A PRAGMATIC ANALYSIS ON CRYPTOGRAPHY IN NETWORK SECURITY AND FORENSIC APPLICATIONS

Shina Arora[1], Ruchi Singla[2]

[1]*M.Tech. Research Scholar, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Landran, Mohali, Punjab, India*

[2]*Professor, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Landran, Mohali, Punjab, India*

Abstract

Cryptography assumes a noteworthy part in securing information. It is utilized to guarantee that the substance of a message are privately transmitted and would not be changed. System security is most essential part in data security as it alludes to all equipment and programming capacity, attributes, highlights, operational methodology, responsibility, access control, and managerial and administration approach. Cryptography is key to IT security challenges, since it supports protection, secrecy and personality, which together give the basics to trusted e-business and secure correspondence. There is an expansive scope of cryptographic calculations that are utilized for securing systems and in no time consistent looks into on the new cryptographic calculations are continuing for developing more propelled methods for secures correspondence. Cryptographic is a system of changing a message into such frame which is incomprehensible, and after that retransforming that message back to its unique structure. Cryptography works in two strategies: symmetric key otherwise called mystery key cryptography calculations and hilter kilter key otherwise called open key cryptography calculations.

Keywords: *Symmetric Key, Asymmetric Key, Hash Function, Hybrid, Quantum Cryptography, Network Security*

----------***----------

I. INTRODUCTION

Cryptography before the advanced period was viably considered as identical to the encryption,that includes renovation of data means to add on something to it known as comprehensible state of data to the apparent jabber. The originator of an encoded message (Alice) shared the making an interpretation of system anticipated that would recover the principal information just with proposed recipients (Bob), along these lines blocking undesirable persons (Eve) from doing moreover. The cryptography writing frequently utilizes Alice ("A") for the sender, Bob ("B") for the planned beneficiary, and Eve ("spy") for the foe. Since the improvement of rotor figure machines in World War I and the approach of PCs in World War II, the techniques taht we utilize for cryptology have ended up being continuously astounding and its function more no matter how you look at it.[1]

A. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Secret Key Cryptography (SKC): In this method only one is used for both encryption and decryption purpose.

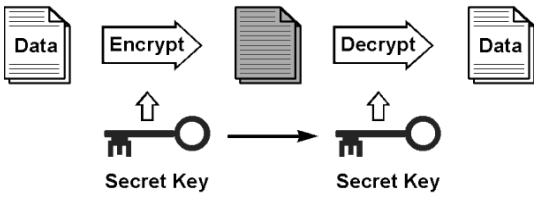

Figure 1: Cryptography by Secret Key

Public Key Cryptography (PKC): In this method one key is used for encryption and the other one for decryption purpose.

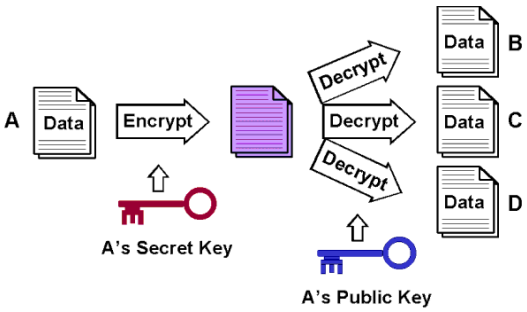

Figure 2: Cryptography by Public Key

Hash Functions: Utilizes one key for encryption and another for unscrambling

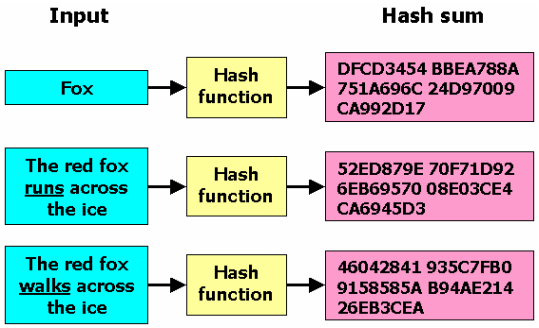

Figure 1: Hash Function in Cryptography

B. PURPOSE OF CRYPTOGRAPHY

Authentication: The procedure of demonstrating one's character. (The essential types of host-to-host verification on the Internet today are name-based or address-based, both of which are famously powerless.)

Privacy/confidentiality: Guaranteeing that nobody can read the message with the exception of the proposed recipient.

Integrity: Guaranteeing the beneficiary that the got message has not been changed at all from the first.

Non-repudiation: An instrument to demonstrate that the sender truly sent this message[2]

C. FUNDAMENTAL TERMINOLOGIES OF CRYPTOGRAPHY

Cryptography is the change of intelligible and justifiable information into a structure which can't be comprehended with a specific end goal to secure information. cryptography alludes precisely to the procedure of disguising the substance of messages, the word cryptography originates from the Greek word "Kryptos", that implies covered up, and "graphikos" which implies composing.

The data that we have to stow away, is called **plaintext** , It's the first content, It could be in a type of characters, numerical information, executable projects, pictures, or some other sort of data The plaintext for sample is the principal draft of a message in the sender before encryption, or it is the content at the collector after decoding.

The information that will be transmitted is called figure content or **Cipher**, it's a term alludes to the string of "meaningless"data, or misty content that no one must comprehend, aside from the beneficiaries. The information will be transmitted Exactly through system, Many calculations are utilized to change plaintext into figure content

The **Key** is an information to the encryption calculation, and this worth must be free of the plaintext. This information is utilized to change the plaintext into figure content, so diverse keys will yield distinctive figure content, In the translate side, the converse of the key will be utilized inside the calculation rather than the key.

Computer security it's a nonexclusive term for a gathering of devices intended to shield any information from programmers debasement, or regular fiasco while permitting these information to be accessible to the clients at the same time. One illustration of these apparatuses is the A-tremendous antivirus program [3].

Network security alludes to any action intended to ensure the ease of use, trustworthiness, unwavering quality, and wellbeing of information amid their transmission on a system. System security manages equipment and programming, The action can be one of the accompanying hostile to infection and against spyware, firewall, Intrusion counteractive action frameworks, and Virtual Private Networks.

Internet Security is measures and methods used to ensure information amid their transmission over a gathering of interconnected systems .while data security is about how to avert assaults, and to distinguish assaults on data based frameworks .

Cryptanalysis (code breaking) is the investigation of standards and techniques for translating figure content without knowing the key, regularly this incorporates finding and speculating the discharge key It's an unpredictable procedure including factual investigation, expository thinking, math devices and example finding, The field of both cryptography and cryptanalysis is called cryptology [4].

Symmetric encryption alludes to the procedure of changing over plaintext into figure content at the sender with the same key that will be utilized to recover plaintext from figure content at the beneficiary while asymmetric encryption alludes to the procedure of changing over plaintext into figure content at the sender with various key that will be utilized to recover plaintext from figure content at the beneficiary.

II. SYMMETRIC AND ASYMMETRIC KEY

In case of symmetric key based encryption, similar key is utilized for the encryption as well as unscrambling process. Symmetric based calculations are having upside of not expending a lot of computing force and it is working in fast in encoding them. This approach occurs in two modes including square figures or stream figures. In the piece figure mode the whole data is isolated into number of pieces. “Such information depends on the square length and the key is accommodated encryption. On account of the stream figures the information is partitioned as little as single bits and randomized then the encryption happens. Symmetric key cryptosystems are much speedier than the asymmteric key cryptosystems. The execution assessment is occurred for the accompanying symmetric key encryption systems, for example, The DES Algorithm, Triple DES calculation, the AES algorithm and Blowfish algorithm [5].

These algorithms have numerous focal points:

- Execute at high speeds
- Consume less computer processor time and resources of memory
- Efficient and secure

Notwithstanding, symmetric key cryptographic procedures experience the ill effects of numerous issues:

- Key management problem
- Key distribution problem
- Inability to digitally sign a message

Asymmetric key encryption is the procedure, in which the diverse keys are for the encryption and the decoding process or decryption process. One key is open (distributed) and second is kept private. They are also familiar as public key encryption. In the event that the lock/encryption key is initially distributed then the framework empowers private correspondence from the general population to the unlocking key's client [9]. In the event that the unlock/decryption key is the one distributed then the framework serves as a mark verifier of reports bolted by the proprietor of the private key. Open or Public key techniques are imperative since they can be utilized for transmitting encryption keys or other information safely notwithstanding when the both the clients have no chance to concede to a mystery key in private Algorithm. The keys utilized as a part of open or Public key encryption algorithms are generally any longer that enhances the security of the information being transmitted.

A. KEY FACTORS ON PERFORMANCE

In this work, the accompanying elements are utilized the execution methodology, for example, computation speed, tenability, length of key, security issue, encryption proportion, throughput and time of information against assaults [6].

a. Tunability
It is exceptionally well known to characterize a scrambled components and parameters of encryption used to various applications.

b. Computational Speed
In the ongoing applications, the classical encryption and decoding or simply decryption algorithms are quite swift and adequate to meet constant prerequisites.

c. Key Length Value
In encryption based modules, the key administration is vital element for demonstration of the how the information is scrambled. The symmetric algorithm utilizes a variable key length which is longer. In this way, the key administration is a tremendous angle in encryption preparing.

d. Encryption Ratio
The encryption proportion is the estimation of the measure of information that is to be encoded. Encryption proportion must minimize to decrease the intricacy on calculation.

e. Security Issues
Cryptographic security characterizes whether encryption plan is secure against animal power, time assault and diverse plaintext-figure content assault. For exceptionally critical sight and sound application to the encryption plan ought to fulfill cryptography security. We measure cryptographic security in the three levels for instance low, medium and high.

f. Time
The time fundamental by calculation to add up to the operation relies on upon processor rate and calculation multifaceted nature. Less time calculation take to whole its operation enhanced it is.

g. Throughput
Throughput of the encryption calculations is computed by isolating the aggregate plaintext in Megabytes scrambled on aggregate encryption time for every calculation. In this manner, if throughput expanded the force utilization is abatement.

B. HASH FUNCTIONS

The phrase hash capacity can be utilized as a part of software engineering from a long while and it alludes to a limit that packs a string of self-decisive information to a string of adjusted length. Be that as it may on the off chance that it fulfills some extra prerequisites, at that point it can be used for cryptographic applications and a short time later known as Cryptographic Hash limits. Cryptographic Hash functions are a standout amongst the most vital device in the field of cryptography and are utilized to accomplish various security objectives like realness, advanced marks, pseudo number era, computerized steganography, computerized time stamping and so on. Gauravram [7] in his postulation has proposed that the utilization of cryptographic hash capacities in a few data handling applications to accomplish different security objectives is a great deal more broad than use of block ciphers and stream ciphers.

a. One Way Hash Functions (OWHF)

Merkle [8]characterized OWHF as a hash capacity ‘h’ that fulfills the accompanying necessities:
I. F can be connected to square of information of any length. (By and by, 'any length' might be really limited by some tremendous consistent, bigger than any message we ever would need to hash.)
II. F generate output having fixed length.
III. Set F and a i.e. input provided, then it become effortless having computer message digest F(a).
IV. Set F and F(a), it becomes harder to discover x.
V. Set F and F(a), it is becomes harder to discover x and x’ such that F(a) = F(a’)

The initial three prerequisites are must for down to earth uses of a hash functions to message computerized marks and for validation. The fourth prerequisite otherwise called pre-picture resistance or restricted property, expresses that it is anything but difficult to create a secret code for the given message however hard (for all intents and purposes incomprehensible) to produce a secret code for the message. The last one prerequisite otherwise called Second pre-picture resistance property ensures that an optional message hashing to the same code as a given message can't be found.

b. Collision Resistant Hash Functions (CRHF)

Merkle [9] provided the meaning for CRHF as in light of the same, CRHF might be characterized as a Hash function F, that fulfills every one of the prerequisites of OWHF and what's more fulfill the accompanying crash resistance property:
Set F, it becomes harder to discover a pair
(a, b) such that F(a)) = F(b)

c. Universal One Way Hash Functions (UOWHF)

One thought of Universal One Way Hash capacities is presented by Mani Naorand Moti Yung [10] and utilizing the equivalent, exhibited an advanced mark plot that was not in view of trapdoor capacities. It is possible that Mani Naorand Moti Yung, utilized One path capacities for the development of UOWHF and thus actualize the scheme of Digital Signature. The property of security for UOHWF is defined as:

Let V contains a limited number of hash capacities with each having the same likelihood of being utilized. Let a probabilistic polynomial time calculation T(T is impact foe) works in two stages. At first, A gets enter s and yields t esteem r known as introductory esteem, then a hash work F is looked over the family V. A then gets F and should yield y such that F(s) = F(t). At the end of the day, in the wake of getting a hash work it tries to discover a crash with the underlying esteem. Presently U will be called as a group of Universal One Way Hash Functions if for all polynomial-time A the likelihood that A succeeds is insignificant.

C. HASH FUNCTION'S ATTACKS

Mainly two types of attacks are considered for hash functions and it includes: brute force attacks and cryptanalytical attacks.

- **Brute force Attacks**
  Brute force attacks are considered as a specific methodology use to attempt arbitrarily figured hashes to acquire a particular hash digest. Consequently, the included assaults don't rely on upon the hash function's structure also known as compression function. The hash function security lies on the yield hash digests length. That implies, the more drawn out hash process more additionally security is gained by hash fucntion. The mentioned attack is an experimentation strategy to get a wanted hash capacity [11].

- **Cryptanalytical Attacks**
  A hash capacity cryptanalysis endeavors to assault the properties of hash capacities, for example, a preimage attack, collison attack and second preimage attack. Because of the hash values have settled size it contrast with the messages having larger in size than this, impacts must exist in hash functions. Nonetheless, for the hash function security purpose they should become impossible to discover. Note that impacts in hash capacities are much less demanding to discover than preimages or second preimages. Casually, a hash capacity is considered to be broken at the point when a decreased number of appraisals of the hash work appeared differently in relation to the animal compel assault complexities and the qualities assessed by the maker of the hash limit are used to harm no short of what one of its properties irrelevant of the computational reasonableness of that effort [12].

- **Generic Attacks**
  These attacks are specialized study utilize by assault for general hash capacity developments that includes Merkle-Damgård development. Generic implies that the assault have no intensions for the particular hash capacity. These attacks are ordered into four sorts, talked about in the accompanying segments:

1) Length Extension Attacks
An assailant make use of the benefits by utilizing the cushioning plan that recommended for the messages that includes development by Merkle-Damgård, considered to apply length expansion assault that also known as augmentation assault. Length augmentation assault can be utilize to split mystery prefix MAC plan where the assailant registers the validation labels lacking the information of the mystery key.

2) Joux Attack
Joux attack or Joux multi-collision assault includes an attack on Merkle-Damgård hash capacity, where Antoine Joux demonstrated that finding various impacts in a Merkle-Damgård hash limit is next to no harder than finding single accidents. In his multi-sway ambush, Joux acknowledged access to a machine C that given a fundamental state, returns two affecting messages.

3) Long Message second preimage Attacks
In this attack the assaults, the assailant find a second preimage P for a given message m, where $m \neq P$ and $h(m) = h(p)$ with an exertion under 2T calculation of h. In the long message second preimage assault, the aggressor tries to locate a second preimage for a long target message m of 2s+1 message block. The assailant does this by finding a connecting message square Mlink. Where, the review of FIV of the connecting message piece Mlink matches one of the middle of the road states Hi got in the hashing of M. The calculation expense of this assault is around 2T-s calls to the compression F.

4) Herding Attack
Kelsey and Kohno [13] includes an assault and with the help of second preimage and multi-crash this can be identified. A run of the scenario where this assault can be utilized is the point at which an enemy focuses on a hash esteem E where E is not considered as irregular. The author makes open and claims that he has learning of obscure later on occasions and that E is taken as hash of that information. Later, when the relating events happen, the adversary tries to swarm the learning of those events to hash to D as he already affirmed

5) Specific Attacks
Some specific assaults on hash functions rely only on the hash function itself. For instance, assaults on SHA-0, SHA-1 and MD5 are also familiar as multi-piece crash assaults. Multi-Block Collision Attack (MCBA) strategy on iterated hash capacity (i.e Merkle-Damgård development) discovers two impacting messages each no less than two squares on length. In such assault, crashes

are found by handling more than one message block. Truth be told, multi-square crashes assault is appropriate and substantial on SHA-0, SHA-1 and MD5 since these hash capacities utilize more than a solitary and impacts are dispersed randomly.

III. QUANTUM AND HYBRID CRYPTOGRAPHY

Quantum cryptography is an innovation that guarantees extreme security. Contrasted with current or classical cryptography which could be crushed by improvement of extremely fast systems, quantum cryptography guarantees secure correspondence since it depends on the central physical laws. It is a rising innovation in which two gatherings might all the while produce shared, anonymity cryptographic key material which utilizes the transmission of the quantum conditions of light. “The quantum based cryptography approach is another higher quality and superior technique for mystery correspondences offering a definitive security confirmation of the sacredness of a Law of Nature. The quantum cryptography depends on two vital components of quantum mechanics-the Heisenberg Uncertainty standard and the guideline of photon polarization.”[14]

A. APPLICATIONS ASSOCIATED WITH QUANTUM CRYPTOGRAPHY

The most notorious and created utilization of quantum cryptography is quantum key dissemination (QKD). “Quantum key distribution is a strategy utilized as a part of the system of quantum cryptography with a specific end goal to deliver a flawlessly arbitrary key which is shared by a sender and a beneficiary while ensuring that no one else has an opportunity to find out about the key, e.g. by catching the correspondence channel utilized amid the procedure. The best known and famous plan of quantum key dispersion depends on the Bennet–Brassard protocol, which was developed in 1984 [15]. It relies on upon the no-cloning hypothesis for non-orthogonal quantum states. Quickly, the Bennet–Brassard convention acts as takes after:

- The sender also called as John conveys a progression of single photons. For every photon, it arbitarily chooses one of two conceivable base states, with one of them having the conceivable polarization headings up/down and left/right, and the other one polarization headings which are calculated by 45°. For every situation, the genuine polarization bearing is moreover arbitarly chooses.
- The recipient (called Bob) identifies the polarizations of the approaching photons, likewise arbitrarily selecting the base states. This implies by and large 50% of the photons will be resolved with the "wrong" base states, i.e. with states not comparing to those of the sender.
- Later, John and Bob utilize an open correspondence channel to discuss the states utilized for every photon (except not on the picked polarization headings). Along these lines, they can find which of the photons were by chance they can find which of the photons were by chance ensured with the same base states on both sides.
- At that point they dismiss all photons with a "wrong" premise, and the others connote a succession of bits which ought to be indistinguishable for John and Bob furthermore, should be known just to them, gave that the transmission has not been influenced by anybody. Despite whether this happened they can test by taking a gander at some number of the got bits by method for general society information channel”. On the off chance that these bits concur, they realize that alternate ones are additionally right and can at long last utilized for the genuine information transmission.

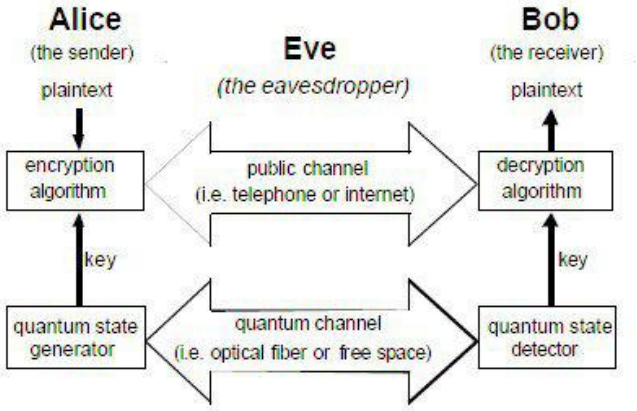

Figure 4: Quantum Cryptography

Hybrid cryptography [16] is a method utilizing various figures of various sorts together, each further bolstering its best good fortune.

A hybrid cryptosystem can be built utilizing any two separate cryptosystems:

- A key has epitome plan which is an open or public key or whatever other sort of cryptosystem.
- An information has encapsulation plan which is a symmetric-key cryptosystem.

The hybrid cryptosystem is itself an open or public key framework, who's open and private keys are the same as in the key encapsulation plan. Set up of open or public key framework we can utilize advanced mark or digital signature like message processing capacity with symmetric key framework to make hybrid crypto framework. For instance, to encode a message tended to client 1 in a hybrid method client 2 does the accompanying :

1. Acquires Client 1 Open or Public Key
2. Produces a fresh symmetric key
3. Encodes the message utilizing the symmetric key.
4. Scramble or encrypt the symmetric key utilizing client 1 open key. Send both of these encryptions to client 1

To decode this hybrid cipher figure content, client 1 does the accompanying:

1. Client 1 utilizes her private key to decode the symmetric key.
2. Client 1 utilizes this symmetric key to unscramble the message.

IV. NETWORK SECURITY USING CRYPTOGRAPHY

End to end assurance of voice correspondence is a generally late marvel. The principle reason has been innovative restrictions, however there is additionally a critical lawful boundary, since governments need to keep up the ability to perform wiretaps for law requirement and national security purposes. Simple voice scramblers don't over a high security level. The US appointment in the 1945 Yalta gathering brought along exceptionally voluminous gadgets for computerized voice encryption; clearly they were never utilized, a.o. for the low quality. Effective advanced coding of voice for mass business sector items touch base in the 1980s: secure advanced telephones (e.g. the STUs) got to be accessible, yet outside the administration and military environment they were never fruitful. Be that as it may, today Voice over IP (VoIP) advancements result in boundless end-to-end security taking into account programming encryption. The primary simple cellular telephones gave no or exceptionally powerless security, which brought about genuine shame (e.g., the private discussions of Prince Charles being uncovered or the spying of the Soviet versatile correspondence frameworks by the US). The European GSM framework composed in the late 1980s gave officially vastly improved security, regardless of the fact that numerous blemishes remain; these imperfections did not stop the framework: in 2010 there are more than 4 billion GSM and WCDMA-HSPA supporters. The GSM security defects have been determined in the 3GSM framework, however even there no limit to-end assurance is given. The present era of advanced cells clients can unmistakably run programming, (for example, Skype) with this capability.[17]

A. TRENDS IN CRYPTOGRAPHIC PROTOCOL

In this area we portray what we see as a percentage of the rising patterns in cryptographic conventions. These patterns exhibit new difficulties to convention examination:

1. Greater Adaptability and Complexity:

Presumably a standout amongst the most evident patterns is the expanding various types of situations that conventions must interoperate with. As systems handle increasingly undertakings in a possibly threatening environment, cryptographic conventions tackle increasingly obligations.As systems administration turns out to be more broad, and distinctive stages must interoperate, we see conventions, for example, the Internet Key Exchange (IKE) convention that should concur upon encryption keys, as well as on the calculations that are to utilize the keys. Then again, we might see conventions, for example, SET that should have the capacity to prepare diverse sorts of Visa transactions.One method for endeavoring to meet this test is to expand the intricacy of the convention. This obviously makes confirmation as well as usage more troublesome too, and thus there is dependably imperviousness to this methodology. In any case, the inclination to more noteworthy many-sided quality will dependably arrive, and it will at last must be met in any event almost by any individual who is endeavoring to perform any kind of security analysis.

2. Adoption of New Types of Cryptographic Primitives

When all is said in done, it will be it is acknowledged that a traditionalist way to deal with calculation is best when outlining cryptographic conventions; just time tested calculations ought to be utilized. In any case, as the field develops the quantity of calculations that are considered to have gotten enough investigation has expanded. Besides, as figuring force builds, calculation that were once considered restrictively costly have ended up simpler to actualize, while others, for example, DES, are generally viewed as didn't really giving sufficient security.

B. NEW TYPES OF THREATS

In the early years of PC security, a significant part of the risk examination was speculative, and centered around assaults in which there would be a clear(usually money related) pick up for the aggressor. Presently, with more experience, we see that there are different sorts of assaults, the vast majority of them identified with foreswearing of administration, that can keep a system from satisfying its capacities. Numerous dissent of administration assaults can be countered by great asset administration. Yet, solid convention outline can do much to offer assistance, for instance by keeping a responder from conferring its assets to corresponding with an initiator until it has satisfactory affirmation that it knows who it's conversing with. This can be a sensitive issue notwithstanding, since a hefty portion of the systems utilized for validation themselves require responsibility of assets, and since the choice of the amount of assets to confer, and when, can be exceptionally execution subordinate. Effective investigation will depend to some degree on the capacity to think about the assets used by an aggressor to the assets used by a defender. Other dangers, for example, activity examination, concentrate on issues that are not by any stretch of the imagination an issue until sufficient cryptographic insurance for correspondence mystery has as of now been accomplished. Security against movement investigation is one of these. Notwithstanding when encryption is utilized source and destination of message activity is not covered up, and it can be feasible for an eyewitness to gain much from this alone. Various distinctive frameworks have been created that endeavor to take care of this issue with shifting degrees of culmination. Notwithstanding, without some capacity to assess and think about the level of assurance offered by these frameworks, it is hard to survey what sum and sort of security they offer. Such investigation strategies ought to consider measurable methods, since much activity examination relies on upon factual analysis.[18]

A to some degree diverse kind of risk develops when we take a gander at electronic business conventions. In this sort of convention, the parties included take part in an exchange that outcomes in specific levels of result to every main included. Besides, the convention might either rely on or

attempt to ensure liveness or decency properties and in addition security properties". A main might attempt to cheat by attempting to expand its result to the detriment of those of different gatherings, yet won't take part in conduct that will bring about a bringing down of its result, or put it at a detriment as for the others.

V. CONCLUSION

Cryptography is utilized to guarantee that the substance of a message are secrecy transmitted and would not be changed. Secrecy implies no one can comprehend the got message aside from the one that has the interpret key, and information can't be changed means the first data would not be changed or adjusted; this is done when the sender incorporates a cryptographic operation known as hash function in the message M hash function is a numerical representation of the data, at the point when data lands at its recipient; the collector figures the estimation of this hash capacity. On the off chance that the beneficiary's hash function worth is equal to the sender's, the respectability of the message is guaranteed. In this review paper we portray and analyze in the middle of symmetric and deviated encryption strategy give numerous illustration to demonstrate the distinctions.

REFERENCES

[1] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh, "*Survey Paper: Cryptography Is The Science Of Information Security*"International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011

[2] Gary C. Kessler, "An Overview of Cryptography",3 March 2016

[3] J. Badeau.,: " *The Genius of Arab Civilization* ", Second Edition. MIT Press,(1983), USA

[4] D.Salomon" *Data Privacy and Security* " First Edition. Springer-Verlag New York, (2003):, Inc.
USA.

[5] Mittal M., "*Performance Evaluation of Cryptographic Algorithms*", IJCA, International Journal of Computer Applications, ISSN 0975-8887.

[6] Ritu T., Sanjay A., National Institute of Technical Teachers' Training and Research Bhopal, India, "*Comparative Study of Symmetric and Asymmetric Cryptography Techniques*" IJAFRC International Journal of Advance Foundation and Research in Computer Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

[7] P. Gauravram, "*Cryptographic Hash Functions: Cryptanalysis, design and Applications*", Ph.D. thesis, Faculty of Information Technology, Queensland University of Technology, Brisbane, Australia, 2003

[8] R. C. Merkle, "*Secrecy, Authentication and Public Key Systems*", Ph.D. thesis, Department of Electrical Engineering, Stanford University, Stanford, USA, 1979.

[9] R.C. Merkle, "*One Way Hash Functions and DES*", in CRYPTO, 1989, pp.428-446.

[10] M. Naor, and M. Yung, "*Universal One-Way Hash Functions and their Cryptographic Applications*", in STOC, 1989, pp.33-43.

[11] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby. "*Collisions of SHA-0 and Reduced SHA-1*", In Ronald Cramer, editor, Advances in Cryptology - EUROCRYPT 2005, vol- ume 3494 of Lecture Notes in Computer Science, pages 36–57. Springer, 2005

[12] Yuliang Zheng, Josef Pieprzyk, and Jennifer Seberry, 1993, "*AHAVAL – A One-Way Hashing Algorithm with Variable Length of Output*‖*",* Lecture Notes in Computer Science, Volume 718, Advances in Cryptology – Auscrypt '92, pp. 83–104.

[13] J. Kelsey and T. Kohno. Herding hash functions and the nostradamus attack. In S. Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006,Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 183–200. Springer, 2006.

[14] Miss. Payal P. Kilor1, Mr.Pravin.D.Soni2," Quantum Cryptography: Realizing next generation information security", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*

[15] C. H. Bennett and G. Brassard, "*QuantumCryptography: Public Key Distribution and Coin Tossing*",In Proceedings of IEEE International Conference onComputers Systems and Signal Processing, Bangalore,India, pp. 175-179,
December 1984. (Bennet–Brassard protocol)

[16] Bhatele, K. Sinhal, A. ; Pathak, "*A novel approach to the design of a new hybrid security protocol architecture*",Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference on Page(s): 429 - 433 Print ISBN: 978-1-4673-2045-0

[17] Mohamed A.Haleem, Chetan N. Mathur, R. Chandramouli, K. P. Subbalakshmi, "*Opportunistic Encryption: A tradeoff between Security and Throughput in Wireless Network*" IEEE Transactions on Dependable and secure computing, vol. 4, no. 3.

[18] Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S. Shebani,"*Communication Cryptography*", 2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.