Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW PAPER
Available Online at www.ijarcs.info

Analysis of Cryptography and Comparison of its Various Techniques

Anu
Assistant professor (Resource Person)
Department of Computer Science (UIET)
Maharshi Dayanand University
Rohtak, India

Divya Shree
Assistant Professor
Department of Computer Science (UIET)
Maharshi Dayanand University
Rohtak, India

Rashmi Sindhu (Student P.G)
Department of Computer Science (UIET)
MaharshiDayanand University
Rohtak. India

Abstract: Now days, data communication mainly depends upon digital data communication, the requirement that has highest priority is datasecurity, and this is because the data should reach to the intended user. So for providing data security many cryptography techniques areemployed, such as symmetric and asymmetric techniques [1]. In this review paper we will analyse cryptography and its different techniques. After analysing these techniques we will also compare them so that it becomes easy to judge which technique is better. The techniques that we analyse are RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography) [1].

Keywords: RSA, DSA, ECC, Cryptography.

INTRODUCTION

Use of Internet is becoming more popular all over the world. But if any unauthorized user gets access to a network, he can't only spy on us but can also mess up our lives. Concept of Network Security and Cryptography is used to protect network and data transmission over wireless network. A secure network system relies on layers of protection and has many other components like network monitoring and security software in addition to hardware and appliances. All these components work in coordination with each other so that the overall security of the network can be increased. Data security can be achieved by using a technique known as Cryptography. Thus we can say that it is the technique which is more appropriate and suitable for network security.
Neural Network provides high security support to the Cryptosystem. The combination of Neural Network and Cryptography can have great impact on network security. Neural Network has a structure which is in the form of weights and neuronal functions; this structure is difficult to break [2]. The content data will be used as input data for cryptography such that the data can't be read by attackers and made secure for the authorized user. Mutual learning, self-learning and stochastic behaviour of neural networks and other similar algorithms can be used for different aspects of cryptography. Security of a network consists of policies that are adapted by a network administrator to monitor and prevent unauthorized access, alteration, misuse and denial of a computer network and its resources [2]. Network security covers various computer networks, both public and private networks.
Cryptography is used for various objectives such as: -

1) Confidentiality: - According to confidentiality the information cannot be understood by anyone except for whom it was intended.
2) Integrity: - integrity means that the information can't be modified in storage or any transaction between sender and intended receiver.
3) Non-repudiation: - Thesender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
4) Authentication: Both sender and receiver have to confirm about each other's identity and should be clear about the destination of the information [2].

Cryptography algorithms can be divided into 2 type's i.e. Symmetric and Asymmetric key cryptography. In Symmetric key encryption, same key is used both for encrypt and decrypt data. Before transmission occurs,the key must be given to both sender and receiver. Key has an important role in encryption and decryption. If we use a weak key then it will be quite easy for an unauthorized user to access that data by decrypting that. The strength of symmetric key encryption depends upon the size of the key. Symmetric algorithms are further divided into two types i.e. block ciphers and stream ciphers.Block ciphers operates on data which is in groups or blocks, e.g. Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers operate on a single bit at a time, e.g. RC4is a stream cipheralgorithm.

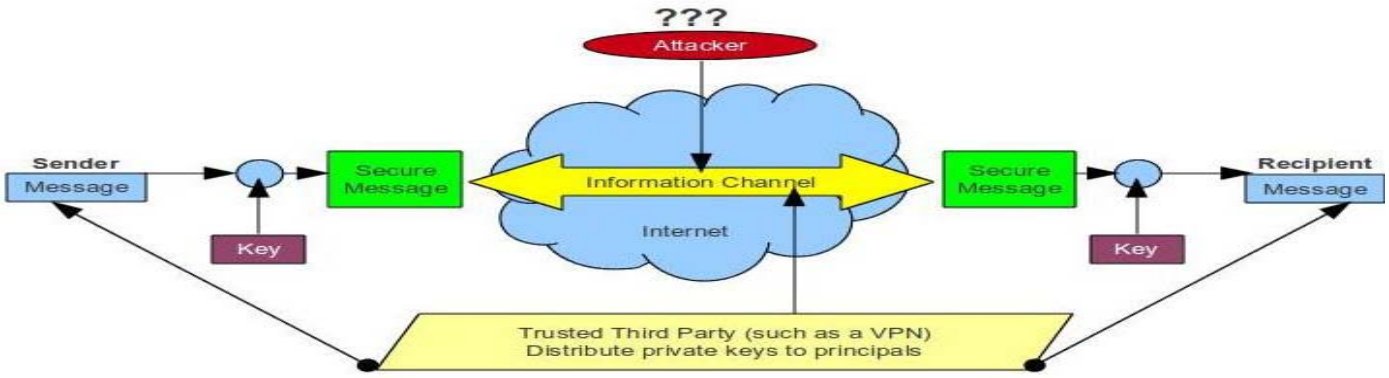


Figure 1: - Model for network security [2]

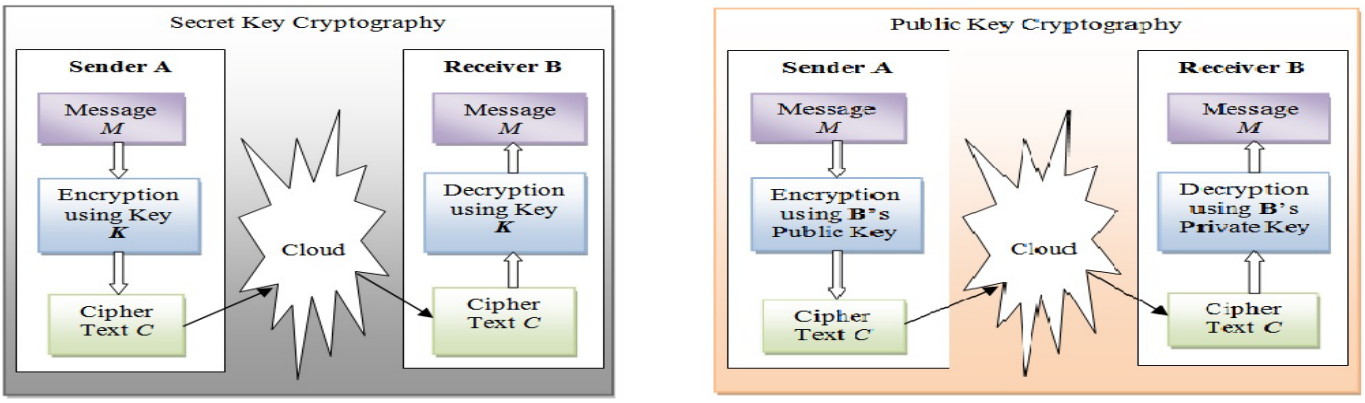
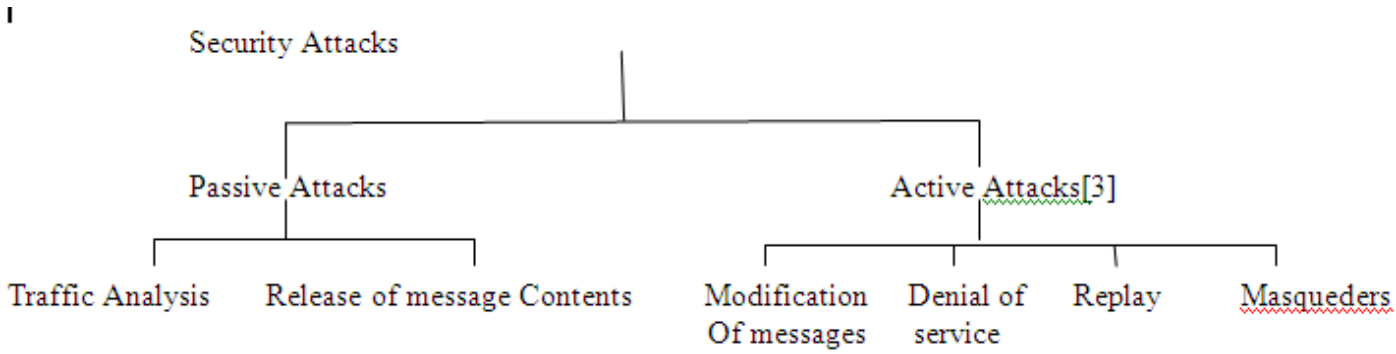


Figure 2: - Types of Cryptography [2]

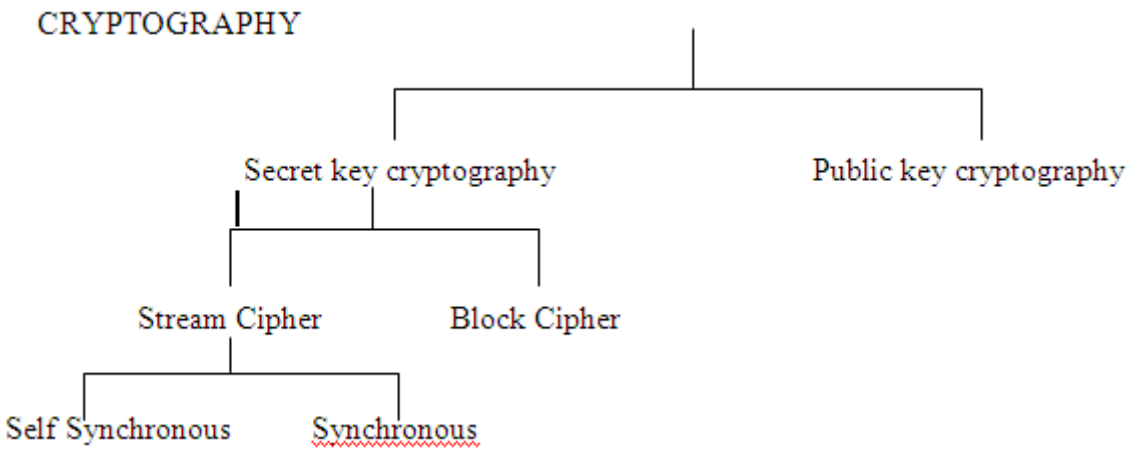
Security Attacks are those attacks that are made by some unauthorised user to threaten the security of network. Security attack can be classified as: -



LITRATURE REVIEW

Young-Chang Hou et Al [4] in 2015proposed a new scheme for encryption of images in which a secret image is encrypted into two meaningful images. Anyone who accesses that image can recognise the content of the cover image which is placed on the share image, but no one can have idea about the secret image. For the encryption purpose, some pixels from secret image and some pixels from cover image are taken to generate a new share image. In this paper they used different types of blocks for showing contrast between dark and light areas in order to show a cover image on the share image.

Pranab Garg et Al [5] in 2012 gives detailed explanation of cryptographic process. He divides cryptographic process as: -



He explains different algorithms for public key cryptography such as RSA algorithm, Hash algorithm, Secure Hash algorithm etc.

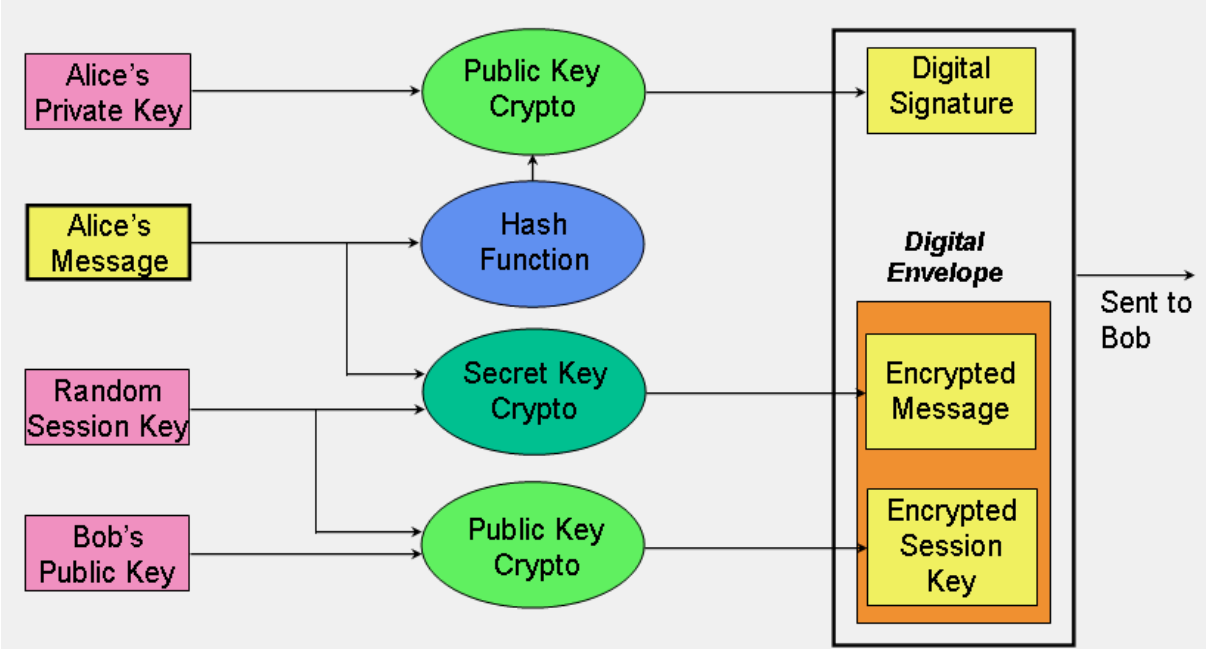


Figure 3: - Application of Cryptographic Techniques [6]

Nitin Jirwan et Al [6] analysed different techniques of cryptography: -

a) RSA: - RSA is a public key cryptography algorithm. RSA can be used in wireless sensor network because WSN is a insecure network and easily be attacked because of its broadcast nature of transmission medium. He explains the RSA algorithm in detail with its various steps.

b) Diffie-Helman algorithm: - This algorithm is used for exchanging cryptography keys between two users. Users does not have any knowledge about the keys used by the other user, they use a shared secret key over the communication channel.

He explained the whole algorithm into 5 steps: -

- Model specification
- Goals definition within model
- Assumption statements
- Protocol description
- Proof of goal achieving

Rajesh R Mane [1]in 2015 had a review on cryptography algorithms and briefly explained about SKC and PKC algorithms. He explained DES algorithm and state that there are 2 significant components that build up DES and they are triple-DES which use 56 keys for encryption and decryption, and second component is DESX in which key length is up to 120 bits. Also mentioned various SKC algorithms such as Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Rivest Ciphers (aka Ron's Code), Secure and Fast Encryption Routine (SAFER), GPRS (General Packet Radio Service) encryption, Blowfish etc. PKC algorithms are Diffie-Hellman, Digital Signature Algorithm (DSA),ElGamal, hash function etc. He also specified 6 types of attacks with Cyber Security Technologies and encryption tools.

ShyamNandan Kumar [7] in 2017 distributed security attacks into active and passive attacks and further classified them into modification of message, denial of service, replay, masquerade and traffic analysis, release of message contents respectively defines security services such as Data Integrity, Data Confidentiality, Authenticity, non-repudiation and access control.

Comparison of various algorithms of Cryptography

PERFORMANCE CRITERION	DES	AES	RSA	BLOWFISH	ECC	IDEA
Development	By IBM in 1970 but published in 1977	VicetRijman, Joan Deaman in 2001	In 1978 by Ron Rivest, Shamir, & Leonard Aldeman	In 1993 by Bruce Schneir	Victor Miller from IBM & Neil Koblitz in 1985	In 1991 Xuejia Lai and James
Key Length (Bits)	64 (56 used)	128, 192, 256	Length of key is dependent on no. of bits in the module	Variable key length 32-448	Smaller but effective key	128
Rounds	16	48	1	16	1	8
Block Size (Bits)	64	64	Variable block size	64	Stream size is variable	64
Attacks Found	Exclusive key search, linear cryptanalysis, differential analysis	Related key attack	Brute force attack, timing attack	No successful attack found against Blowfish	Doubling attack	Linear attack
level of Security	Adequate security	Adequate security	Good level of security	Highly secure	Highly secure	secure
Encryption Speed	Very slow	Very slow	Average	Very fast	Very fast [3], [7]	fast

CONCLUSION

In this paper we analysed different Cryptography algorithms, DES was the first algorithm which was introducedfor the purpose of Cryptography. ECC algorithm has smaller but effective key length. AES algorithm has maximum no. of rounds. BlowFish is the only algorithm against which no successful attack has been found. BlowFish and ECC algorithms are amongthe highly secure and faster encryption speed algorithms.

REFERENCES

[1]. Rajesh R Mane "A Review on Cryptography Algorithms, Attacks and Encryption Tools"International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 9, September 2015.

[2]. Mamta. Juneja and Parvinder S. Sandhu "A Review of Cryptography Techniques and Implementation of AES for Images" International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 4 (2013) ISSN 2320-401X; EISSN 2320-4028.

[3]. Vedprakash Sharma and Nabila sheikh, "Review Paper of Different Cryptography Algorithms for Video",IJARIIE-ISSN (O)-2395-4396Vol-2 Issue-3 2016.

[4]. Young-Chang Hou et Al"New Designs for Friendly Visual Cryptography Scheme"International Journal of Information and Electronics Engineering, Vol. 5, No. 1, January 2015.

[5]. Pranab Garg et Al"A Review Paper on Cryptography and Significance of Key Length"International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012.

[6]. Nitin Jirwan et Al "Review and Analysis of Cryptography Techniques" International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 1 ISSN 2229-5518.

[7]. ShyamNandankumar, "Review on network Security and Cryptography"International Transaction of Electrical And Computer Engineers System, 2015, Vol. 3, No. 1, 1-11.

[8]. Mukund R. Joshi et Al "Network Security with Cryptography" International Journal of Computer Science and Mobile Computing" IJCSMCVol. 4, Issue. 1, January 2015, pg.201 – 204.