IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

[1]Akash Salve, [2]Raul Dhruva, [3]Yogesh Sauw, [4]Yogita Ganage

[1]Student BE, [2]Student BE, [3]Student BE, [4]Professor
[1]Department of Information Technology,
[1]MCT's Rajiv Gandhi Institute of Technology, Mumbai, India

Abstract : Computer networks and internet applications are evolving rapidly, so data security is that the challenging issue of today that touches many areas. To cease unauthorized access to the user data or database, any transmission & storage process must be securely encrypted. The goals of this paper are: 1) To propose new hybrid cryptographic algorithm model employing a mix of two cryptographic algorithms AES and ElGamal; 2) Provide comparison between two symmetric, asymmetric algorithms and proposed hybrid model; 3) to suggest effectiveness and security of recent hybrid model which makes the algorithm strong against vulnerabilities. Currently, many encryption algorithms are available to securely encrypt the information but some algorithms exhaust many computing resources like memory and CPU time. This paper presents a comparative analysis of experimental results on these encryption algorithms supported various parameters affecting security and efficiency. The target of this research is to see the performance of AES, ElGamal cryptography algorithms and AES & ElGamal hybrid cryptography algorithm. The performance of the implemented encryption algorithms is evaluated by means of encryption and decryption time and memory usage. To create comparison experiments, for these algorithms special software was developed. The substitute language JavaScript is used for realizing the encryption algorithms in code. As a result, the paper shows that the new hybrid encryption model is safer and powerful compared to previous cryptography models and it's used for control systems security.

***IndexTerms* - cryptography, encryption, decryption, hybrid cryptosystem, public key cryptosystems.**

I. INTRODUCTION

Symmetric (secret key) cryptography systems use the identical cryptographic keys for both plaintext encryption and ciphertext decryption [1], [2]. Typically, with a symmetric key, you'll be able to exchange the key with another trusted participant. The entire security of this method stands on the secrecy of the key. During this way, the key must be kept secret to every participant.

Asymmetric (public key) cryptography is one in every of the important directions of secure data transferring. There are developed form of public-key encryption systems. Unfortunately, there's significantly fewer developments publicly key algorithms than in symmetric key algorithms [1], [2]. This can be also results of different key sharing technology. Asymmetric cryptography relies on digital signature functions. Is additionally employed in software tools, like browsers, which require to ascertain secure connection over an insecure network just like the internet or have to validate the digital signature. Digital signature is a mathematical technique providing validation of the authenticity and integrity of message, software or digital document.

In general, the strength of the cryptosystem can't be totally ensured. Of course, all cryptography algorithms are developed to supply the best security, but because of the very fact that technology is consistently being developed, security systems are getting less immune to every known or new attack.

II. STRENGTH AND WEAKNESS OF SYMMETRIC KEY AND ASYMMETRIC KEY CRYPTOGRAPHIC SYSTEM

One of the strong points of symmetric key cryptography is resistance of the key key against Brute Force Attack. the aptitude of a cryptographic system to shield data from attack is named its strength. Of course, the best thanks to attack encrypted messages is solely to try decryption the message with every possible key [3]. Strength depends on various factors, including: the secrecy of the key; the issue of guessing the key or trying out all possible keys (a key search); the issue of reversing the encryption algorithm without knowing the encryption key (breaking the encryption algorithm); lack of back doors, or other ways by which an encrypted file is decrypted more easily without knowing the key [1], [4].

The weak side of symmetric key systems is to settle on the correct key. Attacks against encrypted information represent three main categories. Those are: Key search (brute force) attacks; Cryptanalysis; Systems-based attacks [5] – [7].

Through increasing the length of the key, the number of possible permutations is additionally exponentially increased. Meaning following, brute force attack needs more technical resources to attack the system. This type of attack is additionally called key search attack. Key search attacks aren't very effective. If the chosen secret's long enough, a key search attack isn't even possible [8] – [10].

Asymmetric (public key) cryptographic system uses two keys: public keys which can be distributed widely, and personal keys which are known only to the owner [1]. During this encryption system, anyone can encrypt a message using the receiver's public key. The strength of a public key cryptography system relies on the computational effort (work consider cryptography) required to seek out the private key from its paired public key. The most weakness of this technique is number of public keys. Thanks to increasing number of users, quantity of shared keys is additionally proportionally increased [11]. So that, public key algorithms are easier to attack than symmetric key algorithms for the explanation that the attacker (probably) encompasses a copy of the general public key that was accustomed encrypt the message [4].

III. HYBRID CRYPTOSYSTEM

Hybrid encryption merges two or more encryption systems [12] – [14]. It's a mix of asymmetric and symmetric encryption to learn from the strengths of every variety of encryption. These strengths are respectively defined as speed and security [15], [16]. Hybrid encryption is taken into account a highly secure form of encryption as long because the public and personal keys are fully secure [17]. A hybrid system is introduced with the subsequent schema: Key encapsulation scheme, which may be a public-key cryptosystem; an information encapsulation scheme, which may be a symmetric-key cryptosystem [1].

Public key cryptosystems depend on hard mathematical functions. For instance, RSA relies on the sensible difficulty of product factorization by large prime numbers. In hybrid systems for encryption and decryption process is employed fast symmetric key systems. For key management is employed slower asymmetric algorithms, with strong mathematical functions within the background.

Both symmetric and asymmetric key algorithms have their advantages and drawbacks. Symmetric key algorithms are faster than asymmetric algorithms. The most requirement is that secret key must be shared during a secure way. Asymmetric systems provide secure transmission of keys, but this process needs far more time. To enhance this problem is to use the hybrid algorithm, which implies using differing kinds of cryptosystems together.

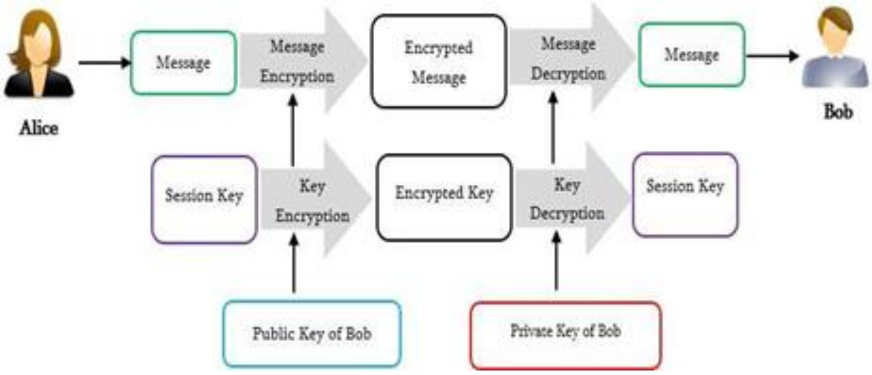


Fig. 1. The General idea of Hybrid cryptosystem

The main idea of a hybrid cryptographic system is the generation of random keys for symmetric systems. The next step is to encrypt the key for asymmetric systems. As a result we have secret key which can be used for encryption of plaintext. During the decryption process first, we use private key, and then we publish the key (Fig. 1). In Figure 1 Alice wants to send a message to Bob in a secure way, considering all aspects of security. For that, both sides use a hybrid cryptosystem.

IV. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) or the same Rijndael is the symmetric key encryption algorithm. For AES there are selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits [1], [2]. Algorithms can be judged on their ability to resist attack as compared to other submitted ciphers. Security is considered the most important factor in the competition. Algorithms can be evaluated also with suitability and overall, relative simplicity of implementation in hardware or software.

V. ELGAMAL CRYPTOGRAPHY

ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange and provides additional security layer by asymmetrically encrypting keys, previously used for symmetric message encryption. The security of this algorithm is based on Discrete Logarithm Problem. Generally, the ElGamal cryptosystem is used in a hybrid cryptosystem. The plaintext is encrypted with a symmetric cryptosystem and ElGamal is then used to encrypt the key. Asymmetric cryptosystems like ElGamal are usually slower than symmetric ones. It is faster to encrypt the key with ElGamal and the message (which can be randomly large) with a symmetric cipher [16].

ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

At first happens key generation process with following steps [16]:

- Alice generates random prime p;
- then is chosen g generator, with following criteria g < p;
- Alice randomly choses integer x with following criteria 1< x < p;
- Alice computes y = gx mod p ;
- Alice publishes y, g, p and sends them to Bob as an public keys. Alice retains x as her private key, which must be kept secret.

The second step of ElGamal algorithm is encryption of plaintext. After receiving public keys from Alice, Bob starts to encrypt plaintext using those keys. We have following steps [16]:

- at first we have plaintext M. Bob chooses random prime key k with following criteria 1< k < p – 1;
- than computes a and b numbers whereas, a = gk mod p, and b = yk M mod p;
- exactly those (a, b) is the encrypted plaintext.

The decryption algorithm works as follows: to decrypt a ciphertext (a, b) is decrypted with private key x. For this must calculate following M = b (ax) 1 mod p [16].

The security of the ElGamal scheme depends on different length of random k key. The negative side of this algorithm is doubled length of encrypted message. ElGamal algorithm security reasons is necessary to use different k key for each M and M' different plaintexts. Otherwise, if we use same k key we will have (a, b) and (a', b') cyphertexts, for them we have following equation b(b')1 = M(M')1. That means following, we can easily calculate M' if we know M.

VI. SOFTWARE IMPLEMENTATION AND EXPERIMENTS OF AES AND ELGAMAL CRYPTOSYSTEMS

Cryptosystems have different system requirements and time intervals. For calculation of those parameters during the encryption/decryption process, was done through experiment using software code on JavaScript, nodeJS IDE. Generally, the time required to encrypt data is termed as encryption time of the cryptographic system the other way around for the decryption process [16]. Encryption time depends on the structural characteristic of the algorithm. Table I shows the encryption time of the AES algorithm. Experiments on-time efficiency was done on the ElGamal cryptosystem. Was used different size plaintext. As a result, we've Table II.

Table I. EXPERIMENTAL RESULTS ON AES

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size (Kilobytes)
32	10885816	13183260	10438616	44
64	11619392	19435850	11616928	87
128	12595776	23731067	14259312	175
256	14941600	39475025	19446952	350
383	17911200	51462211	25536712	525
512	19578712	56630859	29827912	700
640	21102120	64556965	11701832	876
1024	23745952	72088845	30773720	1401
1664	23917200	67403987	32465440	2277
2048	27348528	135473361	46150064	2802
3328	39767696	250928350	70698544	4554
4096	47157952	227850681	97370664	5604
5120	45313504	283950147	75567816	7006
6144	95522296	308917134	68862920	8407
7168	106414488	354152143	80110040	9808

Table II. EXPERIMENTAL RESULTS ON ELGAMAL

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size(Kilobytes)
32	30563800	28566844	56142968	92
64	111413712	32170582	118217248	736
128	172191288	77038870	291667624	1103
256	275272096	113553330	332891746	1839
383	336428336	145442172	365965008	2942
512	361937784	172920490	271493032	5883
640	439920368	231472754	218697896	7721
1024	557353760	382681610	239611976	13603

VII. PROPOSED AES&ELGAMAL HYBRID CRYPTOSYSTEM FRAMEWORK

This paper proposes a replacement model of a hybrid cryptosystem with a mix of two AES (symmetric) and ElGamal (Asymmetric) algorithms. This model could be a combination of these two cryptosystems. The full process is split into two parts. The primary part is encryption of the encryption key. The second part is that the encryption of the plaintext (Message) with this key.

In the beginning, the sender provides the key, which is employed for the AES system. But initially, this key must be encrypted using the ElGamal algorithm. For encryption, the user must provide y, g, p public keys, and x private key. As a result, we are going to get encrypted key, which is really introduced with A and B encrypted ciphers. The second part, of this model, is that the encryption of the message itself. One amongst these keys (A or B, or A and B) or both are going to be used for encryption of plaintext. The decryption process is going to be drained reverse mode. Figure 2 shows the scheme of the provided hybrid cryptosystem.

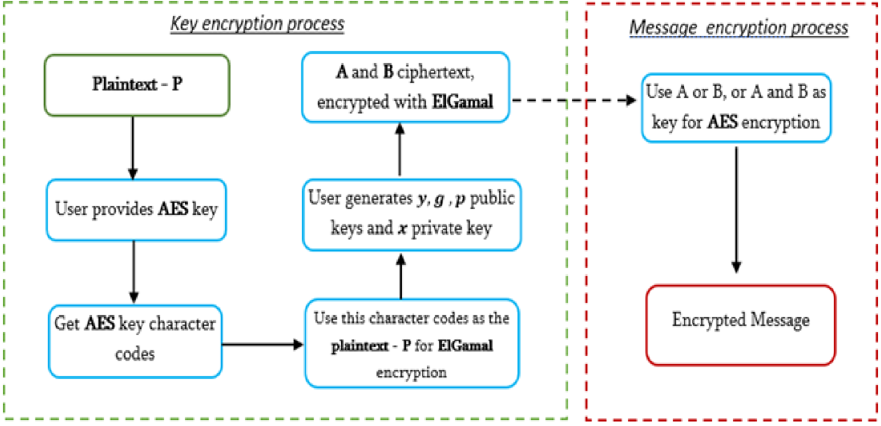

Key encryption process
Plaintext - P
User provides AES key
Get AES key character codes
Use this character codes as the plaintext - P for ElGamal encryption
User generates y, g , p public keys and x private key
A and B ciphertext, encrypted with ElGamal
Message encryption process
Use A or B, or A and B as key for AES encryption
Encrypted Message

Fig. 2. The general architecture of hybrid cryptosystem obtained by the combination of AES + ElGamal cryptosystems.

For provided hybrid algorithm have been implemented encryption and decryption processes of different size data using the software code realized in the nodeJS platform. Table III shows the provided hybrid system efficiency data.

After this experimental research, we can compare the described systems by its encryption time. Was done comparative research on AES, ElGamal and Hybrid AES & ElGamal, so it can be simply understood that the time required for encryption of Hybrid AES-ElGamal is less than time requirement of ElGamal. AES needs less encryption time than provided hybrid system (Figs 3, 4). The strength of this hybrid system could be considered one of the competition with others.

TABLE III. EXPERIMENTAL RESULTS ON AES & ELGAMAL HYBRID MODEL

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size (Kilobytes)
32	11422808	11475187	10554248	44
64	12139408	14042938	12480872	87
128	13122456	19254605	14083528	175
256	15349104	32248157	18823832	350
383	18497728	43386244	24424880	525
512	20011400	48810538	28279896	700
640	21598680	67133177	29075848	876
1024	21195488	81189868	29961968	1401
1664	21283344	96277607	31385096	2277
2048	23800368	115473678	35746432	2802
3328	39792256	175045003	60485784	4554
4096	47208608	200580406	89747792	5604
5120	45346272	255886133	86760704	7006
6144	95557608	301044625	103606520	8407
7168	106426216	332311451	104075496	9808

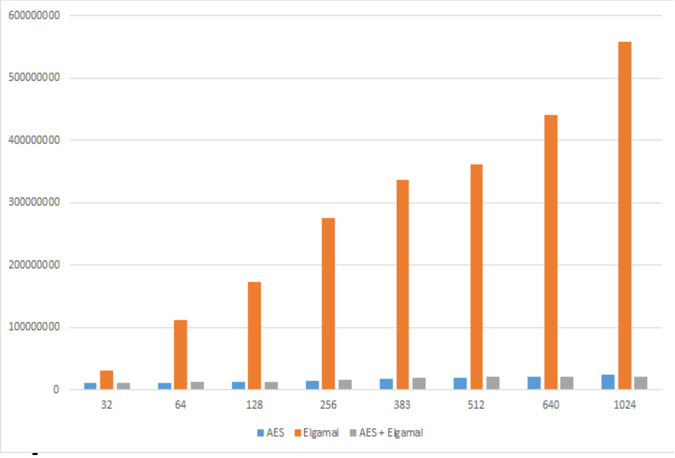


Fig. 3. Encryption time (Nanoseconds) for AES, ElGamal and AES+ElGamal algorithms.

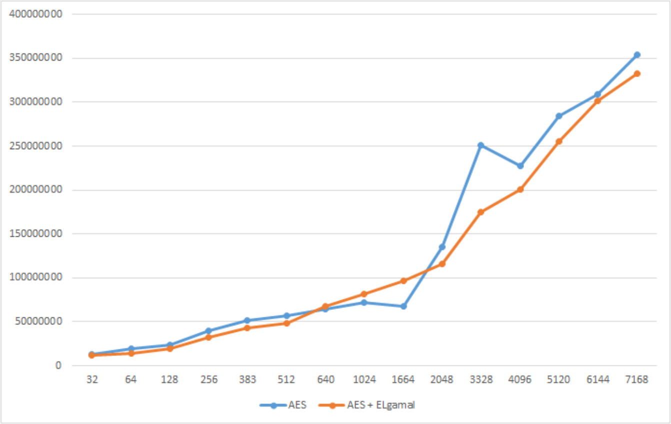


Fig. 4. Decryption time (Nanoseconds) for AES and AES+ElGamal algorithms.

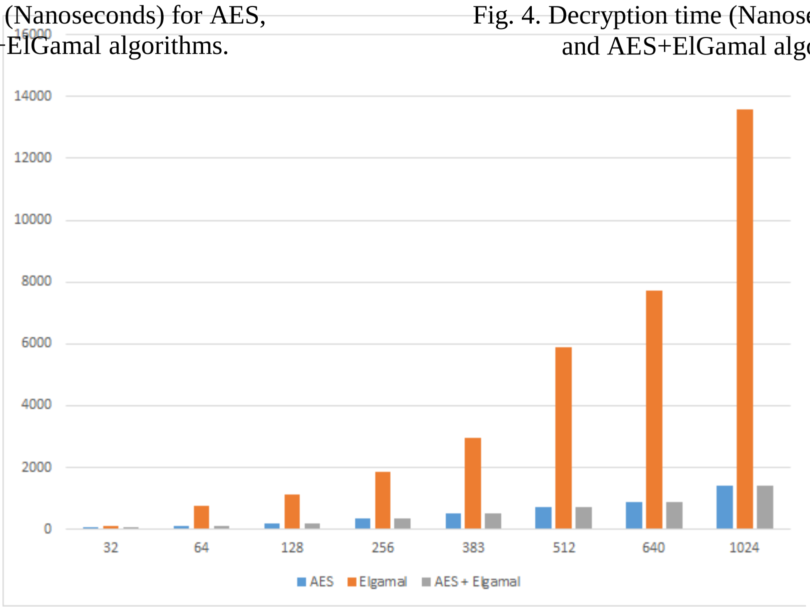
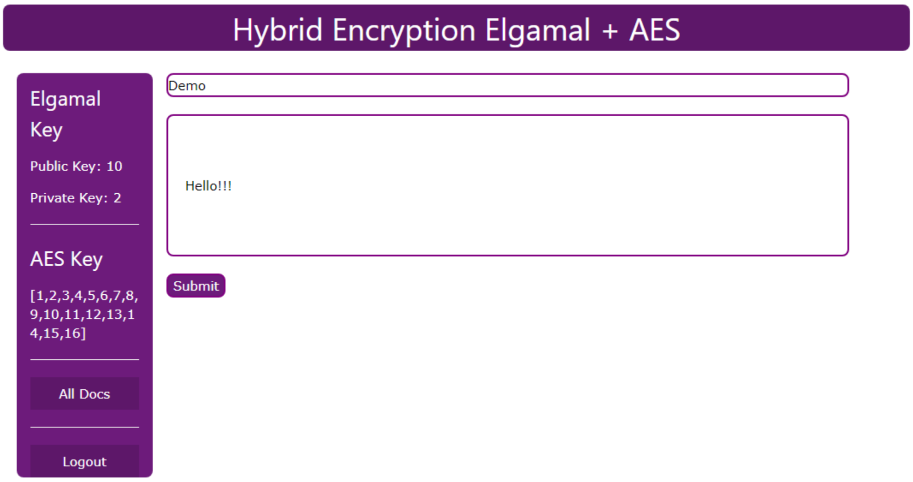


Fig 5. Encrypted file size comparison with plaintext size (Kilobytes) for AES, ElGamal and AES&ElGamal algorithms.



Hybrid Encryption Elgamal + AES

Elgamal Key

Public Key: 10

Private Key: 2

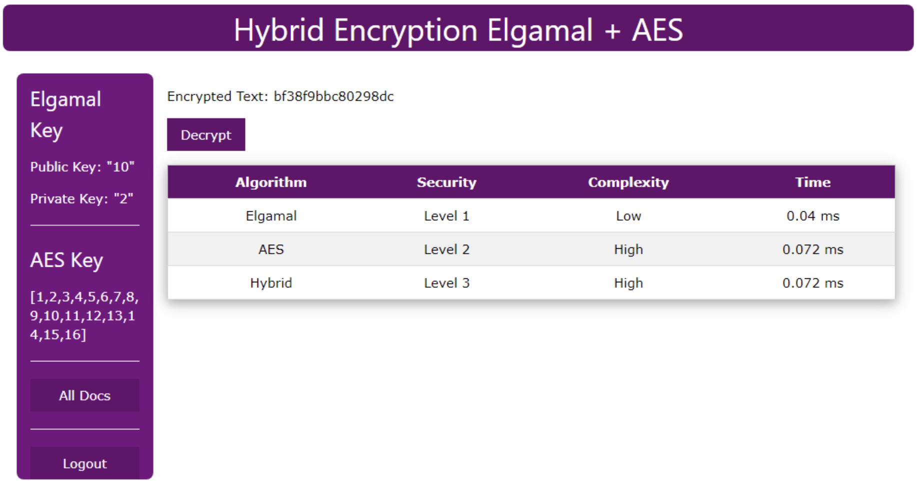
AES Key

[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16]

Demo

Hello!!!

Fig 6. User interface for proposed system



Hybrid Encryption Elgamal + AES

Elgamal Key

Public Key: "10"

Private Key: "2"

AES Key

[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16]

Encrypted Text: bf38f9bbc80298dc

Algorithm	Security	Complexity	Time
Elgamal	Level 1	Low	0.04 ms
AES	Level 2	High	0.072 ms
Hybrid	Level 3	High	0.072 ms

Fig 7. User interface for encryption and decryption in proposed system

During experiments on the proposed hybrid algorithm was done comparison of plaintext size and encrypted file size (Kilobytes). Results show that during an encryption process with AES algorithm encrypted file size becomes averagely ~1.37 times bigger than plaintext file size. If we are using ElGamal algorithm encrypted file size becomes averagely ~9.34 times bigger than plaintext file size. Figure 5 shows encrypted file size comparison chart results on proposed algorithms. According to results new hybrid model has better results compared with the ElGamal algorithm.

VIII. CONCLUSION

This paper explained and analyzed two varieties of systems: Symmetric and Asymmetric cryptosystems. The paper provides a replacement model of hybrid algorithm using AES and ElGamal cryptosystems. A special software tool was created and implemented for the proposed system.

Compared with encryption and decryption speed experimental research shows, that symmetric algorithm AES is quicker, but asymmetric algorithm ElGamal is healthier to produce security. The symmetric algorithm AES requires very low computational power. AES is one amongst the most effective algorithms of symmetric encryption cryptography. ElGamal algorithm gives high throughput as compared to AES and other algorithms. The hybrid of AES and ElGamal algorithm has characteristics of both the algorithms. This makes the algorithm strong against vulnerabilities. This hybrid structure of AES and ElGamal provides more security by increasing the complexity. Because the result shows, the proposed AES & ElGamal hybrid algorithm model is relatively better than ElGamal in terms of encryption/decryption time and better than AES in terms of its security. The complexity of the system is provided by a mixture of two algorithms. Given results are often implemented in aviation for control systems yet as other critical aviation information systems security ensuring.

For future work are often described as an improved version of this hybrid model, can also be tired combination with other cryptography algorithms to produce faster encryption and decryption processes, lower power and memory consumption.

REFERENCES

[1] Atul Kahate. May 2019. Cryptography and Network Security, Tata Mc Graw Hill, 4th Edition.

[2] William Stallings. March 2013. Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education.

[3] Ilya Kizhvatov. 2009. Physical Security of Cryptographic Algorithm Implementations, L'UNIVERSITÉ DU LUXEMBOURG.

[4] Simson Garfinkel, Alan Schwartz, and Gene Spafford. Practical UNIX and Internet Security, 3rd Edition Securing Solaris, Mac OS X, Linux & Free BSD.

[5] The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.

[6] S Baldeep Singh, Maninder Kaur, Navpreet Kaur. 2017 (Fall). Comparative Study of Different Cryptographic Algorithms, 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA).

[7] Lalit Singh, Dr. R.K. Bharti. November 2017. Comparative Performance Analysis of Cryptographic Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11.

[8] B. Mao, Modern Cryptography: Theory and Pactice. Moscow, Wilyams, 2005.

[9] Diao Zhe, Wang Qinghong, Su Naizheng, Zhang Yuhan. 2017. Study on Data Security Policy Based On Cloud Storage, IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids).

[10] Phillip Rogaway and Mihir Bellare, Introduction to Modern Cryptography, 2005

[11] Pradeep Semwal, Mahesh Kumar Sharma. 2017 (Fall). Comparative study of different cryptographic algorithms for data security in cloud computing, 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA).

[12] "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security. 2011.

[13] Adleman, Leonard M., Rothemund, Paul W.K., Roweis, Sam, and Winfree Erik, (June 10–12, 1996). "On Applying Molecular Computation to the Data Encryption Standard," Proceedings of the Second Annual Meeting on DNA Based Computers. Princeton University.

[14] Ronald Cramer, Victor Shoup,. "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack", 2004.

[15] Dennis Hofheinz and Eike Kiltz, "Secure Hybrid Encryption from Weakened Key Encapsulation," 2007.

[16] Taher ElGamal (1985). "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"

[17] https://www.techopedia.com/definition/1779/hybrid-encryption