ALGORITHM DESCRIPTION ENCRYPTION TECHNIQUES

Amit Verma [1*], Karamjeet singh [1], Ranjeeta Kaushik,Bharti[2] Chhabra [3]

[1] Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[1]M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College, Landran, Punjab, India

[2 and 3]Assistant Professor, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India

Abstract: - In recent years, network security has become an important issue. Encryption has become a solution and plays an important role in information security systems. Many techniques are needed to protect shared data. Current work is focused on cryptography to protect data as it travels across the network. First, the data transmitted from the sender to the receiver in the network must be encrypted using an encryption algorithm. Second, by using decryption technology, the receiver can view the original data. In this paper, we presented two encryption techniques, such as Blowfish, and RSA algorithms. In this paper, we presented different encryption techniques, like RC4, Blowfish, AES, DES, triple DES, RSA and Blowfish. The comparison on the basis of speed, key size and security is also presented, which shows that the speed of AES is higher than other encryption algorithms.

I. INTRODUCTION

Each user needs a secure network for communication in order to communicate Safe and no intruders can read their data. To provide secure data communication Cryptography for wireless and wired networks is used in which cryptography converts plain text into cipher text. In the transmitter side plain text is converted into cipher text by using the process known as "Encryption" and on the receiver side reverse process is performed, which is known as "decryption"[1].

Cryptography is the practice and research of secure communication technology in the presence of the third parties; more usually, it's about building and analyzing related protocols to provide information security. Cryptographic applications comprise of ATM cards, computers Password and e-commerce etc[2]. The terms such as Plain text and Cipher text are used in Cryptography, which are defined below:

Plain text: It an original information

Cipher text: The original message is converted into coded form, which is known as "Cipher text".

Encryption: The term which is used to transmit plain text into cipher text in known as Encryption technique.

Decryption: To extract plain text from cipher text is known as Decryption technique [3].

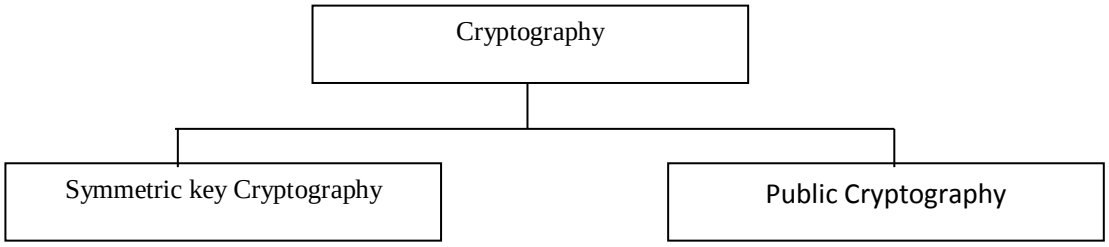

Figure 1: Types of Cryptography

i. Symmetric key Cryptography

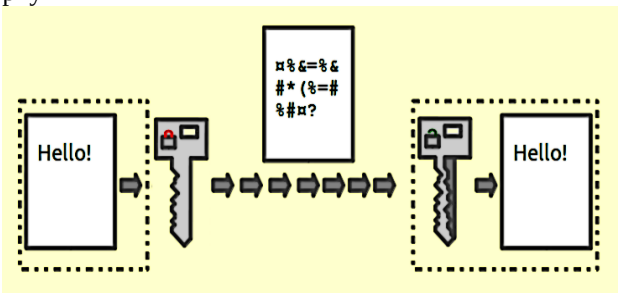

Figure 2: Symmetric key encryption

This is the simplest encryption technique in which the sender and receiver have same key to encrypt or decrypt data for providing secure communication. From the figure 2, it is clear that the message we want to send is "Hello". Hello is converted into coded text so that the data remains secure and at the receiver we get the same data i.e. "Hello" by using some description algorithms [4].

II. PUBLIC CRYPTOGRAPHY

In public-key encryption method, encryption key release for anyone to use and encrypted messages. However, only the recipient can access the decryption key to the messages can be read.

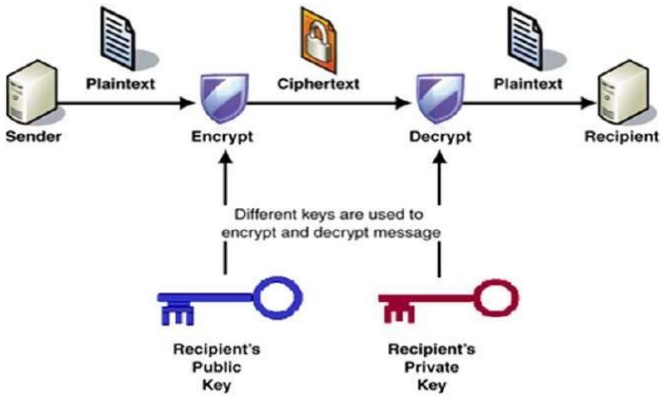

Figure 3: Public key cryptography

From the above figure, it is clear that different keys are used for encryption and decryption [5].

Table 1 Comparison of different Encryption techniques

Encryption techniques	RC4	Blowfish	AES	DES	Triple DES
Speed	Very High	High	High	Low	Very Low
Is speed depends upon key size	No	No	Yes	Yes	No
Security	Might be secure for reasonable numbers of encrypted process of reasonable length. RC4 has the saving feature of being fast.	Believed secure, but with less attempted cryptanalysis than other algorithms. Attempts to cytolyses Blowfish soon after publication are promising, but similar to AES, this technique does not obtained much attention. Similar to Two fish algorithm, this algorithm is not supported by Java language.	It is secure as it has the benefit of permitting the 256-bit key size that helps to secure data against attack such as collision attacks.	This algorithm is not secure.	Insecure

i. RSA

In modern computer RSA algorithm is used to encrypt and decrypt messages. It is an asymmetric encryption algorithm. Asymmetry means that two different keys. It is also known as public key cryptography, because one of them will be given to each person. Another key must be kept private. The RSA Operations is defined in figure 4.

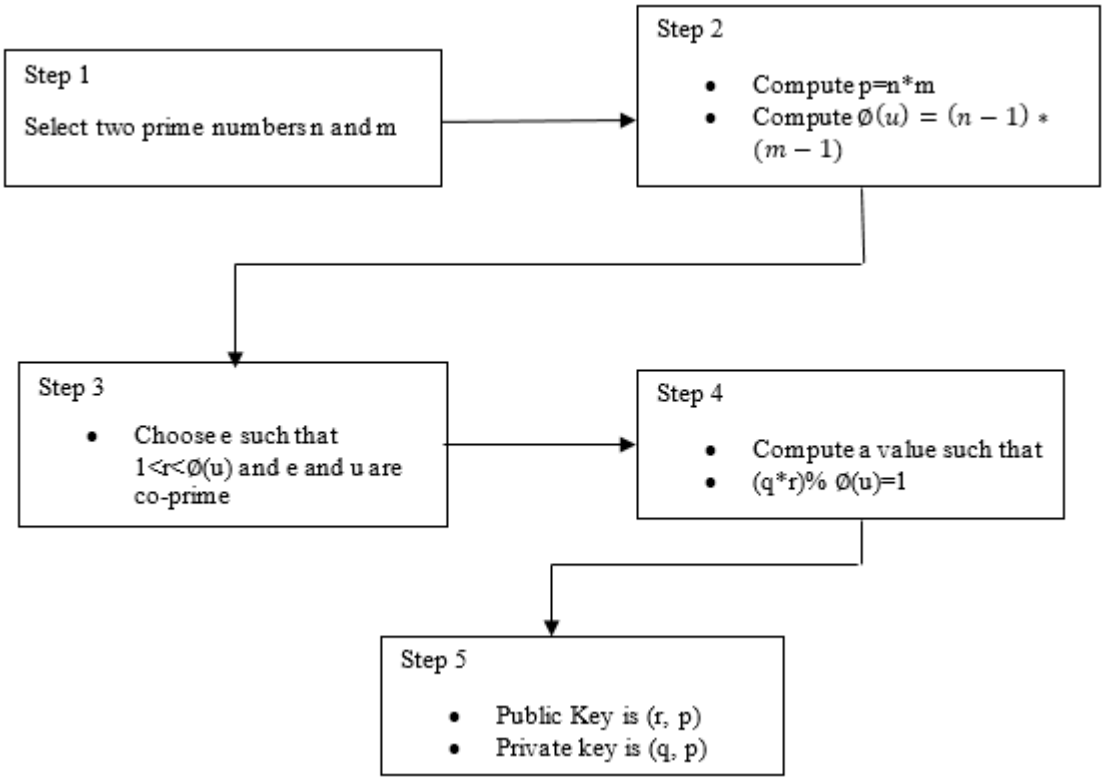

Figure 4: Flow chart of generation of public and private key in RSA

In RSA two keys Public Key and Private Key are used. Everyone knows the public key, which is used to encrypt messages. The messages which are encrypted with the Public key could only be decrypted with the Private Key [6].

ii. BLOWFISH ALGORITHM

The Blowfish is another algorithm developed by Bruce Schneier in 1993 and designed to replace DES. This symmetric cryptographic breaks message into 64-bit blocks and encrypt them individually. Blowfish can be found in the software category, from e-commerce platform to payment protection to protect password management tools. It is undoubtedly one of the most flexible encryption methods. Their great speed and overall efficiency are well known, as many people claim that they have never been defeated. At the same time, providers have made the most of their free availability in the public domain [7].

Blowfish is a symmetric block encryption algorithm designed with,

- **Fast:** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
- **Compact:** It can run in less than 5K of memory.
- **Simple:** It uses addition, XOR, lookup table with 32-bit operands.
- **Secure:** The key length is variable, it could be in the range of 32 to448 bits: default 128 bits key length.
- It is suitable for applications where the keys are not changes very fast like communication link or an automatic file encryption.

i. Blowfish algorithm structure

Blowfish has a 64-bit block size and anywhere from 32-448 key length. It is a 16-round encrypted Feistel and uses large S-boxes relative to the key. It is similar to the use of fixed S-boxes in structure to CAST-128 [8].

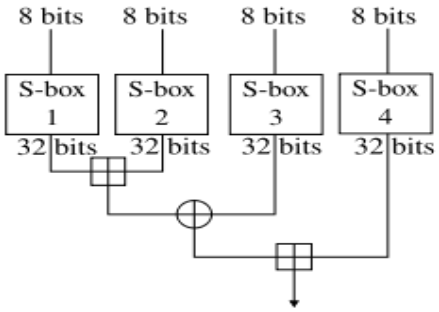

Figure 5: Block diagram of BlowFish

As shown in the figure above 8 bit data input is given to each of the S-Box which produces 32-bit output. Each line here represents 32 bits. This algorithms has two sub keys which consists of 18-entry P-array and Four 256- entry S-boxes. In every round one entry of the P-array is used, each

half of the data block is XORed with one of the two remaining unused P-entries [9]. Blowfish's F-function is shows in the right of the diagram. The function splits the 32-bit input into four eight-bit quarters, and uses these quarters as input to the S-boxes. The outputs are added to 232 modulo and XORed to get the final 32-bit output [10].

III. RELATED WORK

D.I.George Amalarethinam et al [11] introduced a level of security by using singly even magic rectangle. It increases the calculated value in the cipher text. In this paper same cipher value is repeated and the cipher text is in the format of image. In this even same value get repeated, it assigns different values for each occurrence. **Manoj patil et al. [12]** proposed a technique of sending SMS text using combination of compression and encryption. The ended data will be first encrypted using Elliptic curve Cryptographic technique, But the length of encrypted data is so large so we have to compress the data so that data can be send in short duration, Compress technique that is implemented here will compress the data up to 99.9%, hence the large bandwidth get saved. **Yashpalsingh Rajput et al. [13]** presented an advanced scheme to encrypt the plain text message for its security. Whole of the conventional encryption techniques are every weak and traditional cryptanalysis could be used to early determine the plain text from encrypted text. In this paper a new concept is used to increase the security of the text which is stronger and secure than the earlier concept. **Vinay Verma et al [14]** has proposed an efficient symmetric key based security approach which develop dynamic key from a file of multimedia to encrypt multimedia data. In this technique, dynamic key has chosen randomly from the multimedia file by using special function. **Dimple et al.[15]** presented different encryption techniques like (RSA) Rivest Shamir and Adleman, Diffie-Hellman, (Digital Signature Algorithm) DSA are analyzed. It is experienced that in Diffie-Hellman cryptography algorithm secret keys are exchanged between two users. In DSA a digital signature is used to confirm that the signal received is unchanged. **Nentawe Y. Goshwe. et al. [16]** implemented data encryption and description in a network environment . This paper used RSA algorithm for encryption description of the data. In this algorithms sender generate a public key to encrypt message and at the receiver end a private key is generated using a secure database. If the generated private key is wrong then it still decrypts the encrypted message but it is different from the original message. **Rohan Rayarikar et al. [17]** performed a work, "SMS Encryption using AES Algorithm on Android". Author has developed an application on Android platform which allows the user to encrypt the messages before it is transmitted over the network.

Table 2: Comparison of existing techniques

Author	Year	Proposed Techniques	Outcome/Advantages	Limitations
Xin Zhou, Xiaofei Tang [18]	2011	RSA algorithm	High sped and provide security	Problem for RSA encryption on the file, it indicates the RSA mathematical algorithms in the computer industry's importance And its shortcomings.
Wen-Xiang Zhang,Si-You Xiao,Yi Zhang [19]	2010	IDEA algorithm; X-IDEA algorithm	provide secure transmission of graphic-text used in mobile phones, and more suitable for 3G communication	Computing power cannot be compared with the computer
Dr. V.K. Govindan1 B.S. Shajee mohan2 [20]	2005	Huffman encoding, arithmetic encoding, the LZ (Lempel-Ziv) family,DMC (Dynamic Markov Compression) PPM (Prediction by Partial Matching), and BWT (Burrows-Wheeler Transform) Based algorithms.	In an ideal channel, the reduction of transmission time is Directly proportional to the amount of compression.	In Internet scenario with fluctuating bandwidth, congestion and protocols of packet switching, this does not Hold true.
Dawn Xiaodong Song David Wagner Adrian Perrig [21]	2000	Controll searchinf scheme,Schem for hidden search	They are secure. They provide question isolation for searchers They provide controlled searching. Support hidden quarries. The algorithm applied here is simple and fast	whenever Alice changes her documents, she must update. The index. There is a trade-off between how much index Alice updates and how much information Bob might be able to learn.

IV. PARAMETERS MEASURED

Following are the parameters included for simulating the environment:

i. Precision: It is the ratio of the number of relevant data record retrieved to the total number of irrelevant data records in the encryption technique. It is defined as

$$Precision = \frac{Relavant\ Data - Retrieved\ data}{Retrieved\ Data}$$

ii. Recall: It is the ratio of the number of relevant data record retrieved to the total number of relevant data records in the encryption technique. It is defined as

$$Recall = \frac{Relavant\ Data - Retrieved\ data}{Relavant\ Data}$$

iii. F-measure: The measure in which the combination of precision and recall takes place is the F-measure.

$$F = 2.\frac{Precision.recall}{Precision + recall}$$

V. CONCLUSION

Cryptography plays an important role in the increasing growth of digital data storage and communication. It is used to achieve the main content of security objectives, such as confidentiality, integrity, Authentication, non-repudiation. It has been analyzed that in asymmetric cryptography a single is used both at the transmitter as well as at the receiver side. Whereas, in the symmetric key cryptography, two different keys are used at the sender and receiver end respectively. In this paper, different encryption algorithms used in the text data have been studied. It has been concluded that the speed of AES is more than other encryption techniques along with high security.

VI. REFERENCES

[1]. Dakhare, B., Shinde, N. N., Salvi, S. S., Kadam, A. H., Wagh, P. G., & Student, B. E. (2018). Performance Analysis of Data Encryption Algorithms using AES BLOWFISH and SNAP. *International Journal of Engineering Science*, *16466*.

[2]. Sivakumar, R., Balakumar, B., & Pandeeswaran, V. A. (2018). A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security.

[3]. Villanueva, E. B., Medina, R. P., & Gerardo, B. D. (2018, April). An enhanced RC5 (ERC5) algorithm based on simple random number key expansion technique. In *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. IEEE.

[4]. Dixit, P., Gupta, A. K., Trivedi, M. C., & Yadav, V. K. (2018). Traditional and Hybrid Encryption Techniques: A Survey. In *Networking Communication and Data Knowledge Engineering*(pp. 239-248). Springer, Singapore.

[5]. Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). An improved security schema for mobile cloud computing using hybrid cryptographic algorithms.

[6]. Kushwaha, A., Sharma, H. R., & Ambhaikar, A. (2018). Selective Encryption Algorithm Based on Natural Language Processing for Text Data in Mobile Ad hoc Network. In *Innovations in Electronics and Communication Engineering*(pp. 355-360). Springer, Singapore.

[7]. Das, R., & Dutta, S. (2018). A Private Key Encryption Scheme based on Amicable Number with User defined Cipher Block Sequencing Techniques.

[8]. Dixit, P., Gupta, A. K., Trivedi, M. C., & Yadav, V. K. (2018). Traditional and Hybrid Encryption Techniques: A Survey. In *Networking Communication and Data Knowledge Engineering*(pp. 239-248). Springer, Singapore.

[9]. Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption using advanced encryption standard. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *3*(3), 118-126.

[10]. Zhu, K., Lin, Z., & Ding, Y. (2018). A New RSA Image Encryption Algorithm Based on Singular Value Decomposition. *International Journal of Pattern Recognition and Artificial Intelligence*.

[11]. D. I. G. Amalarethinam and J. S. Geetha, "Image encryption and decryption in public key cryptography based on MR," *2015 International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, 2015, pp. 133-138.

[12]. M. Patil, V. Sahu and A. Jain, "SMS text Compression and Encryption on Android O.S," *2014 International Conference on Computer Communication and Informatics*, Coimbatore, 2014, pp. 1-6.

[3].Rajput, Yashpalsingh, Dnyaneshwar Naik, and Charudatt Mane.,"An Improved Cryptographic Technique to Encrypt Text using Double Encryption,"*International journal of Computer Applications* 86.6 (2014).

[13]. Verma, Vinay, and Rajesh Kumar.,"A Unique approach to multimedia based dynamic symmetric key cryptography,"*International Journal of Computer Scienceand Mobile Computing* 3.5 (2014): 1119-1128.

[14]. SHAKTI, SHIV, Dimple ,"ENCRYPTION USING DIFFERENT TECHNIQUES: A REVIEW," Vol. 2, No. 1, January-February-2013(ISSN 2278 – 5973) "

[15]. Goshwe, Nentawe Y,"Data encryption and decryption using RSA Algorithm in a Network Environment," *International Journal of Computer Science and Network Security (IJCSNS)* 13.7 (2013):

[16]. Rohan Rayarikar, "SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications (0975 – 8887), Vol. 50– No.19, pp 12-17, 2012.

[17]. Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," *Proceedings of 2011 6th International Forum on Strategic Technology*, Harbin, Heilongjiang, 2011, pp. 1118-1121.

[18]. W. X. Zhang, S. Y. Xiao and Y. Zhang, "Research on Image-Text Encryption Techniques in Mobile Communications," *2010 Second WRI Global Congress on Intelligent Systems*, Wuhan, 2010, pp. 115-118.

[19]. Govindan, V., and B. Shajee-Mohan, "An intelligent text data encryption and compression for high speed and secure data transmission over internet," *International Conference on Information Technology Coding and Compression, ITCC*. 2005.

[20]. Song, Dawn Xiaoding, David Wagner, and Adrian Perrig, "Practical techniques for searches on encrypted data," *Security and Privacy, S&P 2000, Proceedings. IEEE Symposium on*. IEEE, 2000.