SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms

Muhammad Aamir Panhwar[1], Sijjad Ali khuhro[2], Ghazala Panhwar[3], Kamran Ali memon[1]**

[1]School of Electronics Engineering, Beijing University of Posts and Telecommunications, China
[2**]School of Computer Science and technology, University of Science and technology of china, China
[3]Institute of Science, Technology and Development Jamshoro, Mehran University of Engineering &Technology, Pakistan

Abstract
The security plays very important role in any mechanism (algorithm).In network broad system and technology domain security comes as a challenging part. It becomes a preliminary need now days. The data sent on internet becomes more secure after encapsulating. For this purposes cryptography is most popular and basic need for data security. The cryptography uses different method by encrypting data at sender side and decrypted at receiver side .For securing the data there are two main types of cryptography algorithm, one is called symmetric and other is called asymmetric algorithms. In this paper various symmetric and asymmetric algorithms like AES DES, and triple DES, are discussed for their properties and use in mobile computing based worked solution.

Key words:
Encryption, Decryption, Cryptography, Symmetric, Asymmetric

1. Introduction

Encryption and decryption mechanism are used for security purposes in network. Security of data over network is completed due to these two mechanisms. The cryptography is used for writing such a code which is understandable only for those, for these codes are written. There are different types of data that are sent using encryption process. These data including Audio, Video, image and text. These data are meaningless, unreadable during transmission [7].the basic purposes of cryptography is to avoid data from attackers during transmission, so that data receive successfully at receiver side, after receiving data by receiver, the data is restore by using decryption mechanism. The encryption has following basic steps [1].if sender/dealer he wants to send a "SECRET" message to the receiver. The unique information, also called plain-text, is transformed to a Random bit called a cipher text by using a key and an Algorithm. The algorithm used could be generating different outputs on a per-use basis which based on the key values. The cipher text is communicated over the broadcast channel. At the receiving end point, the cipher text could be transformed back to the unique text by using the similar algorithm and key would be used to encrypt the message. There are two terms used in encryption. Plain-text and second is called Cipher-text. The Cipher text is also called random bits. By using key and algorithm original message changes into cipher text, depending upon key each time the output of algorithm is different, and that output transmitted over the medium. At receiver side same key used to convert that message back into original shape using same algorithm.

Our construction of paper follows as: second part of paper we discuss about literature review of previous work, third part: belongs to basic background of cryptography fourth part: study about symmetric algorithms fifth part: asymmetric study back ground. Sixth part: results and discussions.

2. Literature Review

In [2], Aleve, Drpalanisamy and k.kanagaram proposed a paper on cryptography. In this paper they gives encryption parameter and classified the types of encryption techniques. The parameter of encryption included key length, encryption ratio and speed are discussed with the help of algorithm and also placed security issue. In [3], Ranjeetmasram, vierkshahare, jibiabraham, rajnimoona proposed a paper. In this paper they discussed different file features e.g. data type, data size and key size. For these features they analyzed different symmetric key algorithm .They also discussed different algorithms like AES, DES, Triple DES, RCZ, and these algorithm behave different at encryption time.

In [7], in this papers different types of algorithm based on cryptography is discussed. This algorithm provides security information and all are different types. In [9], this paper a survey has done. This survey is about existing work.in this survey work on different techniques of encryption has discuses. Each technique has its own advantages and disadvantages. Each technique is useful for different application .Basically all the techniques discussed in that survey is useful for real time encryption. The AES

Manuscript received January 5, 2019
Manuscript revised January 20, 2019

technique is most popular in term of throughput, speed and time.

While in [14], a study is done in which both symmetric and asymmetric are briefly described, and also a comparison between these two algorithms is done in this study. After comparison it is clear that symmetric algorithm is better in term of rapidity as well as power although asymmetric is improved in term of tenability. $Ee = s$ Algorithm in key symmetric encryption is originated improved in term of rate, safety and implementation while RSA algorithm is better in asymmetric key encryption in term of speed and security.

3. Cryptography

Cryptography is a technique and science for securing the confidential data against the adversary to use the encryption and decryption techniques according to proper rules and methods. Generally speaking, cryptography targets to protect data from the unauthorized person. Data could be hacked in different forms, such as, content of information, text data, images, audios and videos so on which are co-relate data to combine during the communication process or storage, these techniques called an encryption process. The reverse process of these techniques we able to called a decryption.

There are two main types of cryptography first: Secret Key Cryptography this is also called as Symmetric Key Cryptography. Second: Public Key Cryptography this is also called as Asymmetric Key Cryptography. Follow figure no.1.

The main purpose of cryptography it to give a lot of solution for security goals and achievements. In the sense of security improvement it's useful now days in a communications networks. Some of multiple goals we discussed under bellow.

Data confidentiality: when we are talking about confidentiality of information, in other words we can say protecting the data from disclosure to adversaries. Data is most important in the recent days in several governments sectors, such as, banks, military, secret trade's etc. each and everyone wants to keep information as a secret purpose. For hiding such kind of information is important part of information security.

Authentication Process: this process acknowledge us the receiving information by the system and after able to check ID of sender whether the data is received from the authorized party or unauthorized party or the identity of person is wrong.

Integrity: The integrity of the data refers to the defense information from the existence changed by the illegal party. If the information is correct or real data, it may be valuable. Disturbance of the information will prove to be expensive. Let's give an example if we send an online remittance of 100 of dollars, but the information is tampered with in a way that you actually send $1000, which will prove to be very expensive for you. Like data privacy, cryptography plays a very important role in safeguarding data honesty. Methods that are typically used to maintain the integrity of statistical information include hashing the information you obtain and comparing it to the hash of the original message. However, this means that you must be provided with a hash of the original data in a secure manner. A more convenient approach could be to digitally sign the data using the current structure, such as GPG.

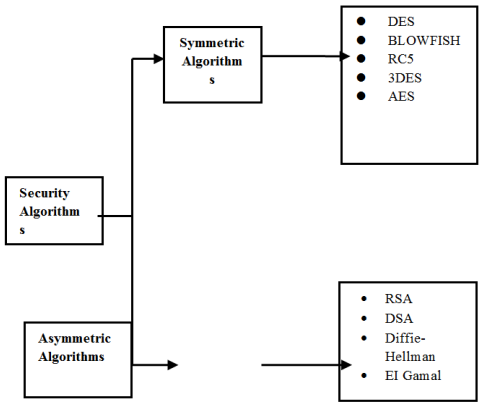


Fig. 1 Types of Algorithms

4. Overview of Symmetric Algorithm

In the regard of symmetric key encryption, we always use same key among the encryption as well decryption techniques. The main benefit of this algorithm is low computing power and its works very fast during the encryption process. This algorithm divides in two modes such as blocks ciphers and stream cipher. In the regard of block cipher all data would be dividing in the form of chunks or blocks. Data based in size of block and key would be provided for the encrypting the data. Stream cipher, data divide in the bit such as 0101010101 and randomized after the encryption rule will be applied. Symmetric is faster than the asymmetric algorithm. Figure no.1. Clarify the symmetric and asymmetric algorithms.

Mathematical Explanation: for example Bob and Alice, they want to ex-change the secret key k. They able to encrypt and decrypt the secret messages, they both have a symmetric key. They uses a symmetric key k which choose from a set. Conceivable keys k to use for encrypt a plaintext s which could be choosing from conceivable

messages S, the result will be for encryption process is Cipher text t, which concerned to direct for conceivable cipher text T. The encryption process would be follows as,

$$e: K*S \to T$$

The domain among $K*S$ is set of pairs (k,s) containing a key k and plain text s and this range is specified to cipher text T. Alternatively for decryption process follows as,

$$d: K*T \to S$$

Generally speaking, we can get the decryption process to revert the results for the encryption techniques. This can be expressed as mathematically following,

$$d(k,e(k,s)) = s \text{ For each } k \in K \text{ and } s \in S.$$

This is sometimes suitable to explain the dependency on k. After all for every key k, we able to achieve the pair of functions.

$$e_k : S \to T \text{ As well } d_k : T \to S$$

Filling the decryption property follows as,

$$d_k(e_k(s)) = s \text{ For every } s \in S$$

In other condition, all key k, function would be d_k would be the inverse function of e_k. Specially, it prove that e_k should be one to one, subsequently if, $e_k(s) = e_k(s')$ so it would be follows as,

$$s = d_k(e_k(s)) = d_k(e_k(s')) = s'$$

This is very safest for Alice and bob to be assume that adversary identifies the encryption techniques that have been applied. In mathematically wording, its shows he meaning that adversary could know the functions e and d. Adversary what he don't know, specific key k even Alice and bob still they both are using. Take an example, if Alice and bob will use a simple cipher, they could be undertake that adversary surely knows this fact. This kind of condition in modern cryptography simply we called as "Kirchhoff principle". This basic principle says" security of cryptosystem could be depending on secrecy of the different keys and it's not depending on the secrecy of encryption techniques ".

If (K,S,T,e,d) these factors could be successfully cipher text. They contain the following conditions;

1. For each key $k \in K$ and plain text $s \in S$. These conditions could be easily to compute $e_k(s)$.
2. For each key $k \in K$ and plain text $t \in T$. These must conditions could be easily to Compute $d_k(t)$.
3. By providing some more cipher text $t_1, t_2, t_3 ... t_n$ by using encrypted key $k \in K$. This could be very difficult to calculate any of consistent plaintext $d_k(t_1), ... d_k(t_n)$ deprived of k.

The following property is too much beneficial, but it's difficult to compute.

4. Provided one or more than one pairs of plaintext and there's alternative cipher text $(s_1,t_1),(s_2,t_2),(s_n,t_n)$ .this could be very difficult to decrypt any of cipher text t.

4.1 AES

This standard was published first time in NIST (national institute of standard technology) and developed by two belgin cryptographer Daemon & Trijiman. AES algorithm is type of symmetric key Cipher which has been used to encrypt and decrypt a block of 128 bits. The key size depends upon the number of round. Many key sizes are available which can be 128, 192,or 256 bits and the round it uses may be 10,12,or 14.9 processing will be done on that basis.11 processing is done when key size is 128 if block and key length is 192 bits. Each processing has 4 steps.

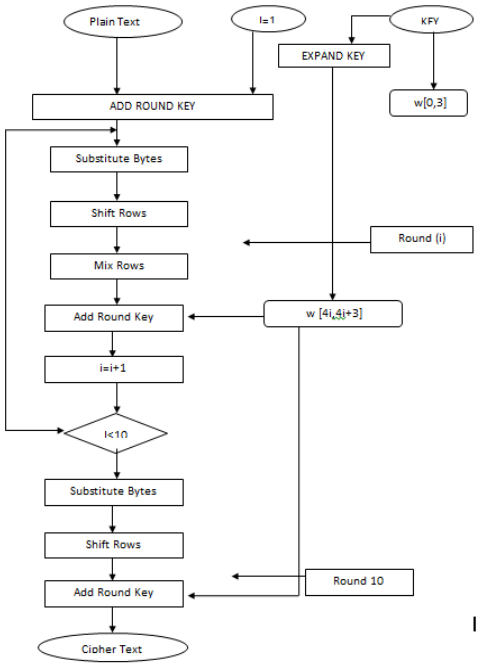


Fig. 2 Four steps of AES algorithm

1...Substitute Bytes:
S block is used by this phase to perform a byte by byte sub situations.
2...Shift Row:
This phase is simple permutation.
3...Mix Columns:
This is basically sub situation method where algorithm is multiplied by data in each column from shift row.
4...Add Row Key:
The key for the processing round in XOR with data.

The first three function of algorithm are made especially to prevent cryptanalysis, viva method of confusion and diffusion. the fourth function is re used to encrypt the data. AES plaintext contains 16 bytes block and each block treats as 4*4 state arrays. The information about row and columns maintained by array, especially mix columns () and shift row ().timing analysis attack can be apply on AES. It can be happen when malice innings the deputize byte technique on dissimilar information and observed execution time.

4.2 DES

DES is basically the main encryption standard used now a days.it can encrypt data of 64 bits at a time because it is64 bit cipher block.in this initially from 64 bits 56 bits are selected for key and remaining bits are used for priority checked or discard. Two halves of 28 and 287 bits are made by dividing the 56 bits by treating each one separately. 48 bits 24 from left half and
Remaining from right are selected randomly in every round. Encryption key schedule is same for DES [4].
When des is adopted in 1977, it has been discussed that some kind of backdoor was designed into the cryptic s boxes, allowing that "in" the "know" to effectively cracks des.
At last in 1988 a des cracker was developed for fewer than $250000 that could be decode DES message in less than a week. This was developed by EFF.

4.3 Triple DES

In this algorithm, on each data three time data encryption standard cipher is applied. Three keys are used essentially in standard way.one key is used for data encryption, the second key is used for data decryption and the third key is used for finally encrypted .For overall total key length of 192 bits, it takes three 64 bits keys. When that algorithm was developed than key size was 56 bits sufficient, but due to computational power brute force attack was feasible to protect from such attack triple DES provides better way to increase key size. Triple DES algorithm is three time slower than DES but provides high security using similar encryption process but in opposite order. Working of algorithm is given below in the figure 3.

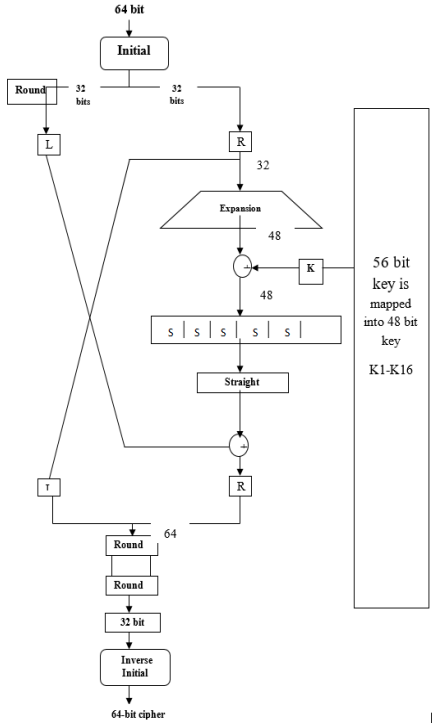


Fig. 3 Triple DES process.

5. Overview of Asymmetric Algorithms

In the regard of symmetric key encryption, we always use same key among the encryption as well decryption techniques. The main benefit of this algorithm is low computing power and its works very fast during the encryption process. This algorithm divides in two modes such as blocks ciphers and stream cipher. In the regard of block cipher all data would be dividing in the form of chunks or blocks. Data based in size of block and key would be provided for the encrypting the data. Stream cipher, data divide in the bit such as 0101010101 and randomized after the encryption rule will be applied. Symmetric is faster than the asymmetric algorithm. Figure no.1. Clarify the symmetric and asymmetric algorithms.

Asymmetric key encryption is a technique, by this method different keys could be used for the encryption techniques and as well as decryption process. Here First key set is public. Second we kept as a private. These both keys are similarly we able to call "public key encryption". Let's take an example:

If we want to publish first key as an encryption then the system communication as a private from the public in regard of unlocking user's keys. Second condition, if we going to publish one unlock key decryption, after this our system would be perform as id based verification for the purpose of documents lock by the dealer of that private key. This kind of public keys techniques very important because they can be used for over shifting encrypted keys or could be data secure, when both of users they don't have such opportunity for the purpose of agreement secret key in the regard of private key.

Mathematically explanation: as usual, there is some space of keys K , and plaintexts S , Cipher text T . Nevertheless, a part

Of k for the space key is actually a pair of keys,

$$k = (k_{pr}, k_{pb})$$

Called as private & public key, correspondingly, encryption function would be,

$$e_{k_{pb}} : S \to T$$

For every private key k_{pr} there is an alternative decryption process is following,

$$d_{k_{pr}} : T \to S$$

They both have the property if they contain the pairs (k_{pr}, k_{pb}) is the key space K , then this condition will be happened,

$$d_{k_{pr}}(e_{k_{pr}}(s)) = s \text{ For each } s \in S .$$

In condition, if asymmetric cipher will be secured, then this must be difficult for the adversary to resolve the decryption algorithm $d_{k_{pr}}(t)$, although she knows the public key k_{pb} . Its noticeable due to this assumption, bob could send the back the cipher text $e_{k_{pb}}(s)$ without any worry that eve will decrypt the information s . It's easily to decrypt, and it's very necessary to get the secret key k_{pr} , however, Alice only a person with this kind of message. Sometimes private key called to be Alice trapdoor information. Because its provide the short cut for resolve the inverse function $e_{k_{pb}}$. In fact decryption and encryption keys k_{pb} and k_{pr} unlikely to make the asymmetric cipher.

5.1 RSA

This algorithm is used in the recent systems for the encryption and decryption to exchange messages. This algorithm belongs to the asymmetric algorithm. Asymmetric means two different keys which are used in this algorithm. In simply we called this is public key cryptography, because one the key could be given by anyone. Other key should be in private mood. This algorithm used for the finding large number of factors.

BOB	Alice
Key Generation	
Choose two large secret prime number p and q. Apply encryption processe. In regard of $\gcd(e,(p-1)) = 1$ Can be created $N = Pq$ and e.	
Encryption Process	
	This step we can choose plain-text t. This step bob can use the public key (N, e). For calculate $c = t^2 (mod\ N)$. Send cipher-text c to Bob.
Decryption Process	
Calculate For satisfy d $ed = 1(mod(p-1)(q-1))$. Calculate $t = c^d (mod\ N)$. After this t equal to the plain-text t.	

Fig 4 Exchange messages between Alice and Bob.

Bob and Alice they have the common issues to exchanging very sensitive data over a protected communication channel. This algorithm security depends on the following steps.

1. **Setup:** take two large p and q, we can write as $N = pq$, here e and t would be integers.
2. **Problem:** by resolve the congruence $x^e = t(\text{mod } N)$ in the variable x.
3. **Easy:** Bob, who already known the values of p and q, and this can be easily solve for x value.
4. **Hard:** adversary, he do not know the value of p and q. He could not find easily x.
5. **Dichotomy:** by resolving $x^e \equiv t(\text{mod } N)$ it could be an easy for a person which holds convinced additional secret information.

5.2 Diffie-Hellam

Diffie-Hellman they want to exchange information by the some standard methods. Let's suppose, if Alice and Bob they willing to share a secret key by using the symmetric cipher, but the condition is communication is insecure. All information the interchange which is observed by the hacker. How it could be possible that Alice and Bob to distribute a key deprived of making it available to adversary? At the first moment it acknowledges that Alice and Bob could face an impossible task.

The initial step for Alice and Bob to be agree to generate very large two prime numbers p and q as well as nonzero number g over modulo p. These two large primes' numbers are publicly generated for acknowledgment. They could may generated on their social sites, in this case adversary well known about it.

The next condition, Alice wants to choose a secret value x, after this she could not expose to anyone. At the same moment Bob can choose a value y he can keep it secret. After this Alice and Bob they both use secret integers to compute the information.

$$A \equiv g^x (\text{mod } p) \text{ And } B \equiv g^y (\text{mod } p)$$

Again they want to compute for next exchange, Alice want to send x value to the Bob and Bob want to send y value to the Alice. Make sure them sending value over a secure communication channel. Which is follows as;

$$A' \equiv B^X (\text{mod } p) \text{ And } B' \equiv A^Y (\text{mod } p)$$

They could compute the value, A' as well as B' correspondingly follows as;

$$A' \equiv B^X \equiv (g^y)^x \equiv g^{xy} \equiv (g^x)^y \equiv A^y \equiv B' (\text{mod } p)$$

6. Discussions and Performance Analysis

Here in this section we compare the different parameters. The encryption relationship defined in terms of smallest, reasonable and extreme. The speed has been defined by the resulting term suppose as fast, slow as well as moderate. We stipulate tenability in the term of yes or no. The values of key are dignified in regard of bit value used. Throughput is dignified as high and less. power depletion (used memory) is clear as high and less. The experimental results are shown in TABLE 1.

Table 1: Comparison study between Symmetric and Asymmetric algorithms

Parameter	Symmetric Encryption				Asymmetric Encryption	
	DES	**3DES**	**AES**	**Blowfish**	**RSA**	**Diffie-Hellman**
Key Used	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Different key used for encryption and decryption	Key Exchange
Throughput	Lower than AES	Lower than AES	Lower than Blowfish	Very High	Low	Lower than RSA
Encryption Ratio	High	Moderate	High	High	High	High
Tunability	No	No	No	Yes	Yes	Yes
Power Consumption	Higher than AES	Higher than AES	Higher than Blowfish	Very Low	High	Lower than RSA
Key Length	56 Bits	112 to 168 Bits	128, 192 or 256 Bits	32 Bit to 448 Bit	>1024 Bit	Key Exchange Management
Speed	Fast	Fast	Fast	Fast	Fast	Slow
Security Against Attack	Brute Force Attack	Brute Force Chosen-Plaintext, Known Plaintext	Chosen- Plain, Known Plaintext	Dictionary Attack	Timings Attacks	Eavesdropping

7. Conclusion

In this paper, the idea of cryptography is described. Cryptographic area essentially has Two types of parts: symmetrical and asymmetric. The symmetric algorithm uses the same key for encryption and decryption, while the asymmetric algorithm uses a different key for encryption and decryption. It can be determined that AES is greater to other algorithms DES and Triple DES for numerous parameters such as validity, speed, encryption time, decryption time, memory usage and so on. In terms of security and speed, AES is better than DES and Triple DES. Future work may include different parameters to increase the encryption ratio.

Acknowledgments

This research work has been carried out in the State Key Laboratory Intelligent Communication, Navigation and Micro-Nano System, Beijing University of Posts and Communications. The research reported in this paper has been financially supported by the National High Technology 863 Program of China (No.2015AA124103) And by the National Key R&D Program no 2016YFB05502001.The authors are thankful to the financial support and guidance and assistance provided by the State Key Laboratory Intelligent Communication, Navigation and Micro- Nano System, BUPT.

References

[1] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[2] AL.Jeeva,Dr.V.Palanisamy,K.Kanagaram,"COMPARATIV E ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622,Vol. 2, Issue 3, May-Jun 2012.

[3] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona, "ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014.

[4] E. Surya C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", E Surya et al, International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477.

[5] Gurpreet Kaur, Manish Mahajan, "Evaluation and Comparison of Symmetric key algorithms", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, Issue 10, October 2013.

[6] Gurvinder Singh Sandhu, Vinay Verma, "Comparing Popular Symmetric Key Algorithms Using VariousPerformance Metrics" , International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013.

[7] Disha Shah, "Digital Security Using Cryptographic Message Digest algorithm", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 10, October 2015.

[8] Himani Agrawal and Monisha Sharma, "Implementation and analysis of various symmetric cryptosystems", Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846.

[9] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[10] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617.

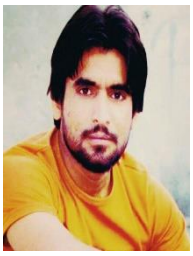
[11] Pratap Chandra Mandal , "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish ", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.

[12] Narender Tyagi Anita Ganpati, "Comparative Analysis of Symmetric Key Encryption Algorithms ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014 ISSN: 2277 128X.

[13] Nivedita Bisht, Sapna Singh," A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March 2015.

[14] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh, "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS", Singh et al., International Journal of Advanced Engineering Technology E-ISSN 0976-3945.

Muhammad Aamir Panhwar received his B.E in Biomedical Engineering degree and M.E in Telemedicine & e-health system in 2006 and 2014 respectively from Mehran University of Engineering & Technology (MUET), Jamshoro, Pakistan. He has been working as a lecturer in the department of Biomedical Engineering at MUET for eight years. He has some International and National papers on his credit. He is Member of IACSIT, member of Pakistan Engineering Council and IEEE.



Sijjad Ali Khuhro was born in 1991 Islamic Republic of Pakistan. He received his MSc degree in Information Technology from Quaid-i-Azam University (QAU) Islamabad and currently MS degree Scholar in Information Security from University of science and technology of china. Currently he has published several international Research Articles and conference papers, and other articles are under review. His research interests includes wireless sensor network, Ad-hoc network, Security of Wireless and Ad-hoc Networks, Cryptography and Network Security.

Ghazala Panhwar received his B.E in Electronics Engineering degree and M.E in Computer System Networks in 2007 and 2009 respectively from Mehran University of Engineering & Technology (MUET), Jamshoro, Pakistan. She has been working as a Teaching Assistant in the Institute of Science, Technology and Development Jamshoro, MUET for Two years. Currently she is pursing M.Phil. in the Management of Engineering from MUET, Jamshoro.

Kamran Ali received his Bachelor in Electronics degree (2009) from Mehran University of Engineering Technology, Jamshoro Pakistan, and Masters in Communication (2015) from Quaid-e-Awam UEST Nawab shah Pakistan. He is working toward his Ph.D. at State Key Laboratory of Information Photonics and Optical Communications (IPOC), Beijing University of Posts and Telecommunications, China. His research interests include optical and Wireless communications, PONs, Radio over fiber and WSNs.