encryption algorithm produces apparently random output and can be used to build a PRNG[18]. Because asymmetric algorithms are much slower than symmetric algorithm.

- 1) PRNG Based on RSA
- 2) PRNG based on Elliptic curve cryptography

9 MODERN CRYPTOGRAPHY

9.1 For secret key cryptography

- 1) DATA ENCRYPTION STANDARD (DES)- DES was construct by IBM in the 1970 and adopted by the National Bureau of Standards(NBS) for commercial and unclassified government application, in 1977.It is the most common scheme which is used today. NBS is now National Institute for standards and Technology(NIST)
- 2) ADVANCED ENCRYPTION STANDARD(AES)- NISTinitiated a very public, 4-1/2 years process to develop a new secure cryptosystem for U.S. government applications, in 1977. In December 2001, the result of the Advanced Encryption Standard became the official successor to DES.
- 3) CAST-128/256-CAST-128, described in request for comments (RFC) 2144, is a DES-like substitution-permutation crypto algorithm, employing a 128- bit key operating on a 64 bits block. CAST-256 (RFC 2612) is an extension of CAST-128.[19]
- 4) INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)-In 1922 Xuejia Lai and James Massey writes Secret-Key cryptosystem and patented by Ascom; a 64 bits SKC block cipher.
- 5) RIVEST CIPHERS (aka Ron's Code)- It is named Ron Rivest, a series of SKC algorithms.
- 6) BLOWFISH- It is invented by Bruce Schneier. It is a symmetric 64 bits block cipher which is optimized for 32 bit processors with large data catches. It is sufficiently faster than DES.
- 7) TWOFISH- It is a 128 bits block cipher by using 128192,or 256 bits keys, which is designed to be highly secure and highly flexible.

9.2 For public key cryptography.

- 1) RSA- Today is most used in hundreds of software products and can be used for key exchange, digital signature. RSA uses a various size encryption block and a varia ble size key.
- 2) DIFFIE-HELLMAN- After the RSA algorithm, Diffie and Hellman came up with their own algorithm. It is used for secret key exchange only not for digital signature.
- 3) DIGITAL SIGNATURE ALGORITHM (DSA)-This algorithm is designated in NIST's Digital Signature Standard, provides Digital Signature capability for the authentications of messages.
- 4) ElGamal- It is designed by Taher Elgamal, which is similar to Diffie Hellman for key exchange.
- 5) Elliptic Curve Cryptography- It provides a level of security with small keys comparable to RSA and other PKC methods. It is designed for such devices which have limited compute power.

- 6) Public Key Cryptography Standards (PKCS)-This is designed by RSA data security. It is a set of interoperable standards and guidelines for public key cryptography.
- 7) Cramer Shoup- In 1998, R. Cramer and V. Shoup of IBM proposed a public key cryptosystem.
- 8) Key Exchange Algorithm(KEA)- Variation in Diffie Hellman they proposed as the key exchange method for Capstone.
- 9) LUC- It is designed by P.J. Smith and based on Lucas sequences. It can be used for encryption and signatures, using integer factoring.

9- SOME EXAMPLE ON CRYPTOGRAPHY

Example no. 1: Encrypt and decrypt the message “India is not safe” by using symmetric key cryptography(Shift cipher) with using the key K=8

Solution: For encrypt the message first we write the alphabets of lower case letters(a,b,c,d,...) then note the key and place value of key (e.g. K=8 and 8 is place value of ‘i’). Now start from I with upper case letter(A,B,C,D,...) subsequently move forward till Z, and again start with A in the same way.

to convert into the cipher text first look at the plain text, go to the small alphabetic chart , identify the corresponding capital letter from the chart for the each alphabets of the plain text and write it into the cipher text.

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

Plain Text: India is not safe.

Cipher Text: QVLQIQAVWBAINM

Now for converting the cipher text into Plain text, reverse the process.

Cipher Text: QVLQIQAVWBAINM

Plain Text: India is not safe.

Example no. 2- Encrypt and decrypt the message “there is a major problem” by using symmetric key cryptography (Hill cipher) with using the key $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

Solution: Here $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

$$|K| = 11 \neq 0$$

$$\gcd(|K|, 26) = 1$$

$$K^{-1} = 1/11 \begin{bmatrix} 7 & -2 \\ -5 & 3 \end{bmatrix}$$

$$Plaintext = \begin{bmatrix} t & e & e & s & m & j & r & r & b & e \\ h & r & i & a & a & 0 & p & o & l & m \end{bmatrix}$$

$$Placevalue = \begin{bmatrix} 19 & 4 & 4 & 18 & 12 & 9 & 17 & 17 & 1 & 4 \\ 7 & 17 & 8 & 0 & 0 & 14 & 15 & 14 & 11 & 12 \end{bmatrix}$$

$$Encryption C \equiv (KP)(mod26)$$

$$C \equiv \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 19 & 4 & 4 & 18 & 12 & 9 & 17 & 17 & 1 & 4 \\ 7 & 17 & 8 & 0 & 0 & 14 & 15 & 14 & 11 & 12 \end{bmatrix} (mod26)$$

$$\begin{aligned} &\equiv \begin{bmatrix} 71 & 46 & 28 & 54 & 36 & 55 & 81 & 79 & 25 & 36 \\ 144 & 139 & 76 & 90 & 60 & 143 & 190 & 183 & 82 & 104 \end{bmatrix} \pmod{26} \\ &\equiv \begin{bmatrix} 71 & 46 & 28 & 54 & 36 & 55 & 81 & 79 & 25 & 36 \\ 144 & 139 & 76 & 90 & 60 & 143 & 190 & 183 & 82 & 104 \end{bmatrix} \\ &\equiv \begin{bmatrix} T & U & C & C & K & D & D & B & Z & K \\ 0 & J & Y & M & I & N & I & B & C & A \end{bmatrix} \end{aligned}$$

Cipher text: TOUJCYCMKIDNDIBBZCKA.

Now for decryption $P \equiv (K^{-1}C) \pmod{26}$

$$\begin{aligned} K^{-1} &= \frac{1}{11} \begin{bmatrix} 7 & -2 \\ -5 & 3 \end{bmatrix} \\ &= 19 \begin{bmatrix} 7 & -2 \\ -5 & 3 \end{bmatrix} \pmod{26} \\ &= \begin{bmatrix} 133 & -38 \\ 95 & 57 \end{bmatrix} \pmod{26} \\ &= \begin{bmatrix} 3 & 14 \\ 9 & 5 \end{bmatrix} \pmod{26} \end{aligned}$$

Now, $P \equiv (K^{-1}C) \pmod{26}$

$$\begin{aligned} &= \begin{bmatrix} 3 & 14 \\ 9 & 5 \end{bmatrix} \begin{bmatrix} 71 & 46 & 28 & 54 & 36 & 55 & 81 & 79 & 25 & 36 \\ 144 & 139 & 76 & 90 & 60 & 143 & 190 & 183 & 82 & 104 \end{bmatrix} \pmod{26} \\ &= \begin{bmatrix} 253 & 186 & 342 & 174 & 142 & 191 & 121 & 17 & 103 & 30 \\ 241 & 225 & 138 & 78 & 130 & 92 & 67 & 14 & 235 & 90 \end{bmatrix} \pmod{26} \\ &= \begin{bmatrix} 19 & 4 & 4 & 18 & 12 & 9 & 17 & 17 & 1 & 4 \\ 7 & 17 & 8 & 0 & 0 & 14 & 15 & 14 & 11 & 12 \end{bmatrix} \\ &= \begin{bmatrix} t & e & e & s & m & j & r & r & b & e \\ h & r & i & a & a & 0 & p & o & l & m \end{bmatrix} \end{aligned}$$

Plain text: there is a major problem.

10- Conclusion

In the current situation everyone wants to secure their data and private information through the network security. Cryptography is the technique to protect the data from third party and give everyone's faith on internet or computer. In this paper, a short history of cryptography, definitions related to cryptography, types of cryptography, types of keys use in cryptography and few examples related to encryption decryption.

REFERENCES:

1. A.M Quadir, Nurhayat Varol, "A Review paper on Cryptography"
2. O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.
3. Sandeep Tayal N. Gupta, D Goyal and M Goyal A review paper on "Network security and cryptography" Advances in computational science and technology, vol. 10, no. 5, pp.763-770, 2017.
4. Esha Rawat, Anuska Singh, Alap Mahar, Prof. Amit Agarwal, A Review Paper on "Cryptography and Network security" Department of Computer Science and Engineering, Dr. APJ Kalam Institute of Technology, May 15, 2022.
5. V. Esther Jyothi, Dr. BDCN Prasad, Dr. Ramesh Kumar Mojjada, "Analysis of Cryptography Encryption for network security" IOP Conf. Series: Materials Sciences and Engineering 981(2020).

6. O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.
7. Martin E. Hellman, "An Overview of public key cryptography", originally published in IEEE Communications Magazine, November 1978- Volume 16, Number 6.
8. Srinivasan Nagaraj, Dr. G. S. V. P. Raju, V. Srinadth, "Data Encryption and Authentication Using Public Key Approach", International Conference on Intelligent Computing, Communication & Convergence, (ICCC-2015) Procedia Computer Science 48 (2015) 126 – 132.
9. Abdalbasit Mohammed Qadir, Nurhayat Varol, "A Review Paper on Cryptography", Firat University Elazig, Turkey, Conference Paper · June 2019.
10. Asaf Varol, Omer Durmu, s , "Analysis and Modeling of Cyber Security Precautions", 2021 9th International Symposium on Digital Forensics and Security (ISDFS).
11. Nitin Jirwan, Ajay Singh, dr. Sandip Vijay, "Review and analysis of Cryptography Techniques" International journal of Scientific and Engineering Research, vol. 3, no. 4, pp. 1-6, 2013.
12. [12 Neha Sharma, Prabhjot and Er. Harpreet Kaur, "A Review of Information Security using Cryptography Technique", International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.
13. Pranab Garg, Jaswinder Singh Dilawari, "A Review paper on Cryptography and Significance of Key Length", International Conference On Emerging Trends In Engineering, ICTIE/155, October 2012.
14. Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering(IJCSE),Vol. 4 No. 05 May 2012, pp. 877-882.
15. Bart Preneel, " Cryptography for Network Security: Failures, Successes and Challenges", In Conference of the 5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, Dec. 2010, pp. 36-54.
16. Madhumita Panda, "Security In Wireless sensor Networks Using Cryptography Techniques", In American Journal of Engineering Research(AJER), 2014, Vol-03, Issue-01, pp-50-56.
17. Abdalbasit Mohammed Qadir, Nurhayat Varol, "A Review Paper on Cryptography", Firat University Elazig, Turkey, Conference Paper · June 2019.
18. William Stallings, "Cryptography and network security", Sixth edition, ISBN 9780133354690, Published by Pearson Education Inc.2014.
19. M Kundalakesi, Sharmathi. R, Akshaya. R, "Overview of Modern Cryptography" International Journal of computer Science and Information Technologies, Vol.6, 2015, 350-353.