ENCRYPTION TECHNIQUES

Deepak Verma, Hardik Bhardwaj
Student, Department Of Information Technology
Dronacharya College Of Engineering, Gurgaon-123506, India

***Abstract*- In today scenario, the networking technology is leading a practice of interchanging of digital messages very frequently. In order to protect the data or sensitive information like credit cards, banking transactions, etc. from unauthorized access can be done with different encryption techniques. In this paper, the main focus is on the different kinds of encryption techniques that are exist and an equivalent study of all the techniques is being indulged as an information survey. This paper aims at the comprehensive tentative study of implementations of different available encryption techniques and emerges focus on image as well as information encryption techniques. The study of these techniques enhances the execution parameters used in encryption processes and analyzing on their security concern.**

I. INTRODUCTION

Each client while conveying needs a protected system so that information correspondence ought to secure and no interloper can read their information. For giving secure information correspondence cryptography is utilized as a part of remote and wired system, where cryptography believers to plain content into figure content and figure content into a plain text. At a sender side plain content is changed over into a figure content known as encryption and recipient side figure content is changed over into a plain content known as decryption.

Cryptography is the practice and investigation of methods for secure correspondence in the vicinity of outsiders. All the more for the most part, it is about developing and dissecting conventions that are connected to different viewpoints in data security, for example, information privacy, information honesty, validation, and non-denial. Applications of cryptography incorporate ATM cards, machine passwords, and electronic business. Emulating terms are utilized within cryptography: Plaintext: A unique message is known as plaintext.

Figure content : Coded message is called figure content. Encryption or Enciphering : the procedure from changing over plain content to figure content is called Encryption or Enciphering. Decoding or Deciphering : Restoring plain content from figure content is called unscrambling or Unraveling. Cryptography : The numerous plans utilized for enciphering constitute the territory of study known as cryptography.

II. TYPES OF CRYPTOGRAPHY

There are two main types of cryptography:

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

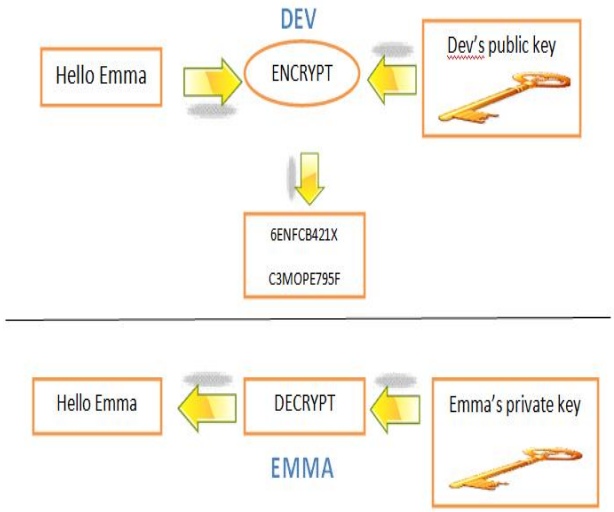
Symmetric-key cryptography :-

Symmetric-key cryptography alludes to encryption strategies in which both the sender and beneficiary have the same key. In symmetric-key cryptography, the same key is utilized by both gatherings. The sender utilizes this key and an encryption calculation to scramble information; the collector utilizes the same key and the relating unscrambling calculation to unscramble the information. This was the main sort of encryption freely known until June 1976 symmetric key figures are actualized as either piece figure or stream figure. A square figure enciphers include in pieces of plaintext rather than individual characters, the information structure utilized by a stream figure.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are square figure outlines. Stream figures, as opposed to the "piece" sort, make a self-assertively long stream of key material, which is joined with the plaintext bit-by-bit or character-by-character. In a stream figure, the yield stream is made focused around a concealed inward state which changes as the figure works. That inward state is at first situated up utilizing the mystery key material.

A huge inconvenience of symmetric figures is the key administration important to utilize them safely. Every different pair of conveying gatherings must, preferably,

impart an alternate key, and maybe every ciphertext traded too. The quantity of keys obliged increments as the square of the quantity of system parts, which rapidly obliges complex key administration plans to keep all of them straight and mystery. Figure below depicts symmetric key cryptography:



Public-key cryptography :-

Open key cryptography,where distinctive keys are utilized for encryption and decoding. In lopsided or open key cryptography, there are two keys: a private key and an open key are utilized. The private key is kept by the collector and open key is declared to the public.some usually utilized awry cryptography systems are RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm). All these system are examined beneath in this paper.

Public Key Cryptography

III. ANALYSES OF DIFFERENT TECHNIQUES

- **RSA Algorithm**

RSA is a calculation for open key cryptography that is focused around the assumed trouble of figuring extensive numbers, the considering issue. RSA remains for Ron Rivest, Adi Shamir and Leonard Adleman, who first freely portrayed the calculation in 1977.

A client of RSA makes and afterward distributes the result of two extensive prime numbers, alongside an assistant worth, as their open key. The prime variables must be kept mystery. Anybody can utilize the general population key to encode a message.

The RSA algorithm involves three steps:-

- key generation,
- encryption and
- decryption.

Key generation :-

RSA includes an open key and a private key. General society key can be known by everybody and is utilized for encoding messages. Messages encoded with the general population key must be unscrambled in a sensible measure of time utilizing the private key. The keys for the RSA calculation are created the accompanying way:

Pick two different prime numbers p and q.

For security purposes, the numbers p and q ought to be picked at irregular. Register n = pq. n is utilized as the modulus for both the general population and private keys. Its length, normally communicated in bits, is the key length.

Register $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient capacity.

Pick a whole number e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and φ(n) are coprime.

e is discharged as the general population key type.

Focus d as $d - 1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative backwards of e (modulo φ(n)).

This is all the more plainly expressed as fathom for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$

d is kept as the private key example.

By development, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. General society key comprises of the modulus n and people in general (or encryption) example e. The private key comprises of the modulus n and the private (or decoding) example d, which must be kept mystery. p, q, and φ(n) should likewise be kept mystery in light of the fact that they can be used to calculate d.

Encryption:-

Emma transmits her open key (n, e) to Dev and keeps the private key mystery. Dev then wishes to send message M to Emma.

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

He then processes the ciphertext c relating to weave then transmits c to Emma.

Decryption:-

Emma 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.

- **Digital Signature Algorithm**

An advanced mark is a numerical plan for exhibiting the validness of a computerized message or record. A legitimate computerized mark gives a beneficiary motivation to accept that the message was made by a known sender, such that the sender can't deny having sent the message (validation and non-renouncement) and that the message was not modified in travel (integrity). Computerized marks are generally utilized for programming conveyance, monetary transactions, and in different situations where it is paramount to discover fabrication or tampering.digital marks are frequently used to actualize electronic marks, a more extensive term that alludes to any electronic information that conveys the aim of a mark, however not all electronic marks use computerized marks Advanced marks are regularly used to actualize electronic marks, a more extensive term that alludes to any electronic information that conveys the expectation of a mark, however not all electronic marks utilization computerized marks. 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 fundamental properties are needed. To start with, a mark created from a settled message and altered private key ought to check the validness of that message by utilizing the comparing open key.

Besides, it ought to be computationally infeasible to produce a legitimate signature for a gathering without realizing that party's private key. "Hash capacity" is utilized as a part of this technique and it creates dynamic and littler size of bits which relies on upon every byte of information. The primary capacity which is utilized for hashing is bitwise or and duplicate capacities.

- **Diffie–Hellman Algorithm:-**

Diffie–hellman key trade is a particular strategy for trading cryptographic keys. It is one of the most punctual pragmatic illustrations of key trade actualized inside the field of cryptography. The Diffie–hellman key trade strategy permits two gatherings that have no earlier information of one another to mutually make an imparted mystery key over an unreliable correspondences channel. This key can then be utilized to scramble resulting correspondences utilizing a symmetric key cipher.the system was emulated in the blink of an eye thereafter by RSA, an execution of open key cryptography utilizing unbalanced calculation.

IV. CONCLUSION

In this paper the current encryption procedures are considered and examined. It is broke down that in Diffie-Hellman cryptography calculation mystery keys are traded between two clients. Though a computerized mark is utilized by recipient as a part of DSA to affirm that the sign got is unaltered. It is likewise inferred that all the strategies are valuable for ongoing encryption. Every method is exceptional in its own particular way, which may be suitable for diverse applications. Ordinary new encryption method is developing consequently quick and secure customary encryption strategies will dependably work out with high rate of security.

ACKNOWLEDGMENT

The authoress sincerely finds it his duty to acknowledge his parents and rest of the family members for supporting him in every single task performed by him while doing this piece of work. It was only due to their generosity and guidance that completion of this work could be accomplished on time and in a systematic order.

REFRENCES

[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 CryptographyTechniques", International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 ISSN 2229-5518

[5]. Simon Blake Wilson et al., "Key agreement protocols and their security analysis," 9-sep-1997.
[6]. David A. Carts, "A Review of the Diffie- Hellman Algorithm and its Use in Secure Internet Protocols", SANS institute, 5-nov-2001.