**IOSR Journal of Engineering (IOSR JEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 81-83

# A Study on Basic Cryptography Techniques

Amutha . S
*Assistant professor, Dept of Computer Science Annai Womens College*

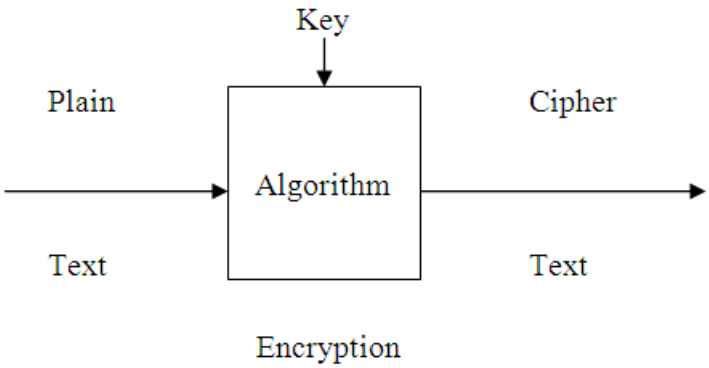
***Abstract:*** *Visual cryptography is associated with the process of converting ordinary plain text into incomprehensive text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice. Visual Cryptography takes a binary image (the secret) and divides it into two or more pieces known as shares. When the shares are printed on transparencies and then superimposed, the secret can be recovered. Visual Cryptography is a unique technique in the sense that the encrypted message can be decrypted directly by the human visual system. In this survey, we will summarize the latest developments of visual cryptography since its inception in 1994, introduce the main research topics in this area and outline the current problems and possible solutions. Directions and trends for future work shall also be examined along with possible visual cryptography applications.*

***Key Words:*** *Visual Cryptography, Security, Encryption, Keys*

## I. Introduction

Cryptography is used in many applications like banking transactions cards, computer passwords, and e-commerce transactions. Visual cryptography allows the transmission of visual information and many aspects of this area are covered, including its inception to the current techniques being employed and actively researched today. This survey covers the progress of Visual Cryptography, along with the current trends and the various applications for Visual Cryptography (Jonathan, 2010).

(Ashwak, 2011) Cryptography process seeks to distribute an estimation of basic cryptographic primitives across a number of confluences in order to reduce security assumptions on individual nodes, which establish a level of fault-tolerance opposing to the node alteration. In a progressively networked and distributed communications environment, there are more and more useful situations where the ability to distribute a computation between a number of unlike network intersections is needed. The reason back to the efficiency (separate nodes perform distinct tasks), fault-tolerance (if some nodes are unavailable then others can perform the task) and security (the trust required to perform the task is shared between nodes) that order differently.

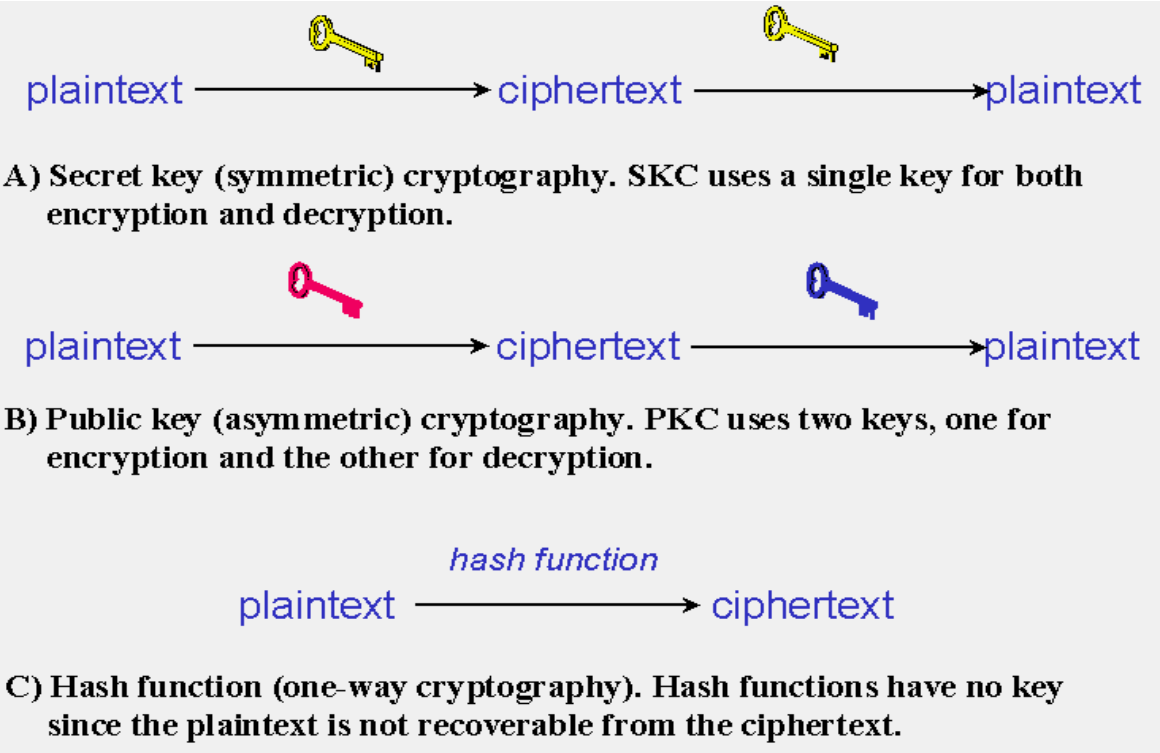



**Three types of cryptographic techniques used in general.**
1.Symmetric-key cryptography
2 Public-key cryptography
3 Hash functions.

**Symmetric-key Cryptography:** Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

**Public-Key Cryptography:** This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

**Hash Functions:** No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.




## II. Problems Solved By Cryptography

A secure system should provide several assurances such as confidentiality, integrity, and availability of data as well as authenticity and non-repudiation. When used correctly, crypto helps to provide these assurances. Cryptography can ensure the confidentiality and integrity of both data in transit as well as data at rest. It can also authenticate senders and recipients to one another and protect against repudiation.

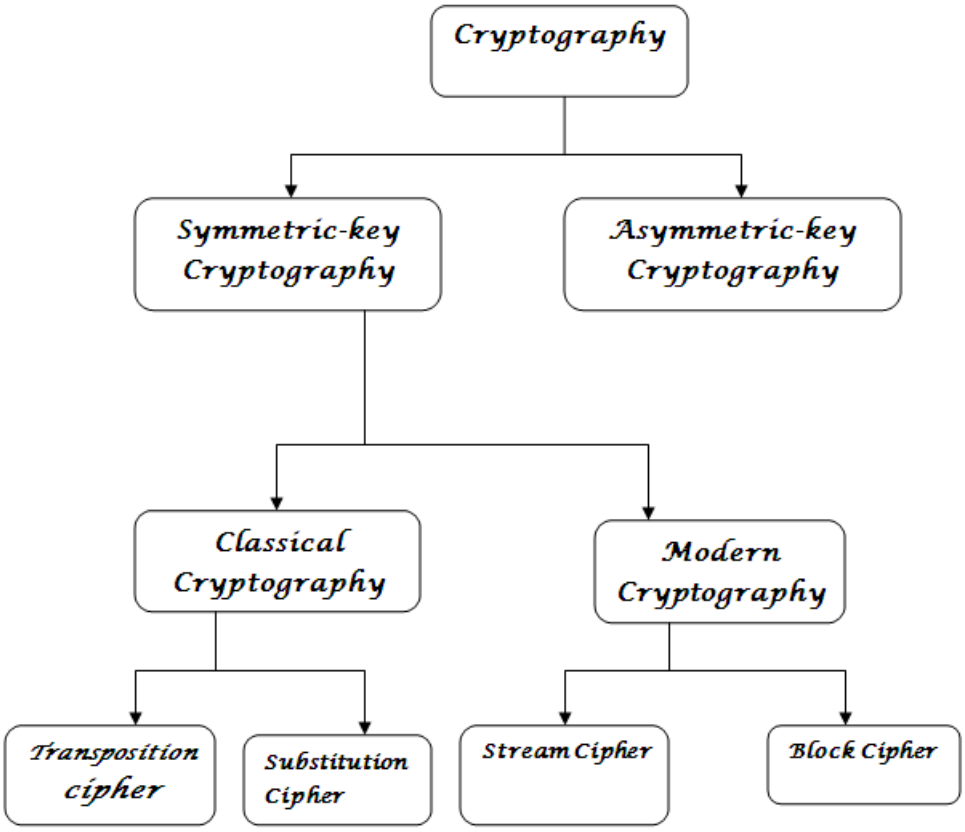
Software systems often have multiple endpoints, typically multiple clients, and one or more back-end servers. These client/server communications take place over networks that cannot be trusted. Communication occurs over open, public networks such as the Internet, or private networks which may be compromised by external attackers or malicious insiders.

It can protect communications that traverse unreliable networks. There are two main types of attacks that an adversary may attempt to carry out on a network.

- Passive attacks
- Active attacks

Passive attacks involve an attacker simply listening on a network segment and attempting to read sensitive information as it travels. Passive attacks may be online (in which an attacker reads traffic in real-time) or offline (in which an attacker simply captures traffic in real-time and views it later—perhaps after spending some time decrypting it). Active attacks involve an attacker impersonating a client or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them on to their intended destination (or dropping them entirely).

**Work Flow of Cryptography**




Now Symmetric key Cryptography is further categorized as Classical Cryptography and Modern Cryptography. Further drilling down, Classical Cryptography is divided into Transposition Cipher and Substitution Cipher. On the other hand, Modern Cryptography is divided into Stream Cipher and Block Cipher. In Cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext.

## III. Conclusion

Data on a removable disk or in a database can be encrypted to prevent disclosure of sensitive data should the physical media be lost or stolen. In addition, it can also provide integrity protection of data at rest to detect malicious tampering. All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner. The security of cryptographic technique is based on the computational difficulty of mathematical problems.

## References

[1]. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Boca Raton 1997, ISBN 0-8493-8523-7.
[2]. Klaus Pommerening, *Datenschutz und Datensicherheit.* BI-Wissenschaftsverlag, Mannheim 1991. [out of print, here is the PDF file.]
[3]. Michael Pröse, *Chiffriermaschinen und Entzifferungsgeräte in Zweiten Weltkrieg.* m press, München 2006. ISBN 3-89975-548-0. [Previous version online.]
[4]. Rainer A. Rueppel, *Analysis and Design of Stream Ciphers.* Springer-Verlag, Berlin 1986. [out of print]
[5]. A. Salomå, *Public-Key Cryptography.* Springer-Verlag, Berlin 1990.
[6]. Bruce Schneier, *Applied Cryptography*. John Wiley, New York 1996(2), ISBN 0-471-11709-9.
[7]. Klaus Schmeh, *Cryptography and Public Key Infrastructure on the Internet.* John Wiley, New York 2003, ISBN 978-0-470-84745-9.