International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Survey on network security using cryptography by both decryption encryptions

N.yamini[1] & J V S Arundathi[2]
[1]Assistant professor in Medha Institute of Science and Technology for Women.
namburi.yamini@gmail.com
[2]Associate professor in Medha Institute of Science and Technology for Women.

Abstract

With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. Data security is the utmost critical issue in ensuring safe transmission of information through the internet. Also network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-criminals. It comprises authorization of access to information in a network, controlled by the network administrator. The task of network security not only requires ensuring the security of end systems but of the entire network. In this paper, an attempt has been made to review the various Network Security and Cryptographic concepts. This paper discusses the state of the art for a broad range of cryptographic algorithms that are used in networking applications.

Keywords: network security; cryptography; decryption; encryption.

1. Introduction

Internet has become more and more widespread, if an unauthorized person is able to get access to this network, he can not only spy on us but he can easily mess up our lives. Network Security & Cryptography is a concept to protect network and data transmission over wireless network. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network. Security of data can be done by a technique called ***cryptography***. So one can say that cryptography is an emerging technology, which is important for network security.

Model for Cryptosystem Using Neural Network [1] supports high security. Neural network and cryptography together can make a great help in field of networks security. The key formed by neural network is in the form of weights and neuronal functions which is difficult to break. Here, content data would be used as an input data for cryptography so that data become unreadable for attackers and remains secure from them. The ideas of mutual learning, self-learning, and stochastic behavior of neural networks and similar algorithms can be used for different aspects of cryptography, like public-key cryptography, solving the key distribution problem using neural network mutual synchronization, hashing or generation of pseudo-random numbers. Another idea is the ability of a neural network to separate space in

non-linear pieces using "bias". It gives different probabilities of activating or not the neural network. This is very useful in the case of Cryptanalysis.

Network security [2] consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Cryptography is the science of writing in secret code. More generally, it is about constructing and analyzing protocols that block adversaries; [3] various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [4] are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The development of the *World Wide Web* resulted in broad use of cryptography for e-commerce and business applications. Cryptography is closely related to the disciplines of ***cryptology*** and ***cryptanalysis***. Techniques used for decrypting a message without any knowledge of the encryption details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code." The areas of cryptography and cryptanalysis together are called cryptology. ***Encryption*** is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). ***Decryption*** is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. ***Cryptosystem*** is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key.

The challenging problem is how to effectively share encrypted data. Encrypt message with strongly secure key which is known only by sending and recipient end is a significant aspect to acquire robust security in sensor network. The secure exchange of key between sender and receiver is too much difficult task in resource constraint sensor network. data should be encrypted first by users before it is outsourced to a remote cloud storage service and both data security and data access privacy should be protected such that cloud storage service providers have no abilities to decrypt the data, and when the user wants to search some parts of the whole data, the cloud storage system will provide the accessibility without knowing what the portion of the encrypted data returned to the user is about. This paper reviews various network security and cryptographic approaches.

2. Related Work

2.1 Types of Security Attacks:

2.1.1 Passive Attacks

This type of attacks includes observation or monitoring of communication. A passive attack attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent is to obtain information that is being transmitted. Types of passive attacks:

• **Traffic Analysis:** The message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

• **Release of Message Contents:** Read contents of message from sender to receiver.

2.1.2 Active Attacks

An active attack attempts to alter system resources or affect their operation. It involves some modification of the data stream or the creation of a false stream. Types of active attacks:

• **Modification of Messages:** some portion of a legitimate message is altered, or that messages are delayed or reordered.

• **Denial of Service:** An entity may suppress all messages directed to a particular destination.

• **Replay:** It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

• **Masquerade:** It takes place when one entity pretends to be a different entity.

2.2 Security Services:

It is a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. It enhances the security of data processing and transferring.

(a) Data Integrity

It can apply to a stream of messages, a single message, or selected fields within a message. A loss of integrity is the unauthorized modification or destruction of information.

(b) Data Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

(c) Authenticity

Provide authentication to all the node and base station for utilizing the available limited resources. It also ensures that only the authorized node can participant for the communication.

(d) No repudiation

No repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

(e) Access Control

Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

(f) Network Security Model

Figure 1 shows the model of network security. A message is to be transferred from one party to another across some sort of Internet service. A third party may be responsible for distributing the secret information to the sender and receiver while keeping it from any opponent. Security

aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Message should be encrypted by key so that it is unreadable by the opponent.
- An encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

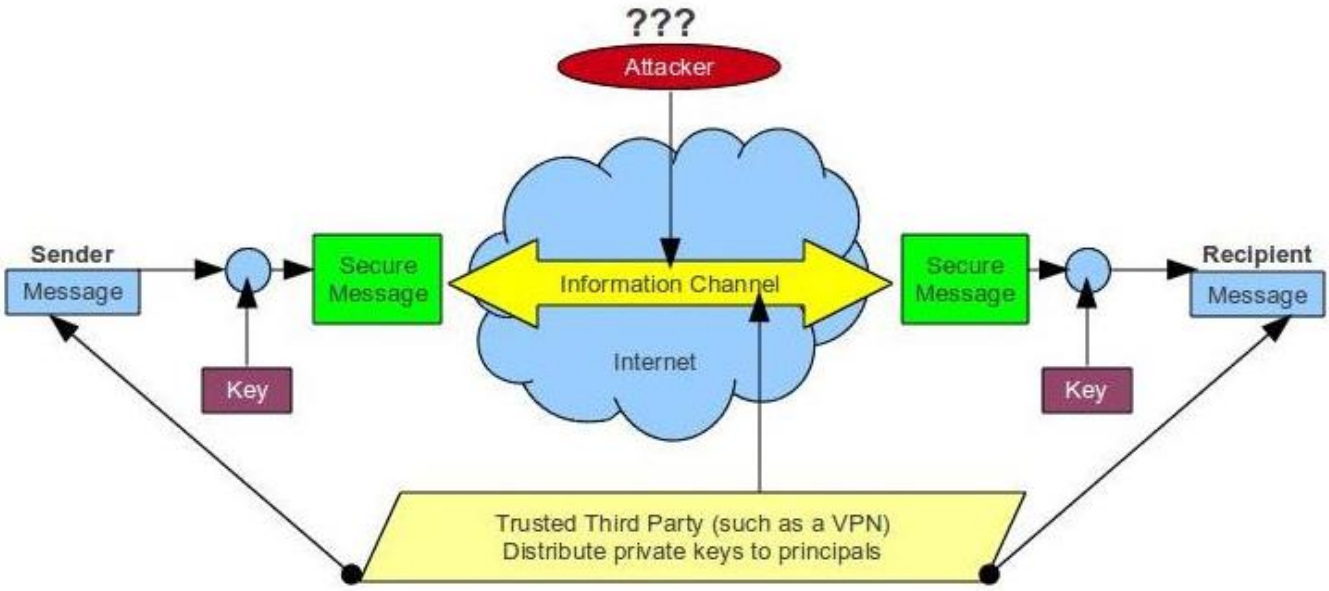

Fig 1. Model for Network Security

Need for Key Management in Cloud

Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. In particular, data to encrypt their own data. Both encryption and key management are very important to help secure applications and data stored in the Cloud. Requirements of effective key management are discuss below.

Secure key stores: The key stores themselves must be protected from malicious users. If a malicious user gains access to the keys, they will then be able to access any encrypted data the key is corresponded to. Hence the key stores themselves must be protected in storage, in transit and on backup media.

Access to key stores: Access to the key stores should be limited to the users that have the rights to access data. Separation of roles should be used to help control access. The entity that uses a given key should not be the entity that stores the key.

Key backup and recoverability: Keys need secure backup and recovery solutions. Loss of keys, although effective for destroying access to data, can be highly devastating to a business and Cloud providers need to ensure that keys aren't lost through backup and recovery mechanisms.

3. Implementation

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

3.1 Cryptography Mechanism:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext message (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.

Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender A uses the key K (or some set of rules) to encrypt the plaintext message M and sends the ciphertext C to the receiver. The receiver applies the same key K (or ruleset) to decrypt the cipher text C and recover the plaintext message M. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

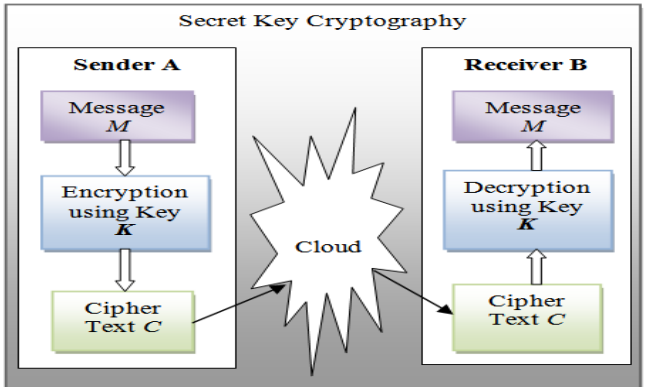

Fig 2. Secret Key Cryptography.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher. Block ciphers can operate in one of several modes; the following four are the most important:

- **Electronic Codebook (ECB) mode is the simplest, most obvious application:** the secret key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks, then, will always generate the same ciphertext block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.
- **Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme.** In CBC, the plaintext is exclusively-ORed (XORed) with the previous ciphertext

block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.

• **Cipher Feedback (CFB) mode is a block cipher implementation as a self-synchronizing stream cipher.** CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.

• **Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher.** OFB prevents the same plaintext block from generating the same cipher text block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bit streams.

Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is. One problem is error propagation; a garbled bit in transmission will result in n garbled bits at the receiving side. Synchronous stream ciphers generate the key stream in a fashion independent of the message stream but by using the same key stream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the key stream will eventually repeat.

Secret key cryptography algorithms that are in use today include:

• **Data Encryption Standard (DES):** DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES algorithm as described by Davis R. [5] takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length. 3DES (Triple DES) [6] is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time.

• **Advanced Encryption Standard (AES):** AES [7, 8] is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128- bit key is 10. Unlike its predecessor DES, AES does not use a Feistel network. Feistel networks do not encrypt an entire block per iteration, e.g., in DES, 64/2 = 32 bits are encrypted in one round. AES, on the other hand, encrypts all 128 bits in one iteration.

• **Blowfish:** Blowfish [9] is a symmetric 64-bit block cipher, invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of

products. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

• **Two fish:** [10] A 128-bit block cipher using 128-, 192-, or 256-bit keys. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Designed by a team led by Bruce Schneier and was one of the Round 2 algorithms in the AES process. Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the pseudo-Hadamard transform(PHT) from the SAFER family of ciphers. Twofish has a Feistel structure like DES.

• **Camellia:** [11] A secret-key, block-cipher crypto algorithm developed jointly by Nippon Telegraph and Telephone (NTT) Corp. and Mitsubishi Electric Corporation (MEC) in 2000. C has some characteristics in common with AES: a 128-bit block size, support for 128-, 192-, and 256-bit key lengths, and suitability for both software and hardware implementations on common 32-bit processors as well as 8-bit processors (e.g., smart cards, cryptographic hardware, and embedded systems). Camellia is a Feistel cipher with either 18 rounds (when using 128-bit keys) or 24 rounds (when using 192 or 256-bit keys). Every six rounds, a logical transformation layer is applied: the so-called "FL-function" or its inverse. Camellia uses four 8 x 8-bit S-boxes with input and output affine transformations and logical operations. The cipher also uses input and output key whitening. The diffusion layer uses a linear transformation based on a matrix with a branch number of 5.

• **KASUMI:** [11, 12] A block cipher using a 128-bit key and block size 64-bit, is part of the Third-Generation Partnership Project (3gpp), formerly known as the Universal Mobile Telecommunications System (UMTS). KASUMI is the intended confidentiality and integrity algorithm for both message content and signaling data for emerging mobile communications systems. KASUMI is used in the A5/3 key stream generator and in GPRS in the GEA3 key stream generator. In 2010, Dunkelman, Keller and Shamir published a new attack that allows an adversary to recover a full A5/3 key by related-key attack [13]. 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.

3.2 Public-Key Cryptography

Public-key cryptography is a form of cryptosystem in which encryption and decryption are performed using the different keys—one a public key and one a private key. These keys are mathematically related although knowledge of one key does not allow someone to easily determine the other key. As shown in Figure 3, the sender A uses the public key of receiver B (or

some set of rules) to encrypt the plaintext message M and sends the ciphertext C to the receiver. The receiver applies own private key (or ruleset) to decrypt the cipher text C and recover the plaintext message M. Because pair of keys is required, this approach is also called asymmetric cryptography. Asymmetric encryption can be used for confidentiality, authentication, or both. Applications for Public-Key Cryptosystems are given in Table 1.

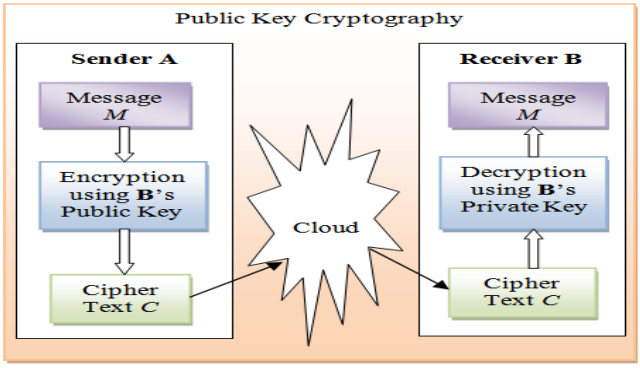

Fig 3: Public Key Cryptography.

(i) RSA

The first, and still most common, public key cryptography implementation, named for the three MIT mathematicians who developed it — Ronald Rivest, Adi Shamir, and Leonard Adleman [14]. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. RSA has three phases: Key Generation, Encryption, and Decryption.

(ii) Diffie-Hellman Key Exchange

A simple public-key algorithm is Diffie-Hellman key exchange [15]. This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established. D-H is used for secret-key key exchange only, and not for authentication or digital signatures. Algorithm is as follow:

1) Select two Global Public Elements: a prime number p and an integer α that is a primitive root of p.

2) Sender Key Generation: Sender selects a random integer XA < p which is private and computes YA = α XA mod p, which is public.

3) Receiver Key Generation: Receiver selects a random integer XB < p which is private and computes YB = α XB mod p, which is public.

4) Sender calculates secret key: K = (YB) XA mod p

5) Receiver calculates secret key which is identical to sender secret key. K = (YA) XB mod p.

(iii) Elliptic Curve Cryptography

It is analog of Diffie-Hellman Key Exchange. ECC [16, 17] is a public key cryptography algorithm based upon elliptic curves. Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptography (ECC) schemes, including key exchange, encryption, and digital signature. For purposes of ECC, elliptic curve arithmetic involves the use of an elliptic curve equation defined over a finite field. The coefficients and variables in the equation are elements of a finite field. Security of ECC is based on the intractability of ECDLP i.e. Elliptic Curve Discrete Logarithm Problem.

(iv) Digital Signature Standard

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

The digital signature standard (DSS) is an NIST standard that uses the secure hash algorithm (SHA) [18]. A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

Figure 4 shows the process of making and using digital signatures. Sender can sign a message using a digital signature generation algorithm. The inputs to the algorithm are the message and sender's private key. Any other user, say receiver, can verify the signature using a verification algorithm, whose inputs are the message, the signature, and sender's public key.

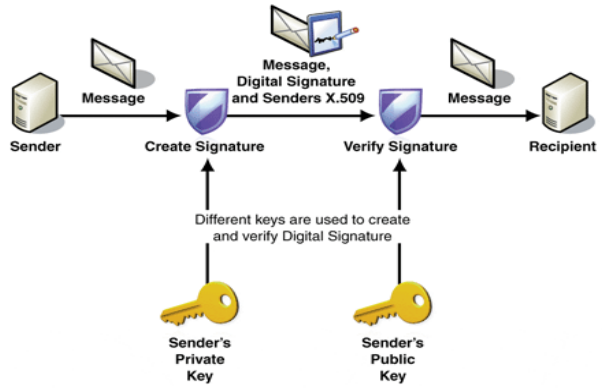

Fig 4: Digital Signature without Hash Function.

4. Conclusion

With the explosive growth in the Internet, network and data security have become an inevitable concern for any organization whose internal private network is connected to the Internet. The security for the data has become highly important. User's data privacy is a central question over cloud. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application.

The paper presented various schemes which are used in cryptography for Network security purpose. Encrypt message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security in cloud. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity. Network security covers the use of cryptographic algorithms in network protocols and network applications. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security

In the future, work can be done on key distribution and management as well as optimal cryptography algorithm for data security over clouds.

5. References

[1] Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network," Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014 In article

[2] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323. In article CrossRef

[3] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10. In article

[4] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. "A. Handbook of Applied Cryptography". ISBN 0-8493-8523-7. In article

[5] Davis, R., "The Data Encryption Standard in Perspective," Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978. In article

[6] S. NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004. In article

[7] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001. In article

[8] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, November 26, 2001. In article

[9] Bruce Schneier (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings (Springer-Verlag): 191-204. In article

[10] Schneier, Bruce (2005-11-23). "Twofish Cryptanalysis Rumors". Schneier on Security blog. Retrieved 2013-01-14. In article

[11] Matsui, Mitsuru; Tokita, Toshio (Dec 2000). "MISTY, KASUMI and Camellia Cipher Algorithm Development". Mitsibishi Electric Advance (Mitsibishi Electric corp.) 100: 2-8. ISSN 1345-3041. In article

[12] General Report on the Design, Speification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms". 3GPP. 2009 In article

[13] O. Dunkelman, N. Keller, A. Shamir, \A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony," Advances in Cryptology, Proceedings Crypto'10, LNCS, T. Rabin, Ed., Springer, Heidelberg, 2010 In article

[14] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.In article
CrossRef

[15] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644-654.In article Cross Ref

[16] Koblitz, N., 1987. "Elliptic curve cryptosystems. Mathematics of Computation" 48, 203-209.
In article Cross Ref.

[17] Miller, V., 1985. "Use of elliptic curves in cryptography". CRYPTO 85. In article

[18] FIPS 180, Secure Hash Standard, Federal Information Processing Standard (FIPS), Publication 180, NIST, U.S. Dept. of Commerce, May 11, 1993. In article

[19] M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen, M. Schl□a er, \Rebound distinguishers: results on the full Whirlpool compression function," Advances in Cryptology, Proceedings Asiacrypt'09, LNCS 5912, M. Matsui, Ed., Springer, Heidelberg, 2009, pp. 126-143. In article

[20] Bellare, Mihir; Canetti, Ran; Krawczyk, Hugo (1996). "Keying Hash Functions for Message Authentication". In article

[21] NIST Special Publication 800-38B, "Recommendation for Block Cipher Modes of Operation": The CMAC Mode for Authentication, May 2005. In article

Authors Profiles

N.yamini working as assistant professor in medha institute of science and technology for women . namburi.yamini@gmail.com

J V S Arundathi working as associate professor in Medha institute of science and technology for women