I.J. Mathematical Sciences and Computing, **2017, 3, 1-11**
Published Online July 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2017.03.01

Available online at **http://www.mecs-press.net/ijmsc**

Cryptographic Security using Various Encryption and Decryption Method

Ritu Goyal [a], Mehak Khurana [b]

[a] *Research Scholar,Northcap University,Gurugram and 122001, India*
[b] Assistant Professor, *Northcap University,Gurugram and 122001, India*

Abstract

Fast development in universal computing and the growth in radio/wireless and mobile strategies have led to the extended use of application space for Radio Frequency (RFID), wireless sensors, Internet of things (IoT). There are numerous applications that are safe and privacy sensitive. The increase of the new equipments has permitted intellectual methods of linking physical strategies and the computing worlds through numerous network interfaces. Consequently, it is compulsory to take note of the essential risks subsequent from these communications. In Wireless systems, RFID and sensor linkages are extremely organized in soldierly, profitable and locomotive submissions. With the extensive use of the wireless and mobile devices, safety has therefore become a major concern. As a consequence, need for extremely protected encryption and decryption primitives in such devices is very important than before.

Index Terms: Cryptography, AES-128, Tiny encryption, SHA algorithm, Elgamal Encryption, RSA algorithm.

1. Introduction

Cryptography plays a significant role for protected and secure communication through an unsecured channel and making the protected environment for sender and receiver. There are numerous procedures used for this purpose. Generally, these processes are of two types: symmetric key and asymmetric key encoding and decoding processes. This paper deals with the reviews of Data Encryption and decryption standard algorithm, which is one of the symmetric key cryptography procedures. The m file DES.m is produced & the two purposes encrypt () and decrypt () are named into this file. This m file DES.m offers the time complexity for encryption and decryption in instants for the arrived text. The fast progressing of mobile communication, individual communication schemes, provided new problems from the safety point of view by the novel communication technologies. Other procedure is Asymmetric key cryptography which is also called Public-key cryptography.

* Corresponding author. Tel.: +919971677227
E-mail address: ritugoyal1104@gmail.com

Public-key cryptography tools can deal with numerous security problems in communication scheme. The RSA procedure is the best general public-key cryptosystem.

2. Review on Different Methods with Their Authentication Technique

This section includes the details of various techniques

2.1 AES with SHA-1

The Advanced Encryption Standard algorithm is most important and is considered as a standard and trusted through the U.S. Management and frequent organizations [13]. Though it is mainly effectual in 128-bit form, this method also uses keys of 192 and 256 bits for heavy/dense duty encryption with 12 and 14 rounds respectively. AES is mostly measured resistant to all occurrences, with the exclusion of brute force, which efforts to decode communications using all possible combinations of 2^{128}, 2^{192}, or 2^{256}-bit cipher for 3 versions of AES-128, AES-192, AES-256 respectively. Static, safety specialists consider that AES will ultimately be addressed the de facto ordinary for encoding data in the isolated segment. The given procedure contains the 10 sequences/cycle/rounds for data encryption in AES-128; it is shown in Fig. 1. In initial stage key for 128-bit is prolonged into 11 times it is called cycle/cycle/round keys, all of 128-bits must be in accurate or in size too. All cycle/rounds comprise an alteration by the consistent secret message (cipher) key to confirm the security of encryption.

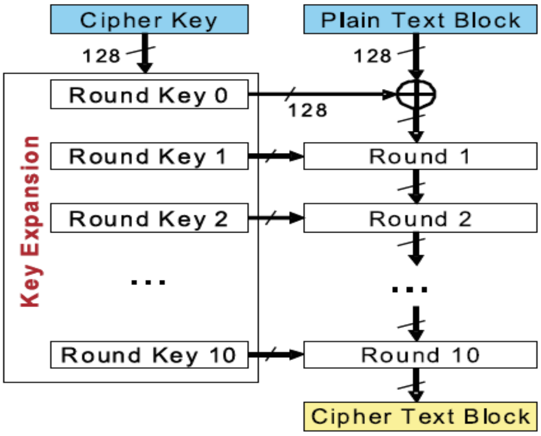

Fig.1. Configuration of AES Process

Afterward a primary cycle/round, throughout that the 1st cycle/round key is XORed to the pure/plain script (Add cycle/round key process), followed by nine similarly organized cycle/rounds. Every cycle/round contains the subsequent processes:

- Substitute bytes
- Shift rows
- Mix columns
- Add round key

Now 10th cycle/round is same as the nine rounds but mix columns stage is not a computed in 10th round. Secure Hash Algorithm-1 (SHA-1) helps to construct a secure text/message verification cipher by presenting a classified 512-bit key *K* by the undisclosed preface technique Secure Hash Algorithm -1(K||x). During this interconnection, SHA-1 calculates a transitional hash rate of K in the 1st repetition that would be pre-computed. Later, calculation of a MAC needs d length (x)/512e. Though, the top-secret preface technique is measured unconfident uniform still SHA-1 comprises the text measurement of hash & tiny. section discloses one partial for the hash consequence [21]. It is the reason behind HMAC that will properly be labeled as:

$$\text{HMACk}(x) = \text{SHA-1}((k \oplus \text{opad}) \,||\, \text{SHA-1}((k \oplus \text{ipad})||x))$$

Generally, 160-bit fundamental/key K is improved by 0's subsequent in K. When relations can be precompiled k ⊕ opad and k ⊕ ipad as of the 512-bit records opad & ipad k. During the interconnection ((k ⊕ ipad)|| x) intermediate cost of hash (k ⊕ ipad) and (k ⊕ opad) that precompiled as fine. Later, MAC calculation needs d-length (x)/512e + 1 processes of secure hash algorithm-1. Acronym of Advanced Encryption Standard helps in CBC-MAC method (Mention in Fig.2) in the direction to calculate and verify ciphers. The approach for comparable to the Block-Code connecting mode that outcome from the previous XORed as encrypt as with subsequent plaintext block and encoded over. The intermediate secret message scripts which will not be used in *cbc-mac* for secure extent text manner. Now the calculation of a media access control necessitates dlength (x)/128e processes. For the line with respect to safety of advanced encryption standard way is a cycle/round 2^{64} not 2128 as unique strength suppose, reason behind to the initial violence/attack.

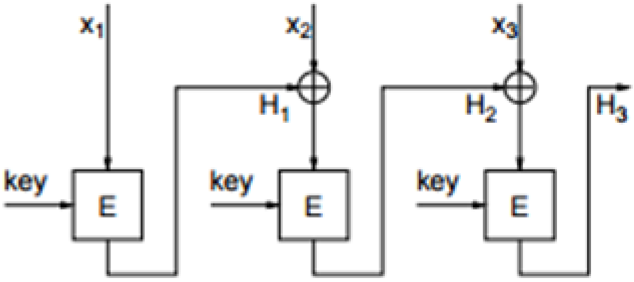

Fig.2. Cbc-mac – Creating a hash with a block Cipher

2.1.1. Limitation of AES with SHA

A block code functions on agreed -sized blocks (128-bit formation for AES), together for outcome using input and output process. A hash function generates output of small fixed length while takes a variable length input. So, ciphers and hash are truly dissimilar in nature and making comparison in both in useless. rather we must see what is common between two. Coders who can design a block cipher can also design hash functions, as the analysis tools are almost same (there is a lot of linear algebra and Boolean functions). Both block ciphers and hash functions is a different concept; and designing a hash function from AES is a big question mark. It's quite difficult, and the limited AES block size is the major issue.

2.2 Hybrid of aes, rsa and md5 to Increase the Safety

A new data security procedure by using the hybrid method of RSA, AES and MD5 has been deliberated in this portion. This hybrid method will deliver the explanations to the numerous data safety attacks and susceptibilities in the cloud environment. This system holds a grouping of RSA Partial homomorphic and MD5 hashing system. In this resolution file is encoded by RSA partially before uploading it on cloud server. Afterward uploading its hash is computed by MD5 hashing system. All these methods perform subsequent stages of Encryption/Decryption, Data uploading on a cloud, Hashing and Corroboration [15].

2.2.1. Execution steps of Hybrid Method

User will input the data that has to be directed to the Cloud Source.

- The RSA procedure will be achieved at the user side which will encode the data prior to transferring it on gateway.
- This encoded data is then moved to the gateway.
- Entrance will accept the data and will achieve the MD5 hashing procedure and will then apply AES (Advanced Encryption Standard) algorithm.
- Then the user details will be stored by the gateway and upload file in the user identity table.
- Later Gateway will send the encoded file to the cloud service provider for loading.
- Cloud supplier will save the data been given by the gateway and take a backup inside backup server.
- The cloud supplier will save the data and will achieve the MD5 hashing procedure on it to produce the hash value. These hash values are saved at the gateway.

2.2.2. Limitation

In RSA encoding and decoding procedure, the foremost difficulty is its encryption rate or speed. It consumes lot of time to encode data. Essentially this is drawback due to the use of asymmetric keys This procedure (Biham et al., 1992) accomplishes whole dispersion (wherever a unique bit modification in the plain script should have derivation virtually 32 bit alterations in the cryptograph/cipher text). When the key process is diffident; the 128-bit key K is separated into four 32-bit blocks K = (K [0], K [1], K [2], K [3]) [17]. It achieves sufficient security but its speed is very low while encrypting input data. Also during decryption, the false keys can be inserted which can hamper the security.

2.3 XTEA (Extended Tiny Encryption Algorithm) Based Hash Function for Verification

A hash function takes a variable length input and converts it to the fixed-length output known as message digest. The message digest is exclusive for every communication and therefore these digests are used for verification of the message. If the digest at sender and receiver side matches then there is no loss of message integrity and it is thereby authenticated. Hash is a one-way determination, that the message cannot be reconstructed by inspecting the digest. The two maximums usually used Hash functions are MD5 and SHA-1. But they are computationally multifaceted and have established to be practically protected, while in 2005 safety errors for both procedures have been stated.

2.3.1. Limitation of TINY Encryption

The major drawback with XTEA [17] is that the bits in keys will continuously make an impact on the similar bits in every cycle/round. This hasn't been demoralized however, but that doesn't mean that it can't be. This first application is a 64-bit block code, that geographies 128 arranged keys. The sources keys are programmed energetically at runtime, and necessitate no recollection. The decided keys are resultant from accomplishment plaintext-dependant repeated bit revolutions on the explanations. Suppose each five bits' needed in rotation have a likelihood of 1/2 and every key to a cipher or code has likelihood of 1/4, all programmed key will have probability of 1/128.

2.4 ECC with Signature Generator for Authentication

At starting stage, server chooses domain values and clients calculate the public [and private keys. Server's file comprises of user information like identity and PIN/password [16]. Clients communicate their Identity and PIN/password to receiver intended for verification. Server must have to check user id and password to authenticate user after that server receive the user requirement. Domain values for ECC over Fp are p, a, b, Gm and n. p is the main quantity is well defined for determinate area of Fp. Now a and b (0, p- 1) are the important factors for curve $y^2 = x^3 + ax+b$ mod p. Here, Gm is the inventor point (xG, yG), a view on the ECC that designated for processes. Also 'n' signifies command for the ECC. The standards for Effective Cryptology (SEC), carries defined in advance principles to parameters {112,128,160,192,224,256,384,521 bits} that has an average curve. In this method, 128-bit prime field is taken after that values for p, a, b, n, G are chosen from standards Effective Cryptology(SEC). Afterward attendant/server chooses the domain values that are directed to entire authentic user. Then user calculates private and public keys with assistance of domain values. Clients chooses an arbitrary quantity:
'x' $\mathcal{E}$[1, p-1] Wherever x is a reserved key and computes public key by,

$$y=x.G \{ G + G + \ldots \ldots + \text{ xtimes} \} \tag{1}$$

The Public key for each authentic user is directed to receiver. In case any user wants additional customer's, public keys and application must be directed to receiver in instruction to acquire it. For every od message among users, receiver produces a couple of private and public key for safety.

2.4.1. Signature Generation

Throughout signature group stage, if source needs to mark a communication and directed towards receiver, that time 1st origin has chosen an arbitrary no. K$\mathcal{E}$(1, p-1) Then translate the communication in form in M to ASCII. The transmitter calculates r and s through:

$$r = M + (kG)\, x \text{ modn} \tag{2}$$

$$s\{k\{Hash(r) \text{ xprivate key of sender}\}\} \text{ modn} \tag{3}$$

To calculate the values of r, k, random numbers are measured with G base values. It contributes (kG) x where only x values are taken into consideration for calculations. Then assume another random k if r=0 in Eq. (2). Use SHA-256 procedure to r value to generate the hash values. The inputs to knapsack algorithm are r and s along with series. In 1970, Merkle and Hellman reversed the knapsack procedure which is a public key cryptology process. It encrypts and decrypts the specified text. The sequence help in knapsack procedure would be super growing order. A super collective classification is unique that subsequent period of the classification is better than the quantity of all previous relationships. It is informal to explain a super collective knapsack by seeing the entire mass of the knapsack and associating it with the leading mass in the classification. If the entire mass is a smaller amount than the principal load, formerly it is not in the knapsack. If the entire mass is superior to the major bulk, then it is in the knapsack. Detract the no. from the total, and associate with the subsequent uppermost number. This organization is constant till the whole influences zero. If the whole doesn't influence zero, then there is no explanation. In 1858, Stern well-defined the demanding order as surveys:

$$Stern\ (1) = 1 \tag{4}$$

Stern (n) t = Stern (n/2) – if n is even. (5)

Stern (n) = Stern (n - 1) + Stern (n + ½) – if n is odd (6)

In Severe sequence, every row is generated through introducing the quantity of couple of successive fundamentals obsessed through the preceding row. Stern presented the ***gcd{s(n),s(n + 1)} = 1*** then each couple of comparatively main +ve numbers (a, b) there occurs an exclusive n>=1 through s(n)=a & s(n+1)=b. After this (a, b) = (0,1), is easy to see where every row made two group recurrences like 1st half of the subsequent row downcast. The series of Stern is improved permitting to the great growing classification constriction.

2.4.2. Limitation of ECC with Signature Generator

The control of ECC is that it upsurges the size of encoded text and second drawback is that ECC performs very composite calculations which makes the encryption algorithm very complex.

2.5 ELGAMEL with Symmetric Message Digest Key

Projected system of ElGamal modified system is variety to it changed from innovative system through key group encoding & decoding procedure [14]. This method uses two different files, one is encrypted file and second for signing the digest of the message. Symmetric key cryptography is used in enhancing ElGamal cryptography. For signing of digest, RSA algorithm is most efficient. Numerous stages in this method are given below:

2.5.1 Key Generation

- Sender and receiver both decide on two prime quantities g and p.
- Source select its own underground number a and calculate A= (g^a) mod p
- Communicate A to receiver.
- Receiver selects its own secret no. b and calculate B= (g^b) mod p
- Communicate B to sender.
- Sender calculate k1= (b^a) mod p
- Receiver calculate k2= (A^b) mod p Here it is strong that k1=k2 resources common secret key is recognized among sender and receiver.
- Select original finite field Fa and primitive root element fit in to this field.

A. Encryption phase

- Select alternative big prime q1 in such a way that 1<k1.

B. Decryption Phase

- Divide otki= (a^-k2) mod p
- Message text =(c*otki) mod p.

Firstly, Signature generation will generate digest or hashing of the message using SHA-512. In this method, the produced digest is of size 512 bits. Then this 512-bit message digest is employed by using improved RSA procedure. Here we usage dissimilar process for encryption and validation procedure to offer more safety associated to current scheme.

2.5.2 Key Signing

Message digest=SHA_512 (message size in numerous of 1024 bits, initial 512-bit message digest)

- Select two big prime statistics n1, n2, and n3.
- n←n1*n2*n3.
- $\emptyset\ (n)$ ← (n1-1)*(n2-1)*(n3-1).

We should select e such that 1<e $\emptyset(n)$ and e is co-prime to $\emptyset(n)$

- Public key ← (n, e).
- Private Key ←d
- Sign s= (Message_digest^d) mod n

2.5.3 Verification

- Message _Digest=(s^e) mod n
- Generate message digest from established message and associate it with step 1. If both are equivalent, then communication is valid.

2.5.4 Limitation of Tiny with Symmetric Message Digest Key

The only one foremost limitation originate is that a known-plain text occurrence is conceivable in ElGamal if the same **r** is used twice through encryption.

A problem of the ElGamal encryption is that there is a message development by a feature of two. That is, the cipher text is twice as long as the dependable plaintext. The unique public key scheme projected through Diffie and Hellman necessitates communication of together revels to compute a mutual isolated key. These situations difficulties of the cryptography must useful to message schemes when mutually events will never capable to cooperate in sensible period in obligations to intermissions in broadcast or inaccessibility for acceptance event. Therefore, ElGamal simple the Diffie-Hellman key exchange algorithm by giving a random follower k. This exponent is an unused for the private booster of the getting thing. Outstanding to this explanation the process can be used to encode in one way, without the requirement of the subsequent event to proceeds dynamically slice.

3. Review of Literature

Generally, encryption and decryption are the two main processes of Cryptography. Data Encryption is the procedure of changing the information in a for that can be only understood by the authorized person. This alteration of plaintext is known as cipher text. Also, the process of changing cipher text to plain text is called decryption. Basically, cryptography deals with four basic things- authentication, privacy/confidentiality, integrity and non-repudiation [12]. There is also a term called cryptanalysis. It is the process of deciphering encrypted communication without the knowledge of the key.

[4] examined a construction and strategy of Rijndael code (novel advance encryption standard), mentioning the leading benefits and limits and also the situation correspondences & variations through DES & T-DES.

Lastly, a presentation evaluation between novel techniques for dissimilar microprocessor have recognized viewing which different AES must be processor rate equivalent command than the unique T-DES.

[5] presented specific encoding and decoding systems which has possessions that makes it appropriate to use controlled surroundings as portable applications, where calculating properties or command obtainability will be incomplete classification of commands performed by this procedure, and protest that a modest workstation is appropriate. Similarly, a group of community key, symmetric key and hash processes appropriate for those settings and deliberately associated for assignment features. As well as defines the commands desirable through dissimilar algos Diffie Hellman key conversation, AES and Hash.

[6] offered, presentation of four secret key procedures (DES, 3DES, AES, Blowfish) were compared on different hardware platform. The input file of various size is encrypted and checked for their performance. The implementation of algorithms is done in a uniform language, using standard specifications, It allowed uniform comparison of execution speeds. The results are summarized based on the performance level and showed the trade-off between performance and security and a conclusion has been presented. The dimension of performance was implemented in JAVA that showed Blowfish as the best procedure between DES, 3-DES, AES and Implementation outcomes are accessible in ECB type (on behalf of slab codes) & CFB (for stream codes) and decided on the behalf of more difficult cycle/rounds and a greater no. of cycle/rounds is usually measured safer. So, decided Blowfish as the wildest/fastest scheme among all schemes presented up till.

[7] examined numerous encoding and decoding systems appropriate for help in WSN that developing MICA z-type particles & tiny operating system is considered. Resource utilization in terms of memory, time and power for every cryptographic algorithm shown experimentally.MD5 and RC4 performed best in aspect of power dissipation and processing time. ATMEL AT mega 128L microchip is boarding in MICA z-based particles. 128KB automatic performance showy retention use for accumulation producible package code, 4KB SRAM use for short-term storing.

In [8] decided to do the terms for Safety field that as new, fast affecting occupation. An attention on safety steadies sequence measurable, decreases concern around apprentice hacking and benefits to deliver scholars the services required to developed safety forecasters. Which also describes a traditional of knowledge compulsory through Network Safety forecasters as network Safety services highlight corporate observes permissible basics, attack acknowledgment, net optimization and defines dynamic knowledge movements that help the scholars in knowledge these significant skills. This essentially pr écised all the assistances connecting to network safety, and deliberated active knowledge exercises that contribution apprentices in knowledge these significant services. Foremost attention was on safety info services that will help in obtaining the system.

In [9] deliberated the safety and outbreak phases of encoding and decoding methods and similarly deliberated the leading issues of safety and numerous attacks. Lastly, worktable manifests particular recognized current encoding and decoding procedures in exploration for the finest collaboration in safety. The author presented a CrypTool was helped in simulator to mien investigates and grow the consequence. Individual alphanumeric and unusual typescripts are castoff for investigation of encoding and decoding methods. In this condition are designated in selection set menu of the CrypTool and graphic consequences are usual in opening selection of CrypTool. Several no. of the encoding and decoding procedures are applied in C, their output is occupied like code script and derivative in certain script folder and that script folder is cast-off for the investigation by CrypTool.

In [10] obtainable the important arithmetic behindhand schedule the AES procedure beside the momentary explanation of certain encoding and decoding primitives are usually help in the area of message safety meanwhile AES delivers improved safety and has a smaller amount of operation difficulty and has developed as one of the solidest and maximum effective procedures in being currently. It similarly contains numerous computational problems, optimization of secret message similarly the investigation of AES safety features beside altered types of attacks counting the security events alongside these occurrences and too emphasized specific of the significant safety problems of AES procedure.

4. Challenges of Cryptography

We live in an era of inconceivably quickly progressing, remarkable machineries that allow rapid flow of information – anytime, anywhere. The merging of computers and networks has been the key force last in developing new technologies. Collective use of schemes constructed using this Information Technologies (IT) is having a deep effect on our usual lives. These approaches are attractive in all dominant and worldwide.

- The encoding and decoding key controlling problems that arise behind dispersed countryside of IT properties and then circulated in environment of their controller, the last divided between numerous cloud performers. Moreover, the design of delivery differs through the kind of provision contribution - Organization as a Service (IaaS), Stage as a Service (PaaS) and Software as a Service (SaaS).
- The distinct experiments complex in organizing encoding and decoding key organization purposes it can happen the safety necessities of the cloud Consumers, dependent upon the nature of the facility and the type of data produced/managed/stored through the service types.

5. Importance of the Cryptography

Cryptology is receiving progressively significant response in information field; it is likewise becoe less and less visible. Cryptography combined into smart cards for commercial contacts, web browsers, working schemes, mobile phones and electric character cards. This achievement clarified through numerous issues: 1st, nearby it strong requirement for encoding and decoding clarifications, 2nd acceptable procedures and procedures has industrialized and 3rd the declining cost of calculation makes it inefficient for cryptography.

- **Low cost and/or low power:** It can be attained via openhanded active high performance or high safety; this method is important to permit implementation of cryptography in very small and tiny devices (e.g., ambient intellect). Project aims application of a stream cipher code that provides immense safety level (say 80 bits) with use of less than 1000 gates.
- **High performance:** This is compulsory for extremely effectual applications such as bus encryption, hard disk encryption, and encryption in Terabit networks.
- **High safety:** particular areas needs encoding and decoding procedures and develop self-assurance and assertion equal to their ability.

6. Discussion

After doing numerous works in literature survey accessible by numerous Authors, we examine about various or many present research idea in terms of cryptography, DES, AES, Blowfish, Tiny, RSA, diffle-Hellman which are given us to developing technique about network safety system on the base of encryption and decryption safety theme that deliver reliable communiqué and conscious from the hacker. We also discussed above about cryptography challenges and its importance.

7. Conclusion

The overall concluding part says that TINY offers immense security than other algorithms such as: Blowfish, RSA, DES, and AES based on foundation of key length and safety. The purpose of TINY procedure gives a great level of safety to encode the 16-bit plain script. Similarly, the TINY procedure runs quicker than further prevalent symmetric key encryption procedures: RSA, Blowfish, Two fish and AES. It is decided that TINY offers better performance then RSA, Blowfish, Two fish and AES in context of encryption and decryption time. Blowfish provides least security when compared with other mentioned processes.

Acknowledgement

We are thankful to the Department of Computer Science and Engineering of Northcap university, Gurugram, India for giving us the platform for planning and developing this work in the departmental laboratories.

References

[1] JaydebBhaumi. N.D. 2012. A Modified XTEA. International Journal of Soft Computing and Engineering. vol. 2. (2). 461-464.

[2] Agrawal Modesnika, Mishra Pradeep. A Comparative Survey on Symmetric Key Encryption Technique, International Journal on Computer Science and Engineering (IJCSE). Vol. 4 No. 05 May 2012, pp. 877-882.

[3] Alam Md Imran, Khan Modeshammad Rafeek. Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.

[4] Sanchez-Avila, C. Sanchez-Reillol, R, The Rijndael block cipher (AES proposal). A comparison with DES‖, 35th International Conference on Safety Technology 2001, IEEE.

[5] Murat Fiskiran, Ruby B. Lee, Workload Characterization of Elliptic Curve Cryptography and other Network Safety Algorithms for Constrained Environments‖, 2002. WWC-5. 2002.

[6] Aameer Nadeem, Dr. M.Younus Javed, A performance comparison of data Encryption Algorithm‖, Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.

[7] Elkamchouchi, H.M; Emarah, A.-A.M; Hagras, E.A.A, A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes‖, the 23rd National Radio Science Conference (NRSC 2006).

[8] Like Zhang, Gregory B. White, Anomaly Detection for Application Level Network Attacks Using Payload Keywords‖, **(**CISDA 2007).

[9] Suhaila Orner Sharif, S.P. Mansoor, Performance analysis of Stream and Block cipher algorithms‖, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[10] Punita Mellu & Sitender Mali, AES: Asymmetric key coding and decoding System‖, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.

[11] YudhvirSingh, YogeshChaba, Information Theory test based Performance Evaluation of Coding and decoding Techniques‖ , International Journal of Information Technology and Knowledge Management, Vol 1,No.2,2008 , pp. 475-483.

[12] YanWang, Ming Hu, Timing Evaluation of known coding and decoding Algorithm‖, International Conference on Computational Intelligence and safety, 2009.

[13] Jens-Peter Kaps and Berk Sunar "Energy Comparison of AES and SHA-1 for Ubiquitous Computing Department of Electrical & Computer Engineering Worcester Polytechnic Institute 100 Institute Road, Worcester, MA 01609, U.S.A.

[14] Yashpal Jitarwal, Pawan Kumar Mangal, Sunil Kumar Suman" Enhancement of ElGamal Digital Signature Based on RSA & Symmetric Key" Computer Science & Engineering.

[15] Pankaj Kamboj "A Review Paper on 3 Step Mechanism Using RSA, AES and MD5 to Improve the Safety in Cloud Environment" Er. Lovnish Bansal, Amer R. Zerek, Mohamed A. Abuinjam "*ElGamal public-key encryption*" International Conference on Control, Engineering & Information Technology (CEIT'14) Proceedings - Copyright IPCO-2014 ISSN 2356-5608.

[16] Latha Parthiban and Nivetha Shree "Using modified stern series for digital signature authentication in elliptic curve cryptography" Department of Computer Science and Engineering, SSN College of Engineering, Tamil Nadu, India.

[17] J.Balakrishna, Philemon Daniel, Rajeevan Chandel "Design & Implementation of VLSI Architecture for XTEA" International Conference on Advanced Computing, Communication and Networks'11.

[18] Mehak Khurana, Meena Kumari, "**Security Primitives: Block and Stream Ciphers",** International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Vol. 4, March 2015.

[19] Mehak Khurana, Meena Kumari, "**Variants of Differential and Linear Cryptanalysis"**, International Journal of Computer Applications (0975 – 8887) Volume 131 – No.18, PP 20-28, December 2015.

Authors' Profiles

Ritu Goyal, B.Tech in IT from BSA College of Engineering & Technology. (UPTU), Uttar Pradesh, India. Worked as assistant lecturer in SGI group in CSE & IT and has around 3 years of experience. Currently pursuing M.Tech in CSE from NorthCap University, Haryana and doing her research work. Her current research interests include: cryptography, information sharing, Cyber Security.

Mehak Khurana is currently working as assistant professor in The NorthCap University in CSE & IT and has around 6 years of experience. She completed her M.Tech from USIT, GGSIPU in 2011 and B.Tech from GTBIT, GGSIPU in 2009. Her key areas of interest are Cryptography, Information Security and Cyber Security. She is lifetime member of Cryptology Research Society of India (CRSI).

How to cite this paper: Ritu Goyal, Mehak Khurana,"Cryptographic Security using Various Encryption and Decryption Method", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.3, No.3, pp. 1-11, 2017.DOI: 10.5815/ijmsc.2017.03.01