*Asian J. of Adv. Basic Sci.: 2(3), 98-102*
*ISSN (Online): 2347 - 4114*
*www.ajabs.org*

# Study on cryptographic techniques in computer network security

**Jyoti Attri, Aarti Devi, Ankush Sharma & Pratibha Sharma**

*Deptt. Of CSE, Career Point University, Hamirpur (H.P.) 176041*
*Email ID: ankushasp@gmail.com*

**ABSTRACT: Cryptography is the most popular approach for information security. Network security is most vital component in information security as it refers to all hardware and software function, characteristics, features, operational procedures, accountability, access control, and administrative and management policy. A number of cryptographic algorithms were developed in order to improve the information security. In this research study paper compares the cryptographic technique son the bases of their speed block size describes the necessary, newly developed, principal concepts for several cryptographic techniques with their merits, demerits used to secure the information.**

**Keywords:** Information Security, Cryptography, Symmetric key, Asymmetric key, Key size, block size.

## INTRODUCTION

Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security[1]. Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control and so forth[2]. In technical terms, the process of encoding plaintext message into cipher text messages is called as Encryption. Diagram 1.1a) illustrates the idea. The reverse process of transforming cipher text message back to plaintext message is called as Decryption. Diagram 1.1 b) illustrates the idea.[3]

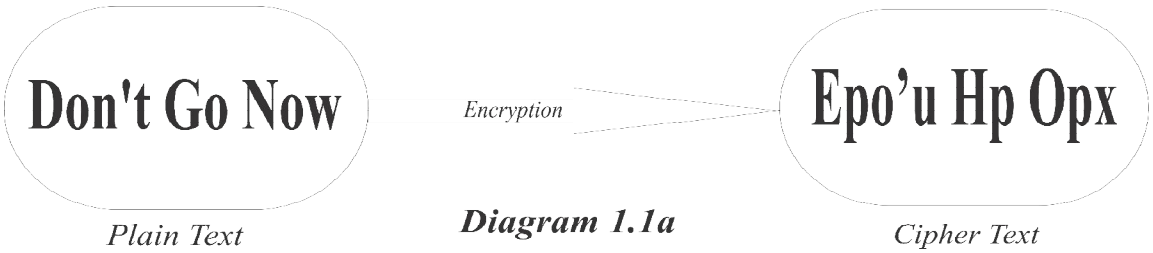



***Diagram 1.1a***

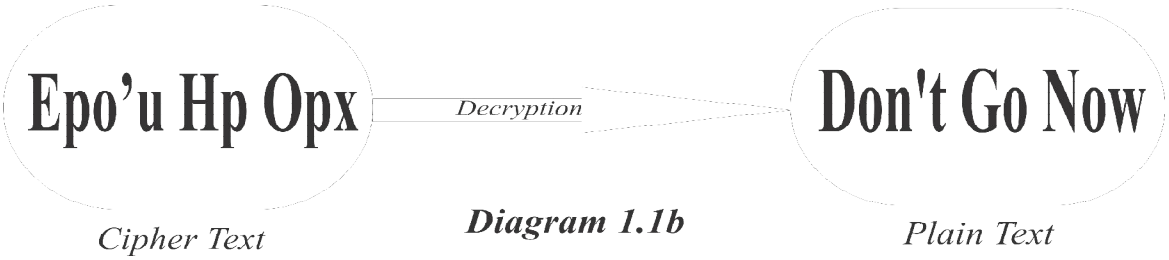



***Diagram 1.1b***

**BASIC TERMS USED IN CRYPTOGRAPHY:**

**Plain Text:** The original message that the person wishes to communicate with the other is defined as Plain the original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text.

**Cipher Text:** The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message.

**Key:** A specific string of data that is used to encrypt and decrypt messages, documents or other types of electronic data, Keys have varying levels of strength. The specific way a key is used depends on whether it's used with asymmetric or symmetric cryptography.

**Encryption:** A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. Encryption takes place at the sender side.

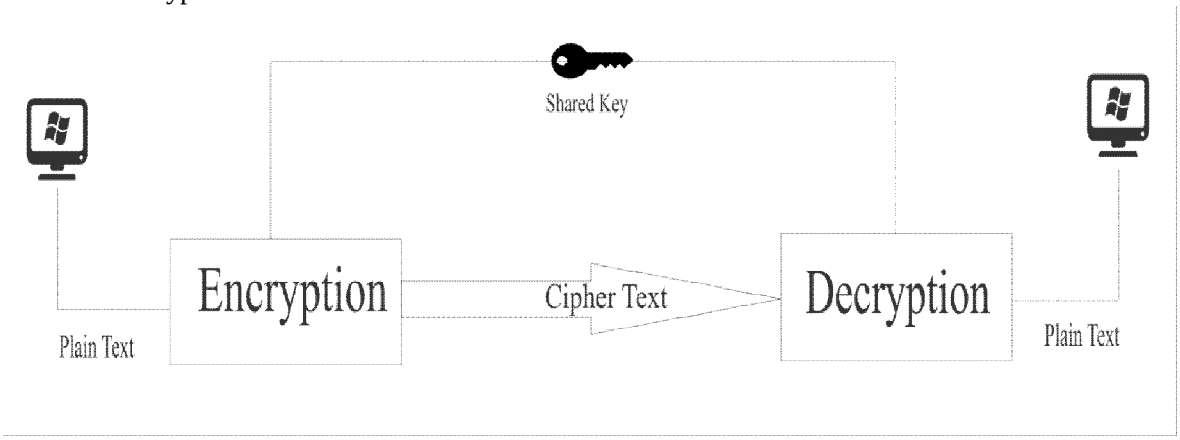
**Decryption:** A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message[4].

**Alice, Bob, and Eve:** In cryptography, it is customary to use three characters in an information exchange scenario; we use Alice, Bob, and Eve. Alice is the person who needs to send secure data. Bob is the recipient of the data. Eve is the person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending his/her own disguised messages. These three names represent computers or processes that actually send or receive data, or intercept or change data[5].

**CATEGORIES OF CRYPTOGRAPHY:**

- Symmetric key (also called secret-key) cryptography algorithms
- Asymmetric key (also called public-key) cryptography algorithms.

**Symmetric Key cryptography:** Symmetric key cryptography sometimes also called as secret key cryptography or private key cryptography. In symmetric key cryptography, single key is used for encryption and decryption process i.e. using same key data can be encrypted and decrypted.[6]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 as shown:




Also, in symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared[5].

**Advantages of Symmetric Key Cryptography:**

Simple: This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt or decrypt messages.

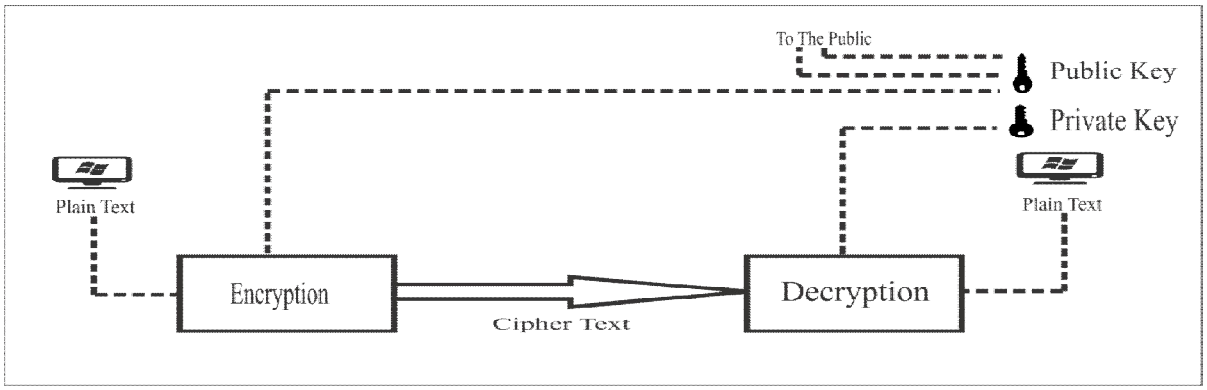
Fast: Symmetric key encryption is much faster than asymmetric key encryption.
Uses less computer resources: Single key encryption does not require a lot of computer resources when compared to public key encryption.
Prevents widespread message security compromise: A different secret key is used for communication with every different party. If a key is compromised only the messages between a particular pair of sender and receiver are affected[7].

**Disadvantages of Symmetric Key Cryptography:**
Need for secure channel for secret key exchange: Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.
Too many keys: A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys[7].
Symmetric Key Algorithms:
DES (Data Encryption Standard): DES is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1[4].
Triple-DES (3-DES): 3-DES is an enhancement of DES; it is 64 bit block size with192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods[4].
AES (Advanced Encryption Standard): AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in10, 12 and 14 rounds depending on the key size[16]. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications[4].
RC4 (Rivest Cipher): RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. It takes in keys of random lengths and this is known as a producer of pseudo arbitrary numbers. The output is then XORed together with the stream of data in order to generate a newly-encrypted data[4].

**Difference between symmetric algorithms:**

| S.No. | ALGO | KEY SIZE | BLOCK SIZE | SPEED | SECURITY | ROUNDS |
|---|---|---|---|---|---|---|
| **1** | **DES** | 56 bits | 64 bits | Slow | Insecure | 16 |
| **2** | **3DES** | 112/168 bits | 64 bits | Very Slow | Moderately secure | 48 DES-equivalent rounds |
| **3** | **AES** | 128, 192 or 256 bits | 128 bits | Fast | Secure | 10, 12 or 14 (depending on key size) |
| **4** | **RC4** | 256 bytes | 40 bits | Very Fast | Moderately secure | 256 |

**Asymmetric Key cryptography:** In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. Imagine Alice wants to send a message to Bob. Alice uses the public key to encrypt the message. When the message is received by Bob, the private key is used to decrypt the message.




In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public; the private key is available only to an individual[5]. Asymmetric key encryption or public key encryption is used to solve the problem of key distribution[8].

**Advantages of Asymmetric Key Cryptography:**

Convenience: It solves the problem of distributing the key for encryption. Every one publishes their public keys and private keys are kept secret.

Provides for messages authentication: Public key encryption allows the use of digital signature which enables the receipt of a message to verify that the messages truly from a particular sender.

Detection of tampering: The use of digital signature in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message can't be modified without in validating the signature.

Provide for Non-repudiation: Digitally signing a message is akin to physically signing a document. It is an acknowledgement of message and thus, the sender can't deny it[7].

**Disadvantages of Asymmetric Key Cryptography:**

Public keys should be authenticated: - No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.

Slow: - Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.

A widespread security compromise is possible: - If an attacker determines a person's private key his/her entire messages can be read.

Loss of private key may be irreparable: -The loss of a private key means that all received messages can't be decrypted[7].

**Asymmetric Key Algorithms:**

- **RSA:** Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm. It can be used to send an encrypted message without a separate exchange of secret keys. It can also be used to sign a message.RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n.[8] In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA computation occurs with integers modulo n = p * q, for two large secret primes p, q. To encrypt a message m, it is exponentiated with a small public exponent e. For decryption, the recipient of the cipher text c = me (mod n) computes the multiplicative reverse d = e-1 (mod (p-1)*(q-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n). The key size should be greater than 1024 bits for a reasonable level of security.
- **Diffie-Hellman Algorithm (DHA):** 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. The Diffie- Hellman protocol is generally considered to be secure when an appropriate mathematical group is used[4].

**Difference between asymmetric algorithms:**

| S.NO | ALGO | KEY SIZE | SPEED | SECURITY | Periodicity |
|---|---|---|---|---|---|
| **1** | **RSA** | 1024 bits and above | Fast | Secure | --- |
| **2** | **DHA** | 1024 bits and above | Very Fast | Very Secure | --- |

## CONCLUSION

Asymmetric encryption techniques are much slower than Symmetric techniques, becausethey require more computational processing power. In the asymmetric techniques rounds and block size notpresent. Symmetric key cryptography is better than asymmetric.

## REFERENCES


1. Kaushik Sumedha& Singhal Ankur" Network Security Using Cryptographic Techniques" Volume 2, Issue 12, December 2012, IJARCSSE.
2. Chandrasekhar Suman, Akash H.P. ,Adarsh. K, Sasi Mrs.Smitha "A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem" Volume 11, Issue 2 (May. - Jun. 2013), IOSR-JCE.
3. Kaur Kulwinder "Performance Evaluation of Ciphers Using CRYPTOOL 2.0" Volume 3. No. 1, AUG, 2012, IJCT.
4. Acharya Kritika, Sajwan Manisha & Bhargava Sanjay "Analysis of Cryptographic Algorithms for Network Security" Volume 3– Issue 2, 130 - 135, 2014,IJCATR.
5. Data Communication and Networking by "Behrouz A. Forouzan".
6. Rajput Yashpalsingh & Gulve A. K. "An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher"Volume 83 – No 13, December 2013,International Journal of Computer Applications (0975 – 8887).
7. http://m.voices.yahoo.com/comparing-symmetric-asymmetric-key-encryption-6329400.html
8. Kumar Yogesh, Munjal Rajiv, Sharma Harsh "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" Vol. 11, Issue 03, Oct 2011, IJCSMS.
9. http://en.m.wikipedia.org/wiki/Cryptographic_hash_function
10. Thakur Jawahar & Kumar Nagesh"DES,AES AND BLOWFISH: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" Volume 1, Issue 2, December 2011, International Journal of Emerging Technology and Advanced Engineering.