ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

COMPARATIVE STUDY OF DIFFERENT AUTHENTICATION AND IDENTIFICATION ALGORITHMS IN SECURED CRYPTOGRAPHY

Nitin Gupta*, Dr. Manoj Kumar
*Research Scholar, Mewar University,Chhittorghara, India
Dept. of Mathematics,R.K. (P.G.) College Shamli,U.P.,India

ABSTRACT

The paper presents comparative study of different authentication and identification algorithms used in secured cryptography. The network security is also a great issue, when the data transfer is taken place over the internet. There are different algorithms available to provide network security like AES, DES, Triple DES, Triple AES, Kasumi, Blowfish, RSA, RC4, XMODES and TACIT. The research can be focused on the integration of network security, authentication, and multiplexing and data communication for a particular network. The wireless communications & technologies coming to homes and offices, demanding to have secure data transmission is of utmost importance. It is very much important that information is sent confidentially, over the network without the fear of hackers or unauthorized access to it. This makes security implementation in networks a crucial demand. Symmetric Encryption Cores provide data protection via the use of secret key only known to the encryption and decryption ends of the communication path. In the paper, study is carried out on the different security algorithms.

KEYWORDS: AES Encryption, DES Encryption, Blowfish, TACIT Network Security.

INTRODUCTION

With the development of technology, the information is shared either through wired or wireless networks. This information needs to be protected [1, 2] for communication over these channels as the risk of losing this information remains to be high. The main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency. Depending upon the needs, this sensitive information should be defended and protected. Cryptography [3] is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data [4, 9], cryptanalysis is the science of analyzing and breaking secure communication.

In the context on network security, the fundamental building block is user authentication. User accountability and access control are dependent on user authentication. Authentication process requires two steps: identification step and verification step. In identification steps, identifiers are assigned carefully for security services, such as access control services. A verification step [5] generates authentication information to bind identifier and entity. For the network based user authentication scheme, cryptographic keys methods are involved and something that individual can know, as a password. There are four general means of authentications, which can be used in combination also or alone.

Something the individual knows: The examples of something the individual knows are Personal Identification Number (PIN), password or answers to a prearranged set of questions.

Something the individual possesses: The examples relating to something the individual processes are dependent on cryptographic keys, smart cards, physical keys or electronics keycards. The type of authenticator is also called a token.

Something the individual is: The examples relates to static biometrics such as recognition of face, retina and finger print.

Something the individual does: The examples relates to dynamic biometrics such as recognition of handwriting characters, typing rhythm and voice pattern etc.

Cryptography is needed, when the user want to communicate over an untrusted medium such as wireless, internet services. A key management approach is applicable for both encryption and decryption algorithms. The encryption and decryption algorithms are very much helpful for cryptography that offer different key length and block size for higher security.

In Cryptography encryption the original message or data is called plain text which is encoded with key, called cipher text and transmitted over a channel. Description is the reverse process, in which the plain text is decoded from the cipher text. With the help of secret key and cipher text it produces the original plain text. Cryptography involves encryption and decryption with the sharing of same key at both end or the different key on both ends. There are mainly two types of encryption algorithms called symmetric and asymmetric algorithm. Symmetric key algorithm is also called a private key algorithm and symmetric key algorithm is called public key algorithm. In private key algorithm, there exist only one key for both encryption and decryption algorithm. The complexity of private key algorithm is less and easier to implement for higher speed applications and can be implemented with hardware. In asymmetric cryptography approach, both encryption and decryption process use different key and difficult to implement having complex structure. The model of cryptography is shown fig.1 in which plaintext *(T)* is encrypted with key value (*Key*) and transmitted cipher text is *B* = *E [key, T]*, the same text is extracted with decryption algorithm *T* = *D [Key, B]*, and same key (*Key*). The example of symmetric cryptography and asymmetric cryptography is shown in fig. 2 and fig. 3. In fig. 3, users tend to use two keys: public key, which is known to the public and private key which is known only to the user.

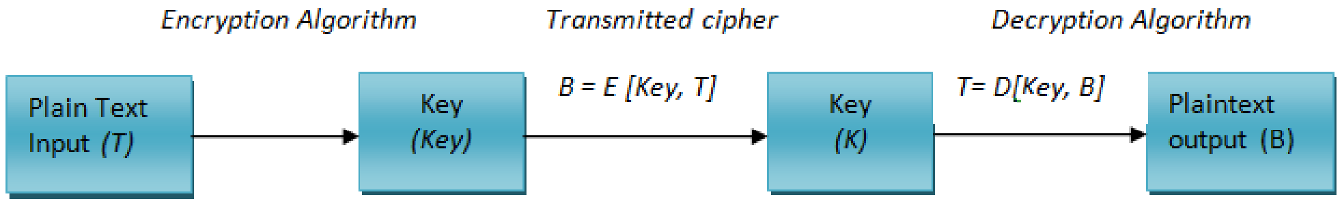

Fig. 1 Encryption and decryption [9]

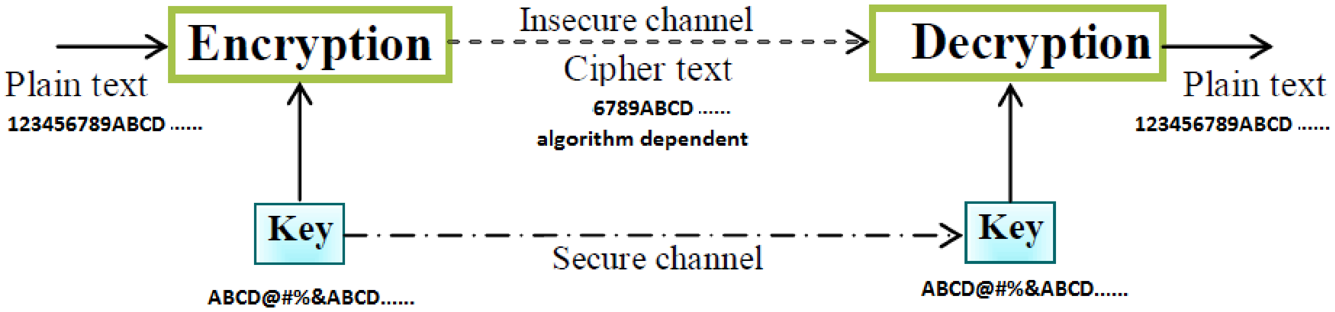

Fig. 2 Symmetric key encryption and decryption [7]

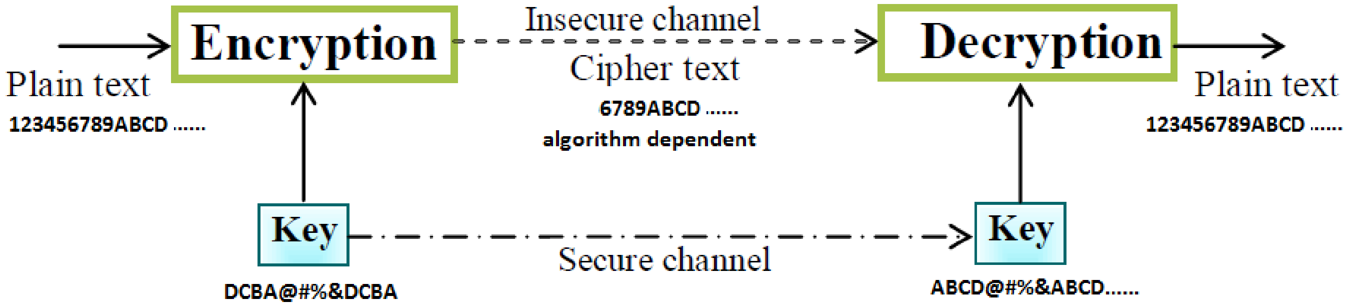

Fig. 3 Asymmetric key encryption and decryption [7]

ENCRYPTION AND DECRYPTION ALGORITHMS

There are many algorithms developed for encryption and decryption of text based on key length and block size and their usage as symmetric and asymmetric key authentication schemes. The algorithms are discussed here.

DES Algorithm

National Institute of Standard and Technology (NIST) [1, 9] published a proposal from IBM in 1973 for symmetric key cryptosystem. In March 1975, DES was accepted and published as a draft of Federal Information Processing Standard (FIPS) and finally published in January 1977 as FIPS 46 in the Federal Register. The algorithm DES is applicable for 64 bit plain text and encoded 64 bit cipher text for text encryption. In the decryption same 64 bit cipher text is decoded as decrypted text. The value of key size is 56 bits. In DES algorithm, there also exists Triple DES algorithm. In DES encryption operation transformation of a 64-bit block into a block of the same size is possible. In Triple-DES, encryption key size is of 56 bits, with one to three keys used. Triple-DES [6, 7] is a minor variation of DES. , it can be much more secure, if used properly. Although. Triple DES is 3 times slower than DES. In present scenario, Triple-DES is more widely than DES, because DES is easy to break with the help of advanced technology that is widely available today. Moreover, 3DES encryption and decryption algorithm are used as because of the longer key length that it uses. The adoption of DES as federal standard, there are concerns about its security levels. The ley length of 56 bits, provide 2^{56} [9, 10] possible keys, In July 1988, DES algorithm was declared insecure by Frontier Foundation (EFF) when EFF published a detailed report of DES Cracker machine and the hardware price was declined due to DES crack and make DES worthless. Triple DES was successful in comparison to DES. Triple DES requires a key length of 56 x 3 = 168 bits, which may be wide in comparisons to plain text.

AES Algorithm

AES is based on the Rijndael cipher and developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen. They submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. The **Advanced Encryption Standard** (**AES**) [7, 9] is standardized by the U.S. National Institute of Standards and Technology (NIST) in 2001 and is a specification for the encryption of electronic data established. For AES, NIST 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. U.S government has been adopted AES and is now accepted worldwide. It is the advanced version of DES algorithm developed in 1977. The algorithm used in AES is based on symmetric key approach in which same key is shared by both encrypting and decrypting. In the US, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable. After the approval of Secretary of Commerce, AES became effective as a federal government standard on May 26, 2002. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module. The criteria defined by selecting AES fall into three areas Security, Implementation and cost of the algorithm. The main emphasis was the security of the algorithm to focus on resistance of cryptanalysis attacks, implementation cost should be less so it can be used for small devices like smart cards. The AES algorithm is a private key block cipher. It encrypts data of block size 128 bits. It uses three key sizes, 128 bits, 192 bits and 256 bits in three versions. AES uses three different types of round operations. Table I shows the number of rounds in three versions of AES. But, in each version final round key is 128 bits.

Table I: Round key size and number of rounds in three versions of AES [7]

Cipher Key size	No. of rounds	Round Key Size
128 bits	10	128 bits
192 bits	12	128 bits
256 bits	14	128 bits

The initialization is done by adding first round key (128 bits) with 128 bits plain text. In subsequent steps, the following transformations are done: sub bytes, mix columns, shift rows and add round key. The last round is different from the previous rounds as there is no mix columns transformation. The internal 128 bits data in AES [8] are represented in the form of 4x4 square matrix containing elements of size 8 bits and named as state elements. The decryption process involves of the inverse steps, decryption round contains of: Inverse S-BOX used for Byte Substitution, Inverse Shift Rows, Add Round Key and Inverse Mix Columns. The round keys will be generated using a unit called the key generation unit. This unit will be generating 176, 208 or 240 bytes of round keys depending on the size of the used key. The Add Round Key adds the round key word with each column of state matrix. It is similar to mix columns; the Add Round Key precedes one column at a time. The most important in this transformation, that it includes the cipher key. The state column will get XOR with key which is generated by key generator and create another state as shown in fig. 1

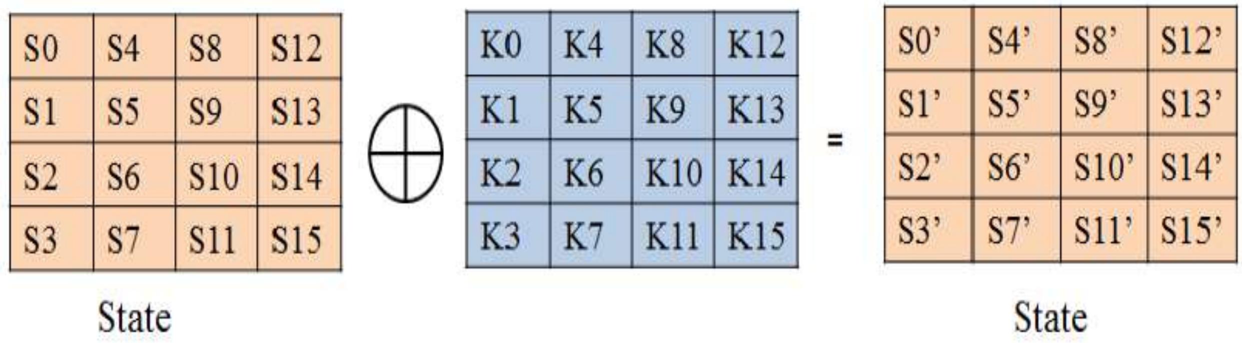

Fig.1 AES encryption with shift row transformations [7, 9]

KASUMI ENCRYPTION

KASUMI is a technique based on block cipher used in Universal Mobile Telecommunication System (UMTS), mobile communication and GSM. KASUMI is used in the integrity and confidentiality algorithms with names UIA1 and UEA1 respectively. In GSM, KASUMI is used in the **A5/3** key stream generator and in GPRS in the **GEA3** key stream generator. KASUMI was used in UMTS security system by the Security Algorithms Group Experts (SAGE) designed for 3GPP to be a part of the European standards body ETS because of schedule pressures in 3GPP standardization. SAGE agreed with 3GPP technical specification group (TSG) for system aspects of 3G security (SA3) to base the development on an existing algorithm that had already undergone some evaluation. They chose the cipher algorithm developed and patented by Mitsubishi Electric Corporation, Instead of developing a new cipher. The original algorithm was slightly modified for easier hardware implementation and to meet other requirements set for 3G mobile communications security. It processes 64-bit blocks using 128-bit key. Basic core is very small (5,500 gates). KASUMI is a block cipher with 128-bit key and 64-bit input and output. The core of KASUMI is an eight-round Feistel network. The round functions in the main Feistel network are irreversible Feistel-like network transformations. In each round the round function uses a round key which consists of eight 16-bit sub keys derived from the original 128-bit key using a fixed key schedule.

Blowfish

Blowfish is a symmetric block key encryption technique which can be used as a drop in the replacement of DES. Blowfish algorithm was designed by Bruce Schneiner in 1993. It is a faster, free alternative to existing encryption algorithms. It has variable size of key has 32 bits to 448 bits in which the concept of S box is used with pseudorandom digits and then alters the contents with the help of key. S boxes are random and key dependent. In key dependent S boxes the great advantage is to analyze the S boxes ahead of time to look for weaknesses. Blowfish is license free, unpatented and easily accessed by all users and available free to use.

RSA

It is a public key cryptography method developed by Ron Rivest, Adi Shamir and Len Adleman (RSA) at MIT. The scheme was widely accepted by public and implemented to general public encryption method. The RSA algorithm is block cipher method in which plain text and cipher text integrates between 0 to n-1 or some value of n. The typical value of size is 1024 bits to 309digits and n is less than 2^{1024}. RSA uses a public key and a private key**.** The public key is known to everybody and is used for encrypting messages. All the messages encrypted with the public key can only be decrypted with the help of private key. In RSA method a user creates and then publishes along with an auxiliary value as their public key the product of two large prime numbers. The prime factors must be kept secret.

RC4

RC4 algorithm is a stream cipher based algorithm designed by Ron Rivest in 1987 for RSA security. It has variable key size stream cipher with byte oriented operations and based on variable permutation. It is widely used software cipher in Transport layer security/ secure socket layers (TLS/SSL) standard, which are defined for communication between servers and browsers. It is also used in IEEE 802.11 LAN standards such as WiFi Protected Access (WPA) protocol and Wired Equivalent Privacy (WEP) protocols. It is declared a trade secret by RSA security. No doubt, it is remarkable for its simplicity and speed in software. RC4 generates a pseudorandom stream of bits. These can be used with any stream cipher for encryption by combining it with the plaintext using bit-wise exclusive and decryption is performed the same way The RC4 algorithm was anonymously posted on internet in Sep 1994 on the Cypherpunks anonymous remailers list. In RC4 algorithm a variable key from 1 to 256 bytes is used to start a 256 byte state vector S, and the elements are S[0[, S[1], …..S [255]. It is based on the generation of a byte k from S with selection one of 255 entries in a systematic fashion for encryption and decryption. The algorithm is based on use on random permutation. The entries in S are once again permuted, as each value of k is generated.

X-MODDES Algorithm

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi fi alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system.X-MODDES is a block cipher algorithm and unique independent approach which uses several computational steps along with string of operators and randomized delimiter selections by using some suitable mathematical logic. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message with limited size. It also protects the cipher text from the attacks like Brute-force like attack because it is fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys.

TACIT Algorithm

The TACIT encryption logic [6] for data communication between two nodes of NoC is presented with the help of following algorithm. The corresponding flowchart of the algorithm is shown in figure 2(a).

Step 1: Text file content is read and position of the character is shuffled by using initial permutation approach using key value.

Step 2: Read the character from the text file corresponding to the text and get the ASCII value of that character.

Step 3: Perform XOR operation with the specific n-bit key value.

Step 4: A secure tacit logic has been introduced (i.e. n^k xor k^k along with some specific operations; where n is the value computed from step 3).

Step 5: Convert the value into binary one.

Step 6: Perform reverse operation on the binary string.

Step 7: Corresponding decimal value is found.

Step 8: The Unicode character corresponds to the decimal value is formed which is none other than the cipher text.

Step 9: Continue step 1 to 7 for the next characters of the file until End of File (EOF) is reached.

The decoding of same data is done at receiving end. The text which is encoded at transmitting end using TACIT encryption technique is converted into cipher text. The decryption algorithm [6] decodes the cipher text with the same key at the receiving end that follows the steps listed below. The corresponding flow chart of the decryption algorithm [6] is shown in figure 2(b).

Step 1: Read the first character from the cipher text and get the corresponding decimal value of it.

Step 2: The corresponding binary value is evaluated and make the reverse of it.

Step 3: Inverse of the tacit logic is applied.

Step 4: Perform XOR with n-bit key value.

Step 5: The character corresponds to it is determined.

Step 6: Now reshuffling is done using key value.

Step 7: Repeat the steps (1 to 6) till the end.

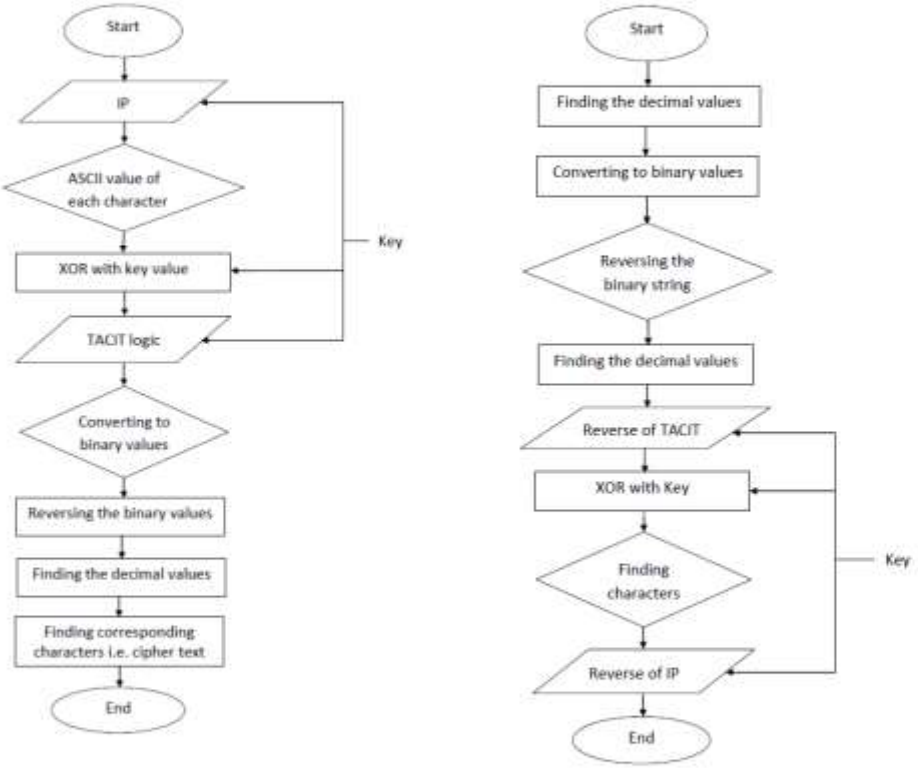
Start
IP
ASCII value of each character
XOR with key value
TACIT logic
Key
Converting to binary values
Reversing the binary values
Finding the decimal values
Finding corresponding characters i.e. cipher text
End
Start
Finding the decimal values
Converting to binary values
Reversing the binary string
Finding the decimal values
Reverse of TACIT
XOR with Key
Key
Finding characters
Reverse of IP
End

Fig. 2(a) & (b) TACIT Encryption and Decryption Technique [6]

Comparison with existing algorithms

The key size is a very important aspect to secure the data, long key size means the data is more secured. Encryption algorithms are very important for cryptography with an approach of key management because there are different algorithms that offer different degree of security based on key size. There are couples of encryption and decryption algorithms which are already proposed. A comparison of these techniques is shown in table 2. Table shows the various cryptographic techniques and their features on the basis of type, key size, and block size. It can be seen that from this comparison table that TACIT encryption technique has a unique independent approach by having a new key distribution system along with mathematical foundation [8]. The main advantage of TACIT logic is that, it can process 'N' bits blocks and 'N' bits key size. This approach may be good if the block size is less than the key size . The algorithm may be implemented in any languages, which support unicode system facility like VHDL, Verilog HDL, Java, C#, System C, .Net, etc.

Table 2 Comparison of various encryption algorithms on the basis of key size and block size [84].

Algorithm	*Key size (bits)*	*Block size (bits)*	*Features*
DES	56	64	The key length is not string and it is a very common method. There are the chances of timing attacks in DES. The exploration of timing attack is the fact that an encryption and decryption takes offers slightly different time for different inputs.
Triple DES	168	64	In this the key length was somewhat widely than block size, It is based on the modification of DES algorithms, and has adequate security
AES	Variable (192 /256)	128	Replacement of DES, Excellent security, limited key size. . It encrypts data of block size 128 bits. It uses three key sizes, 128 bits, 192 bits and 256 bits in three versions. AES uses three different types of round operations
Kasumi	128	64	Designed for Third Generation Partnership Project(3GPP), used in

Encryption core			Universal Mobile Telecommunication System UMTS, limited to 64-bits word
Blowfish	448	64	Excellent security, No. of bits are variable ranging from 32-448 bits. It is concept of S box is used with pseudorandom digits and then alters the contents with the help of key
RSA	1024	128	It is an asymmetric algorithm, speed is low. The common measure of the efficiency of the algorithm is its time complexity. For a given size of input and given processor speed, execution time of the algorithm takes more steps.
RC4	Variable (40 or 128)	Variable (32,64,128)	It is based on random permutation in which eighth to sixteen machine operations are required per output byte. In it, cipher is expected to run in software very quickly. Fast stream chipper in Secured Socket Layer (SSL), more memory is required since they work on large chunk of data (stream) instead of block cipher.
X-MODES	32	32	Enhanced security level & faster.
TACIT Encryption	n-bits	n-bits	Good for small size of packets

CONCLUSIONS

Traditionally, cryptography is used to ensure communication secrecy to pass coded messages between parties. Cryptography systems are techniques used to processes, mechanisms provide for secure communications between authorized parties while preventing unauthorized parties from monitoring communications or counterfeiting messages. In its simplest and way, cryptography substitutes or transposes letters to create a coded message, which is called a cipher, used to transform a readable message called plaintext or clear text into an unreadable, hidden message or scrambled called cipher text. The comparative study of various network security algorithms like AES, DES, Triple DES, Triple AES, Kasumi, Blowfish, RSA, RC4, XMODES and TACIT is done successfully with their key size and block size.

REFERENCES

1. Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, “Implementation of AES Encryption and Decryption” International Conference on “Control, Automation, Communication and Energy Conservation -2009, (page 1-5)
2. I. Hammad, K. E. Sankary and E. E. Masry, “High-Speed AES Encryptor With Efficient Merging Techniques,” IEEE Embedded Systems Letters, Vol.2 (3), pp.67- 71, Sept. 2010.
3. J. M. G. Criado, M. A. V. Rodriguez, J. M. S. Perez, J. A. G. Pulido, “A new methodology to implement the AES algorithm using partial and dynamic reconfiguration,” Integration, the VLSI Journal, Vol.43(1), pp. 72-80, Jan. 2010.
4. J. V. Dyken, J. G. Delgado-Frias, “FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm,” Journal of Systems Architecture, Vol.56(2–3), pp. 116-123, Mar. 2010.
5. Nikos Sklavos, Alexabdros Papakonstinou, Spyros Theoharis Odysseas Koufopavlou, “Low-power Implementation of an Encryption/Decryption System with Asynchronous Techniques”, VLSI Design, Taylor and Francis 2002 Vol. 15 (1), pp. (455–468)
6. Prosanta Gope, Ashwani Sharma Ajit Singh Nikhil Pahwa “An Efficient Cryptographic Approach for Secure Policy Based Routing (TACIT Encryption Technique)”, Conference Proceedings, IEEE Xplorer, (2011), pp (359-363)
7. SAURABH KUMAR Theis on “VLSI Implementation of AES Algorithm” NIT Rourkela, 2013, pp (1-72)
8. Tim Good and Mohammed Benaissa, “Very Small FPGA Application-Specific Instruction Processor for AES”, IEEE Transactions on Circuit and Systems-I, Vol. 53, No. 7, July 2006.
9. William Stallings “Cryptography and Network security” Fifth Edition Pearson india Ch-1 to Ch-5, pp 31-200
10. X. Zhang, K. K. Parhi, “High-Speed VLSI Architectures for the AES Algorithm,” IEEE Transactions on Very Large Scale

Integration (VLSI) Systems, Vol. 12 (9), pp. 957-967, Sep. 2004

11.