SHIV SHAKTI

International Journal in Multidisciplinary and Academic Research (SSIJMAR)

Vol. 2, No. 1, January-February-2013(ISSN 2278 – 5973)

ENCRYPTION USING DIFFERENT TECHNIQUES: A REVIEW

Dimple*

ABSTRACT

In present times, the high growth in the networking technology leads a practice of interchanging of the digital images very frequently. The protection of multimedia data, sensitive information like credit cards, banking transactions and social security numbers is becoming very important. The protection of these confidential data from unauthorized access can be done with many encryption techniques. So for providing data security many cryptography techniques are employed, such as symmetric and asymmetric techniques. In this review paper different asymmetric cryptography techniques, such as RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm) are analyzed. Also in this paper, a survey on existing work which is used different techniques for image encryption is done and a general introduction about cryptography is also given.

KEYWORDS:- Asymmetric key cryptography, Decryption, Encryption, RSA,DSA, Symmetric key cryptography, Diffie-Hellman Algorithm

*CSE Dept., U.I.E.T., Maharshi Dayanand University Rohtak

1. INTRODUCTION

Every user while communicating wants a secure network so that data communication should secure and no intruder can read their data. For providing secure data communication cryptography is used in wireless and wired network, where cryptography converts to plain text into cipher text and cipher text into a plain text[1]. 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[3].

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Following terms are used in cryptography:

Plaintext[2]: An original message is known as plaintext.

Cipher text [2]: Coded message is called cipher text.

Encryption or Enciphering [2]: the process from converting plain text to cipher text is called Encryption or Enciphering.

Decryption or Deciphering [2]: Restoring plain text from cipher text is called decryption or Deciphering.

Cryptography [2]: The many schemes used for enciphering constitute the area of study known as cryptography.

2. Types of Cryptography:

There are two main types of cryptography:

- Secret key cryptography or symmetric key cryptography
- Public key cryptography or asymmetric key cryptography

2.1 Symmetric-key cryptography Symmetric-key cryptography 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. This was the only kind of encryption publicly known until June 1976.

Figure 1: Secret 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. Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material.

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret.

Public-key cryptography

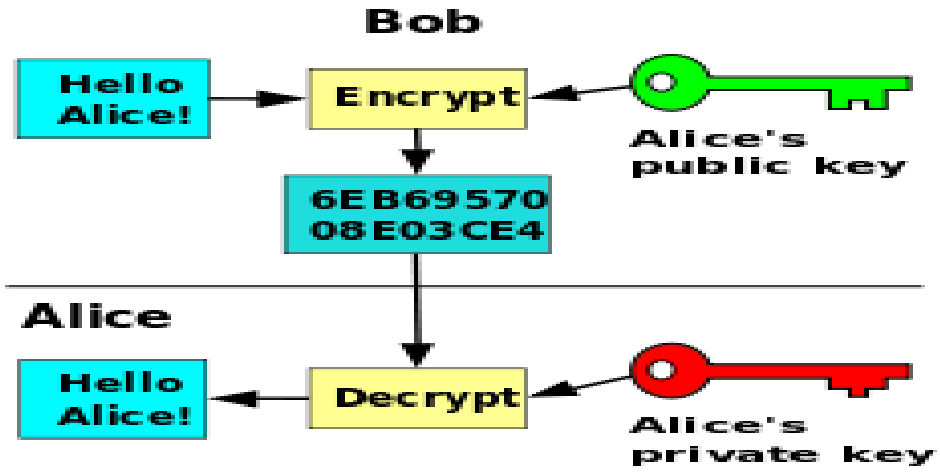

Figure2 : Public Cryptography

Public-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.

Figure3: Block Diagram of Public Cryptography with Different Key.

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

3. ANALYSES OF DIFFERENT TECHNIQUES

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

3.1 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 [5]. 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 [7]. 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.

3.1.1 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 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 $\varphi(n)$ are coprime.

e is released as the public key exponent.

Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

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 $\varphi(n)$ must also be kept secret because they can be used to calculate d.

3.1.2. 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 ciphertext c corresponding to

$$c \equiv m^e \pmod{n}.$$

Bob then transmits c to Alice.

3.1.3. Decryption

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

$$m \equiv c^d \pmod{n}.$$

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

3.2 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)[11]. 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 are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a nonsecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender [12]. 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. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, or a message sent via some other cryptographic protocol.

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 [13].

3.3 Diffie–Hellman Algorithm

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys [8]. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. 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 [9]. This key can then be used to encrypt subsequent communications using a symmetric key cipher.The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.

4 ANALYTICAL TABLE[4]

S. No.	Cryptography Technique ANALYSIS
1.Rivest Shamir and Adleman (RSA) algorithm	• RSA can be used in Mobile nodes; because they are vulnerable to many attacks due to their broadcast nature [5] • RSA is not suitable for WSN because of high time complexity and consumption demand [6]
2. Diffie-Hellman Algorithm	• Here keys are exchanged between two users; unknown to each other [8]. • A proposed for two goals: authenticated key agreement and authenticated key agreement with key confirmation in the asymmetric (public-key) setting [9]. • It can be used in Internet and nearly in every encryption technology used in the Internet today, including SSL, SSH [10]
3.Digital Signature Algorithm	• Used by the receiver to verify that the message received is unaltered; a digital signature is used for performing this task [11]. • Hash function is used to generate dynamic and smaller size of bits which depends on each byte of data [12].

	• Result of Hash function depends on size of data [13].

CONCLUSION

In this paper the existing encryption techniques are studied and analyzed. It is analyzed that in Diffie-Hellman cryptography algorithm secret keys are exchanged between two users. Whereas a digital signature is used by receiver in DSA to confirm that the signal received is unaltered. It is also concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

6. REFERENCES

[1] Komal D Patel, Sonal Belani,"Image Encryption Using Different Technique:A Review

[2]William stallings, ―Cryptography and Network Security:Principles & Practices‖, second edition.

[3]Swati Paliwal Ravindra Gupta,"_A Review of Some Popular Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013 ISSN: 2277 128X

[4]Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay,"_Review and Analysis of Cryptography Techniques",International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 ISSN 2229-5518

[5]_A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks," ACM, Vol. 47, No.653.2004.

[6]_F. Amin, A. H. Jahangir and H. Rasifard, "Analysis Of Publickey Cryptography For Wireless Sensor Networks Security," In Proceedings of World Academy of Science, Engineering and Technology, ISSN 1 307-6884, 2008.

[7]_Chandra M. Kota et al.,"Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002

[8] Wikipedia,"http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange," Dated: 13-dec-2012 at 10:33.

[9]. Simon Blake Wilson et al., “Key agreement protocols and their security analysis,” 9-sep-1997.

[10]. David A. Carts, “A Review of the Diffie- Hellman Algorithm and its Use in Secure Internet Protocols,” SANS institute, 5-nov-2001.

[11]. Vocal, “http://www.vocal.com/cryptography/dsadigital- signature-algorithm/,” Dated: 13-dec-2012 at 13:18.

[12]. Erfaneh Noorouzil et al, “A New Digital Signature Algorithm”, International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.

[13]. William-Stallings, http://williamstallings.com/Extras/Security Notes/lectures/authent.html, Dated: 13-dec-2012 at 14:05.