Survey of Encryption and Decryption for Secure Communication

Shalini Gupta
ECE Deptt.
Rama University,Kanpur,India
sfairy.gupta@gmail.com

Saurabh Gupta
CSE Deptt
PSIT, Kanpur,India
saurabhdavvmtech@gmail.com

***Abstract*—The high growth in the networking technology leads a practice of interchanging of the digital images very frequently in present times,. The protection of multimedia data, sensitive information like credit cards, banking transactions and social security numbers is becoming most important. The protection of these confidential data from unauthorized access can be done by Cryptography, and it is the study of" Secret (crypto-) writing (-graphy) with many encryption and decryption techniques. The Process of Encryption and Decryption is performed by using Symmetric key cryptography and public key cryptography for Secure Communication. . In this paper, we studied that how the process of Encryption and Decryption is perform in case of Symmetric key and public key cryptography using AES and DES algorithms and modified RSA algorithm and some new recent technologies of encryption like Digital Signature Encryption.**

Keywords*— Symmetric key cryptography, Asymmetric key cryptography, Encryption, Decryption, RSA, AES, DES*

I. INTRODUCTION

Here we are discussing about security .Every user while communicating wants a secure network so that data communication should secure and no unauthorised can read their data. For providing secure data communication cryptography is used in wireless and wired network.

Cryptography converts to plain text into cipher text and cipher text into a plain text. At a sender side plain text is converted into a cipher text known as encryption and receiver side cipher text is converted into a plain text known as decryption. In its broadest sense cryptography addresses a number of practical problems:

a) Confidentiality: keeping messages secret;
b) Origin Authentication: verifying a message's source;
c) *Integrity*: assuring that a message has not been modified;
d) *Key management*: distributing the secret "keys" for cryptographic algorithms.

Following terms are used in cryptography:

- Plaintext: An original message is known as plaintext.
- Cipher text: Coded message is called cipher text.
- Encryption or Enciphering: the process from converting
- iv)Decryption or Deciphering: Restoring plain text from cipher text is called decryption or Deciphering.
- Deciphering Cryptography: The many schemes used for enciphering constitute the area of study known as cryptography.

II. TYPES OF CRYPTOGRAPHY

There are two main types of cryptography:
A) Symmetric Key Cryptography
B) Asymmetric Key Cryptography

A. Symmetric Key Cryptography

Symmetric-key cryptography[1] refers to encryption methods in which both the sender and receiver share the same key. In symmetric-key cryptography, the same key is used by both parties. 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 the data. The Symmetric key cryptography is also known as Private key cryptography.

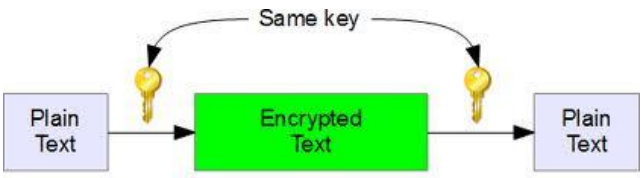

Fig1. Symmetric Key Cryptography

Symmetric key ciphers are implemented as either block cipher or stream cipher. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The Data Encryption

Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs.

B. Asymmetric Key Cryptography

Asymmetric-key cryptography, where different keys are used for encryption and decryption. In asymmetric or public-key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public.

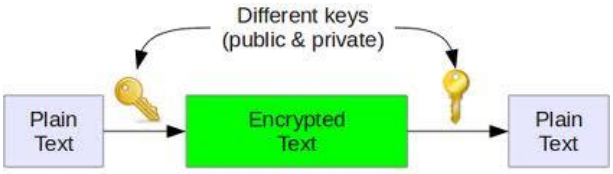

Fig2. Asymmetric Key Cryptography

Some commonly used asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), DSA (Digital Signature Algorithm). All these technique are discussed below in this paper.

TABLE I. ENCRYPTION ALGORITHM CLASSES AND THEIR PROPERTIES

Encryption algorithm classes and their properties.					
Class	**C.**	**O.A.**	**I.**	**K.M.**	**Prior**
Secret-key cryptosystems	Yes	No	No	Yes	Yes
Public-key cryptosystems	Yes	No	No	Yes	No
Digital signature schemes	No	Yes	Yes	No	No
Key agreement algorithms	Yes	Optional	No	Yes	No
Cryptographic hash Function	No	No	Yes	No	No
Authentication codes	No	Yes	Yes	No	Yes
C indicates Confidentiality; OA: Origin Authentication; I: integrity; KM: Key Management. Prior requires that parties first agree on a secret key.					

III. ANALYSES OF DIFFERENT TECHNIQUES

In this review paper above described techniques of cryptography are analysed based on different research paper in respective journals

A. RSA (Rivest Shamir and Adleman) Algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message.

The RSA algorithm involves three steps:

- key generation,
- encryption and
- decryption

a) Key Generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated in the following way:

- Choose two distinct prime numbers p and q.
- For security purposes, the integers p and q should be chosen at random
- Compute n = pq.
- n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and φ(n) are co-prime.
- e is released as the public key exponent.
- Determine d as $d \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)).

This is more clearly stated as solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$ d is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

b) Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

He then computes the cipher text c corresponding to

$$c = m^e \pmod{n} \quad (1)$$

BOB THEN TRANSMITS C TO ALICE.

c) Decryption

Alice can recover *m* from *c* by using her private key exponent *d* via computing

$$m = c^d \pmod{n} \quad (2)$$

Given m, she can recover the original message M by reversing the padding scheme.

B. *AES(Advanced Encryption Standards) Algorithm*

AES [6] is a symmetric cipher that processes data in 128-bit blocks. It supports key sizes of 128, 192, and 256 bits and consists of 10, 12, or 14 iteration rounds, respectively. Each round mixes the data with a round key, which is generated from the encryption key.

The encryption round operations are presented in Fig. 1. The cipher maintains an internal, 4-by-4 matrix of bytes, called State, on which the operations are performed. Initially State is filled with the input data block and XOR-ed with the encryption key. Regular rounds consist of operations called Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. The last round bypasses Mix Columns. Decryption requires inverting these operations.

Sub Bytes is an invertible, nonlinear transformation. It uses 16 identical 256-byte substitution tables (S-box) for independently mapping each byte of State into another byte. S-box entries are generated by computing multiplicative inverses in Galois Field GF(28) and applying an affine transformation. Sub Bytes can be implemented either by computing the substitution or using table lookups. Shift Rows is a cyclic left shift of the second, third, and fourth row of State by one, two, and three bytes, respectively. Mix Columns performs a modular polynomial multiplication in GF(28) on each column. Instead of computing separately, Sub Bytes and Mix Columns can also be combined into large Look-Up-Tables (LUT), called T-boxes. During each round, Add Round Key performs XOR with State and the round key. Round key generation (key expansion) includes S-box substitutions, word rotations, and XOR operations performed on the encryption key**.**

c. Digital Signature Algorithm

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender . Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type.

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. "Hash function" is used in this method and it generates dynamic and smaller size of bits which depends on each byte of data. The main function which is used for hashing is bitwise or and multiply functions.

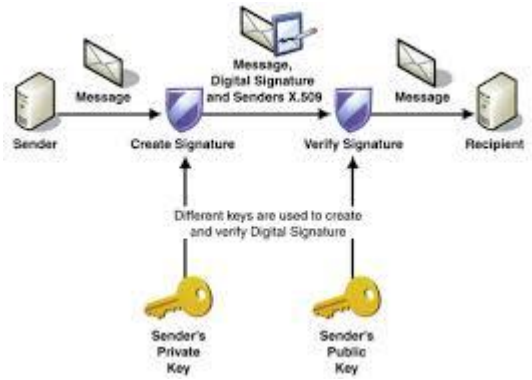

Fig.3.Digiatal signature

IV. **CONCLUSION**

In this paper the existing encryption techniques are studied and analyzed. As with the advancement in the communication technologies there is a need of security and there are many authors that have proposed many ways of providing security but most of them provide the secure way of key distribution. As there is other problem that the key that is being distributed if get to know by the third party then that will lead to the leak of the information. So I am trying in my proposed work to provide the best way of key generation that will provide the security without any overhead of key distribution. .

TABLE III ANALYTICAL TABLE

S. No.	Algorithm Name	Cryptography Technique Analysis
1.	(RSA) algorithm	• RSA can be used in Mobile nodes because they are vulnerable to many attacks due to their broadcast nature • RSA is not suitable for WSN because of high time complexity and consumption demand
2.	Digital Signature Algorithm	• Used by the receiver to verify that the message received is unaltered; a digital signature is used for performing this task • Hash function is used to generate dynamic and smaller size of bits which depends on each byte of data

REFERENCES

[1] N khanna, j nath , j james, s chakraborty, a chakrabarti, a nath, " new symmetric key cryptographic algorithm using combined bit manipulation and msa encryption algorithm: njjsaa symmetric key algorithm", 2011 international conference on communication systems and network technologies, pp 125-130, ieee 2011.

[2] Dutta, Chayan," A New Encryption-Decryption Scheme that Solves Key Management Problem in Remote Sensing Satellite", Emerging Trends in Engineering and Technology, ICETET '08, pp. 1261 – 1266, IEEE 2008.

[3] William Stallings (2004), "Network Security Essentials (Applications and Standards)", Pearson Education.

[4] W.Diffie, "The First Ten Years of Public-Key Cryptography," Proc. IEEE, 1988, pp. 560-577

[5] P. Fahn, Answers to Frequently Asked Questions About Today's Cryptography, Version 2.0, RSA Laboratories Redwood City, Calif., Sept. 1993.

[6] ISOAEC JTC 1ISC6, N6285: Draft Transport Layer Security Protocol, ISO/IEC, Nov. 1990.

[7] Accredited Standards Committee X9, Working Draft: American

[8] National Standard X9.30- 1993: Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 2: The Secure Hash Algorithm (SHA), Am. Bankers Assoc., 1993.

[9] B. Kaliski, RFC 1319: The MD2 Message-Digest Algorithm, RSA Data Security, Inc., Apr. 1992.

[10] R.L. Rivest, RFC 1321: The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science, Cambridge, Mass., and RSA Data Security, Inc., Apr. 1992.

[11] Accredited Standards Committee X9, Working Draft: American National Standard X9.3 1 - 1992: Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Part 2: The MDC-2 Hash Algorithm, Am. Bankers Assoc., June 4, 1993.

[12] FIPS Publication 1 13: Computer Data Authentication, NIST, May 30, 1985.

[13] AccreditedStandardsCommitteeX9,AmericanNationalStandard X9.9: Financial Institution Message Authentication, ANSI, 1982.

[14] Australian Standard 2805.4 1985: Electronics Funds Transfer-Requirements for Interfaces: Part 4-Message Authentication, Standards Assoc. of Australia, 1985.

[15] J. Linn, RFC 1421: Privacy Enhancement for Internet Electronic Mail: Partk Mewge Enciphermentand Authentication, Internet Activities Board, Feb. 1993.

[16] Recommendation X.509: The Directory-Authentication

[17] Framework, CCITT, 1988.