Survey of various Cryptographic Algorithms in Network Security

Prof.S.Priyadarshini[1], Prof.R.Arun Kumar[2], Prof.C.Karthikeyan[3]
Department of Computer Science and Engineering
[1, 2, 3]United Institute of Technology

Abstract-*Information security is part of every IT professional's job. Hackers are constantly trying to compromise your networks, steal sensitive data, and overwhelm your systems. The significance and the value of exchanged data over the Internet or other media types are increasing, the search for the best way out to offer the necessary protection against the data thieves' attacks. Encryption algorithms play a most important role in information security systems. There are two types of cryptography algorithms such as symmetric key cryptography and asymmetric key cryptography. This paper gives the review of various cryptography algorithms for network security, some related work already done by various authors, problems in existing work and some proposals for proposed work.*

Keywords-Encryption, Decryption, Computer Security, Cryptography Techniques.

I. INTRODUCTION

Cryptography is the art and science of achieving security by encoding messages to make them readable. The organizational data is of very important. So there is a crucial need to protect that data against unauthorized access, modification or denial of services etc. Cryptography of the data is nothing but the amalgamation of the contents of data, in such a way that, it is unreadable, invisible or meaningless during transmission over the links. The data contents may include text, images, audio, video, etc. This process of hiding of data is also known as encryption [1]. The main objective of cryptography is to shield the data against the intruders. An encryption is a process to transform the plaintext into cipher text and decryption transforms the cipher text back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure transmission of the message and protect the message from unauthorized users.

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system [3]. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

1) Authentication: The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
2) Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.
3) Integrity: Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.
4) Non-repudiation: A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message.
5) Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

II. CLASSIFICATION OF CRYPTOGRAPHIC ALGORITHMS

Substitution Cipher

Substitution ciphers form the first of the fundamental building blocks. The two basic building blocks of all encryption techniques: substitution and transposition. The core idea is to replace one basic unit (letter/byte) with another. A substitution technique [7] is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. In Monoalphabetic cipher only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. The Play fair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword. The substitution is determined by m linear equations in which each

character is assigned a numerical value (a = 0, b = 1, … z = 25). A one-time pad [16] is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the cipher text contains no information whatsoever about the plaintext, there is simply no way to break the code.

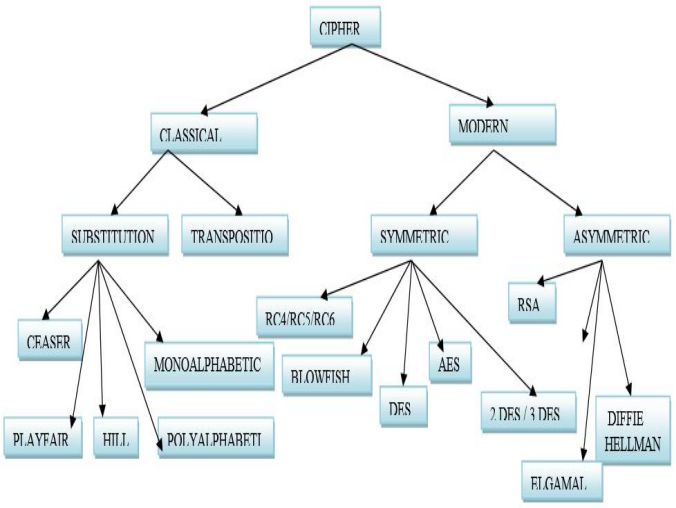

Fig 1: classifications of cryptographic algorithms

Transposition Cipher

A very different kind of mapping [9] is achieved by performing some sort of permutation on the plaintext letters. This technique [12] is referred to as a transposition cipher. A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the cipher text in a matrix and playing around with column positions. Diagram and trigram frequency tables can be useful. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed.

Symmetric (Secret) Key Cryptography

Traditional cryptography uses a single key to encrypt and decrypt a message. An algorithm that uses the same key to encrypt and decrypt is called symmetric [5]. This type of cryptography also deals with authentication, the main technique being the creation and verification of message authentication codes. The difficulty with secret-key cryptosystems is sharing a key between the sender and receiver without anyone else compromising it. In a system supporting a large number of users the key management problems can become very severe. The advantage of traditional cryptography is that it is usually much faster than public-key cryptography. The main techniques are block ciphers and stream ciphers

Block Ciphers

A block cipher transforms a fixed-length block [14] of plaintext into a block of cipher text of the same length, using a secret key. To decrypt, the reverse process is applied to the cipher text block using the same secret key. In the case of DES, the block size is 64 bits (8 bytes) and the key is 56 bits presented as 8 bytes, the low order bit of each byte being ignored. It is usual to set every 8th bit so that each byte contains an odd number of set bits. This process is known as DES key parity adjustment.

To use a block cipher to encrypt data of arbitrary length, we can use one of the following techniques (or modes of operation):

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

Most good block ciphers [15] transform the secret key into a number of sub keys and the data is encrypted by a process that has several rounds (iterations) each round using a different sub key. The set of sub keys is known as the key schedule. In the case of DES the secret key is transformed into 16 sub keys and consequently DES takes 16 rounds to perform an encryption.

1) Electronic Code Book

In ECB mode, each block of data is encrypted independently. If we take eK(D) to mean “encrypt block D with key K”, then the plaintext D1,D2,D3,…..,Dn is encrypted as eK(D1),eK(D2),….,eK(Dn).

The trouble with ECB mode is that plaintext patterns show up in the cipher text, because each identical block of plaintext gives an identical block of cipher text. This can lead to attacks based on rearranging, deleting or repeating cipher text blocks. ECB mode should only be used for encrypting very small blocks of data such as keys.

2) Cipher Block Chaining

In CBC mode each plaintext block is XOR’d with the previous cipher text block before it is encrypted. Because there is no previous cipher text for the first block, an 8-byte block known as the Initial Chaining Value (ICV) is used to

start the process. Patterns in the plaintext are hidden by the exclusive-OR. The ICV should be different for any messages encrypted with the same key, but it does not have to be kept secret and can be transmitted with the encrypted text. If the total length of the plaintext is not a multiple of 8, it is necessary to deal with the final short block. The obvious way to do this is to pad out the last block to 8 bytes, but the final block must contain a count of the number of filler bytes, so the message length is always increased by a maximum of 8 bytes. If this increase in length is not acceptable, a solution is to XOR the short block by re-enciphering the last complete cipher text block.

3) Cipher Feedback

In CFB mode the previous cipher text block is encrypted and is XOR'd with the plaintext to give the current cipher text block. As with CBC mode, an ICV is needed to start the process. As well as full 64-bit feedback, it is possible to define 1-bit, 2-bit, and up to 63-bit cipher feedback. In software implementations there is no advantage over CBC mode, though CFB is often used in link encryption devices.

Stream Ciphers

Stream ciphers [13] are typically much faster than block ciphers. A stream cipher generates a key stream (a sequence of bits or bytes used as a key). The plaintext is combined with the key stream, usually with the XOR operation. Generating the key stream may be independent of the plaintext and cipher text, to give a synchronous stream cipher. Alternatively it may depend on the cipher text, in which case the stream cipher is self-synchronizing. Nearly all stream cipher is of the synchronous type. There is no "standard" stream cipher, and in general stream ciphers are best avoided. Certain modes of operation of a block cipher transform it into a key stream generator and so any block cipher can be used as a stream cipher. Examples are DES in CFB or OFB modes. The cryptographic method uses of two different algorithms for encryption and decryption respectively, and a same key are used both the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data

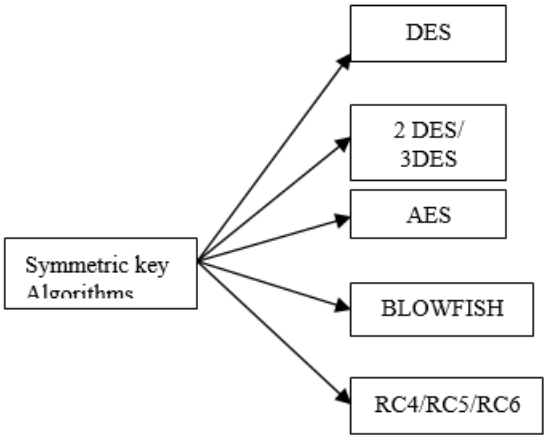

Fig 2: Types of Symmetric key Algorithms

DES (Data Encryption Standard)

DES Algorithm purpose [8] is to provide a standard method for protecting sensitive commercial and unclassified data. The same key used for encryption and decryption process. DES algorithm consists of the following steps[11]

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will processed by following

i. The key is split into two 28 halves
ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
iv. The rotated key halves from step 2 are used in next round.
v. The data block is split into two 32-bit halves.
vi. One half is subject to an expansion permutation to increase its size to 48 bits.
vii. Output of step 6 is exclusive-OR'ed with the 48- bit compressed key from step 3.
viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
ix. Output of step 8 is subject to a P-box to permute the bits. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

2 DES / 3 DES

The pragmatic approach was not to abandon [17] the DES completely, but to change the manner in which DES is used [4]. This led to the modified schemes of Triple DES (sometimes known as 3DES). There are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES). The user first generates and distributes a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length $3\times56 = 168$ bits.

AES

The Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST. AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

BLOWFISH

Blowfish is a symmetric cryptographic block cipher [8] which includes large number of cipher and encryption products. Blowfish's security has been extensively tested and proven. As a public domain cipher, Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. Blowfish is also one of the fastest block ciphers in public use, making it ideal for a product like SplashID that functions on a wide variety of processors found in mobile phones as well as in notebook and desktop computers. Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes.

RC4/RC5/RC6

RC4 a variable key-size stream cipher [10] with byte-oriented operations. The algorithm is based on the use of a random permutation.RC5 is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop-in replacement for DES), and 128 bits. The number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size. RC5 has three routines: key expansion, encryption, and decryption. RC6 is a parameterized algorithm where the block size, the key size, and the number of rounds are variable. The upper limit on the key size is 2040 bits.

Asymmetric (Public) Key Cryptography

Cryptographic method [20] makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender.

RSA

RSA is a public-key system designed by Rivest, Shamir, and Adleman. RSA algorithm is a public-key encryption method of having two keys called private and public keys. It is a block cipher encryption scheme and the key length of 1024 bits. RSA uses two prime numbers to generate public and private keys. These two prime numbers should be chosen randomly

DIFFIE-HELLMAN

Diffie–Hellman key exchange (D–H) is a specific method of exchanging cryptographic keys. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher

DSA

The digital signature can be used to provide assurance that the claimed signatory signed the information. A digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). These assurances may be obtained whether the data was received in a transmission or retrieved from storage. A properly implemented digital signature algorithm that meets the requirements of this Standard can provide these services.

A digital signature algorithm [18] includes a signature generation process and a signature verification process. A signatory uses the generation process to generate a

digital signature on data; a verifier uses the verification process to verify the authenticity of the signature. Each signatory has a public and private key and is the owner of that key pair. The key pair owner is the only entity that is authorized to use the private key to generate digital signatures. In order to prevent other entities from claiming to be the key pair owner and using the private key to generate fraudulent signatures, the Signature Generation Signature Verification Message/Data Message/Data Hash Function Hash Function Message Digest Public Private Signature Key Key Generation Signature Message Digest Signature [19] Valid or Verification Invalid. The approved digital signature algorithms are designed to prevent an adversary who does not know the signatory's private key from generating the same signature as the signatory on a different message. In other words, signatures are designed so that they cannot be forged. A number of alternative terms are used in this Standard to refer to the signatory or key pair owner. An entity that intends to generate digital signatures in the future may be referred to as the intended signatory. Prior to the verification of a signed message, the signatory is referred to as the claimed signatory until such time as adequate assurance can be obtained of the actual identity of the signatory

ELGAMAL

The ElGamal Algorithm provides an alternative to the RSA for public key encryption. The Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prim e modulus. ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext. It has the advantage the same plaintext gives a different ciphertext (with near certainty) each time it is encrypted

III.CONCLUSION

Cryptography [21] is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified; By reviewing the papers we finally conclude that the performance evaluation of cryptography algorithm depends on throughput of encryption scheme, CPU time taken & packet size. The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value increases, the power consumption by this encryption technique is decreased. AES is the far better algorithm in terms of performance and security but its power consumption is on high. The future work can be done in comparative study of symmetric algorithms on the specific or different parameters like flexibility, speed, encryption time, scalability and memory usage. This will lead to find which one is best in all the parameters to reach better security to the complicated or unsecured network.

REFERENCES

[1] Anjula Gupta , et.al. "Cryptography Algorithms: A Review "International Journal of Engineering Development and Research, Vol.2 No.2, (2014).

[2] Prerna Mahajan & Abhishek Sachdeva,"A study of Encryption Algorithms AES, DES and RSA for Security", Global journal of Computer Science and Technology, Vol.8,No.15, (2013) pp.15-22.

[3] Mini Malhotra et.al. " Study of Various Cryptographic Algorithms", International Journal of Scientific Engineering and Research, Vol.1, No.3, (2013), PP.77-88.

[4] Gurpreet Singh, et al." A Study of Encryption Algorithms (RSA, DES, 3DES, and AES for Information Security" , International Journal of Computer Applications, Vol.67, No.19, (2013), pp.33-38.

[5] Rejani. R et.al, "Study of Symmetric key Cryptography algorithms" International Journal of Computer Techniques, Vol.2, No.2, (2015), pp.45-50.

[6] Shashi Mehrotra Seth et.al," Comparative Analysis Of Encryption Algorithms For Data Communication", International Journal of Computer Science and Technology, Vol.2, No.2 (2011) pp.292-294.

[7] M.B.Nivetha, et.al. "A Comparative analysis of Cryptography Algorithms", International Journal of Innovative Research in Electrical Electronical and Instrumentation Control Engineering, Vol.2, No.10,(2014), pp.2102-2105

[8] Srinivas B.L et.al. "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm" International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, No.5, (2014), pp.77-88.

[9] Chadi RIMAN et.al. "Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey", Information Security and Computer Fraud, Vol. 3, No. 1, (2015), pp. 1-7.

[10] Nidhi singhal et.al. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer trends and Technology, (2011), pp.177-181.

[11] Depavath Harinath et.al. "Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security" , International Journal of Advanced Research in Computer Science and Software Engineering, Vol.5, No.7 (2015), pp.680-688.

[12] Alese, B, et.al. "Comparative Analysis of Public-Key Encryption Schemes" International Journal of Engineering and Technology,Vol.2,No.9,(2012) pp. 1552-1568.
[13] Piyush Gupta, et.al "A Comparative Analysis of SHA and MD5 Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5, No.3 (2014), pp.4492-449.
[14] Gunjan Gupta, Rama Chawla " Review on Encryption Ciphers of Cryptography in Network Security", International Journal of Advanced Research in Computer Science and Engineering, Vol 2, No. 7 (2012), pp.211-213.
[15] SumedhaKoushik, AnkurSinghal "Network Security using Cryptography Techniques", International Journal of Advanced Research in Computer Science and Engineering, Vol 2, No. 12, (2012) pp.105-107.
[16] JyotiAttri, Aarti Devi, AnkushSharma&Pratibha Sharma "Study on Cryptographic Techniques in Computer Network Security", Asian Journal of Basic Advanced Sciences, Vol 2, No. 3, pp.98-102.
[17] Divya Sukhija "Study A Review Paper on AES and DES Cryptographic Algorithms", International Journal of Electronics and Computer Science Engineering, Vol 3, No. 4, pp.354-359.
[18] William Stallings, A Book of "Cryptography and Network Security Principles and Practice" Fifth Edition, 2006.
[19] Swati Kashyap, Er.NeerajMadan "A Review on: Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Engineering, Vol 5, No. 4 (2015), pp.1414-1418.
[20] Rajdeep Bhanot, Rahul Hans "A Review and comparative Analysis of Various Encryption Algorithms" International Journal of Security and its Applications, Vol 9, No. 4, (2015) pp.289-306.
[21] Mansoor Ebrahim, "Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Aplications" Vol.61, No.20, (2013), pp.12-19.