[IDSTM: January 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

REVIEW ON NETWORK SECURITY AND CRYPTOGRAPHIC TECHNIQUES

Nupur Chugh, Ritu Kadyan, Abhinav Kanojia
Assistant Professor, Department of Computer Science & Engineering,
Scholar, Department of Computer Science & Engineering, Ganga Technical Campus, Soldha

ABSTRACT

Nowadays the applications like Internet and networks are growing very fast, thereby the importance and the value of the exchanged data over the internet or other media types are increasing. For secure communication the cryptography is essential, therefore we have various cryptography algorithms for securing the data over internet. This paper discuss the state of the art for a broad range of cryptographic algorithms that are used in networking applications. A comparison table is created for various cryptography algorithms used as per the requirement on different networks.

Keywords-. *Secret Key/ Symmetric Key Cryptography*.

Introduction

One of the classic techniques used for ensuring privacy of files and communication is Cryptography is the science of secret writing so that the meaning of a message can be hidden.For securing the data different types of cryptography techniques are used to achieve the goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography.

Secret Key/ Symmetric Key Cryptography

In this type of cryptography a single key is used for encryption and decryption of data. Symmetric key ciphers are implemented as either blockciphers or stream ciphers.The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are examples of Secret Key Cryptography.

Public Key/ Asymmetric Key Cryptography

Asymmetric Key Cryptography use two keys, one is private key and the other is public key for encrypting and decrypting messages. A message that is encrypted by using the public key can only be decrypted by applying the samealgorithm and using the matching private key. Likewise, a message that is encrypted by using the private key can only be decrypted by using the matching public key. RSA, Diffie Hellman and ECC are examples of public key Cryptography.

CRYPTOGRAPHY TECHNIQUES

DES(Data Encryption Standard)

DES (the Data Encryption Standard) is a symmetric block cipher developed by IBM.Goal of DES is to completely scramble the data and key so that every bit of cipher text depends on every bit of data and every bit of key. DES is widely used, despite claims that the key length is too short. Six different permutation operations are used both in key expansion part and cipher part. The DES weaknesses is recorded by many attacks and methods, which implies that it is an insecure block cipher.The following diagram shows the process of encryption and decryption using DES.

ISSN 2348 – 8034
Impact Factor- 4.022

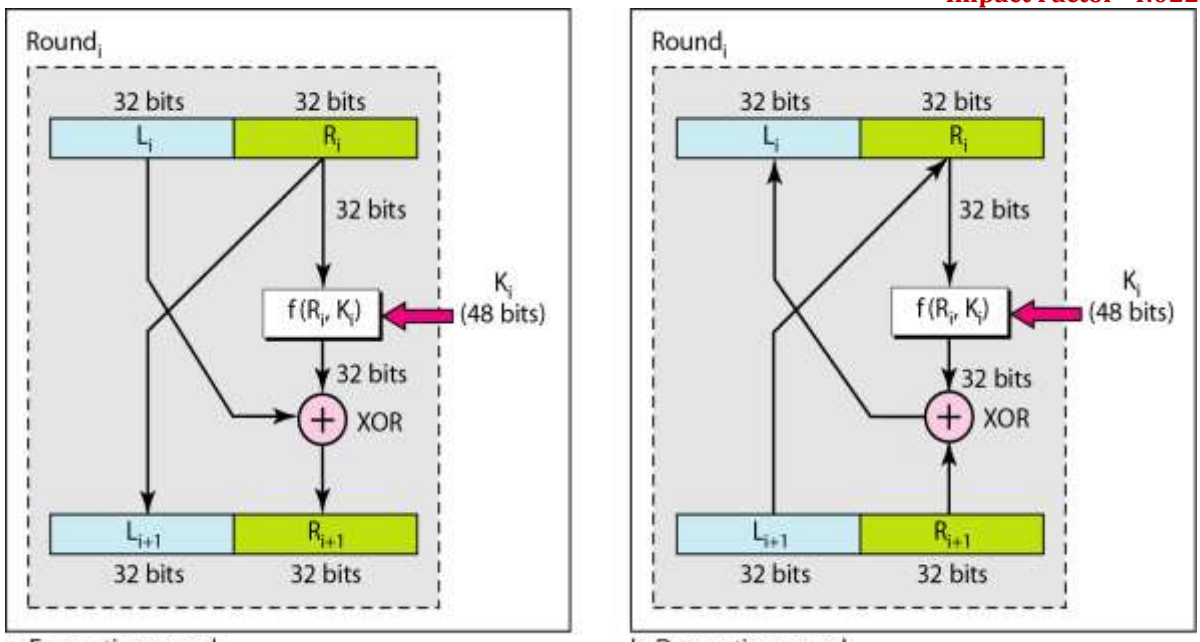

Fig1: Process of DES [3]

AES(Advanced Encryption Standard)

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).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. Unlike DES, the number of rounds in AES is variable and depends on the length of the key.

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

RSA(Rivest -Shamir–Adleman)

RSA standsfor Ron Rivest, Adi Shamir and Leonard Adleman, whofirst publicly described the algorithm in 1977.It was so successful that today *RSA*public key algorithm is themost widely used in theworld.

Using an encryption key (*e*,*n*), the algorithm is as follows:

1. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. N=p*q

ISSN 2348 – 8034
Impact Factor- 4.022

3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1))).

Deffie Hellman

Deffie Hellman is key agreement algorithm that uses exponential key. It allows two users to exchange a secret key. It is based on computing discrete logarithms of large numbers. The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel.

Steps in the algorithm:

1 Alice and Bob agree on a prime number p and a base g.
2 Alice chooses a secret number a, and sends Bob (g a mod p).
3 Bob chooses a secret number b, and sends Alice (g b mod p).
4 Alice computes ((g b mod p) a mod p).
5 Bob computes ((g a mod p) b mod p). Both Alice and Bob can use this number as their key.

Elliptical Curve Cryptography

This algorithm is mainly depend on the algebraicstructure of elliptic curves. The primary benefitpromised by ECC is a smaller key size, reducingstorage andtransmission requirements—i.e., that anelliptic curve group could provide the same level ofsecurity afforded by an RSA-based system with alarge modulus and correspondingly larger key—e.g., a 256bit. ECC has small key size,low memory usage as compared to RSA.Therefore it has attracted attention as asecurity solution for wireless networks.

CONCLUSION

Among these algorithms and concepts the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. ECC has the highest key size and is faster among all. In future we can use encryption techniques in such a way that it can consume less time, have high speed and uses minimum energy.

COMPARISON TABLE

Algorithm	Key Size	Features	Applications
DES	56 bits	It uses Brute force action	Smart Cards, Sim Cards and network devices like modems.
TripleDES	168 bits (112 effective)	Modification of DES, Adequate Security	Authentication
AES	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security	Secure File transfers
RSA	512-2048	Deterministic Encryption	For online credit card security, Payment gateways
DiffieHellman	1024-2048	It relies on discrete logarithm. It is quite fast	Security protocols SSL, SSH and IPsec

ECC	164-1024	Faster and efficient	Mobile communications
Hybrid	Variable	Combination of two or more algorithms	PGP and Wireless Sensor Networks

Table1: Comparison of different Cryptographic Techniques

REFRENCES

[1] Y. Maleh, A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 6, December 2013.

[2] R. Sakai, K. Ohgishi, and M. Kasahara, « Cryptosystems based on pairing », in Symposium on Cryptography and Information Security SCIS'00), Japan, 2000, p. 26–28.

[3] Data Communications and Networking, Fourth Edition by Behrouz A Forouzan.

[4] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, et D. E. Culler, « SPINS: security protocols for sensor networks », Wireless Network., vol. 8, no 5, p. 521–534, sept. 2002.

[5] Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research, Vol. 03, Issue-01, pp50-56.

[6] Bridget Dahill, KimayaSanzgiri, Brian Neil Levine, Elizabeth Royer, and Clay Shields. A Secure Routing Protocol for Ad hoc Networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02), November 2002.

[7] Don Coppersmith and Markus Jakobsson. Almost Optimal Hash Sequence Traversal. In Proceedings of the Sixth International Conference on Financial Cryptography (FC 2002), Lecture Notes in Computer Science. Springer, 2002.