ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

A Survey on Modern Cryptography Techniques

Avadhesh Kumar

Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India

Email Id: avadheshkumar@galgotiasuniversity.edu.in

ABSTRACT: In the present data age, correspondence assume a significant job which help in development of new advancements. So security is a fundamental parameter to be considered. A component is accordingly expected to verify the data that is sent. The way toward changing the first data into a garbled arrangement is known as encryption. The procedure of again changing over the ambiguous organization in to the first data is known as unscrambling. The investigation of both encryption and unscrambling is known as cryptography. This paper centresaround investigating various kinds of cryptography, idea of encryption and decoding, a concise prologue to cryptography procedures. On the off chance that we are taking about security of data, at that point following administrations come as a main priority for example Secrecy (security of data), Authentication, Integrity (has not been modified) .This paper gives a point by point depiction of all these cryptography systems and an open key cryptography calculation RSA.

KEYWORDS*:* Asymmetric Key, Cipher Text, Cryptography, Information, RSA Algorithm, Symmetric Key.

I.INTRODUCTION

A plain text or typical book, which is send over the system is right off the bat get changed into cipher message with the goal that lone the sender and the beneficiary can utilize the data. In specialized terms, the way toward encoding plain instant messages into figure instant messages is known as encryption. Change procedure of figure message again into plain content is known as unscrambling [1]. Unscrambling is only inverse to encryption. In PC to PC interchanges, the PC at sender's end as a rule changes a plain instant messages into figure instant messages by performing encryption. At that point this message is sent to the beneficiary over the system. The beneficiary's PC takes the scrambled message and plays out the decoding procedure to get plain content. The procedure of encryption and unscrambling is known as cryptography. When all is said in done cryptography is the craftsmanship and study of accomplishing security by encoding message to make them non comprehensible. It very well may be utilized to conceal the importance of data in any structure. It can likewise be applied to programming, illustrations or voice [2][3].

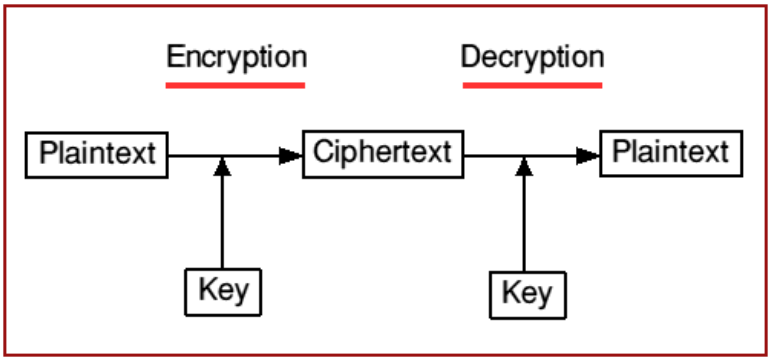

Fig. 1 Typical cryptography process

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

Cryptography is the specialty of mystery coding. The fundamental help gave by cryptography is the capacity to send the data between members in a manner that forestalls others understanding it [4]. The primary motivation behind the cryptography is utilized not exclusively to give privacy, yet additionally to give answers for different issues like: information uprightness, validation, non-revocation [5].
Cryptography is the strategies that enable data to be sent in a safe from so that the main collector ready to recover this data. By and by constant investigates on the new cryptographic calculations are going on [1]. In any case, it is an extremely hard to discover the particular calculation, since we have definitely realized that they should consider numerous components like: security, the highlights of calculation, the time intricacy and space unpredictability [6].

II.TECHNICALITIES

- Plain text -original message
- Cipher text- coded message
- Encrypt -convert plain text into coded text
- Decrypt - convert coded text into plain text
- Cryptography-study of encryption principles and methods.

III.PURPOSE OF CRYPTOGRAPHY

In information and media communications, cryptography is vital when conveying over any non-confided in medium, which incorporates pretty much any system, especially the Internet [7]. Inside the setting of any application-to-application correspondence, there are some particular security necessities, including [8]:

- Authentication: The way toward demonstrating one's personality. (The essential types of host-to-have validation on the Internet today are name-based or address based, the two of which are famously feeble.)
- Privacy/confidentiality: Ensuring that nobody can peruse the message with the exception of the proposed beneficiary.
- Integrity: Assuring the recipient that the got message has not been changed at all from the first.
- Non-repudiation: A component to demonstrate that the sender truly sent this message.

Cryptography, at that point, shields information from burglary or adjustment, yet can likewise be utilized for client verification. There are, when all is said in done, three sorts of cryptographic plans regularly used to achieve these objectives: mystery key (or symmetric) cryptography, open key (or lopsided) cryptography, and hash works, every one of which is depicted underneath. In all cases, the underlying decoded information is alluded to as plaintext. It is encoded into figure content, which will thus (for the most part) be unscrambled into usable plaintext [9][10].

IV.ENCRYPTION APPROACH

In an encryption plot, the message or data, alluded to as plaintext, is encoded utilizing an encryption calculation, producing figure message that must be perused whenever decoded Encryption has for quite some time been utilized by militaries and governments to encourage mystery correspondence. It is currently generally utilized in ensuring data inside numerous sorts of non-military personnel frameworks. Encryption is likewise used to ensure information in travel, for instance information being moved by means of systems (for example the Internet, web based business), cell phones, remote mouthpieces, remote radio frameworks, Bluetooth gadgets and bank programmed teller machines.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

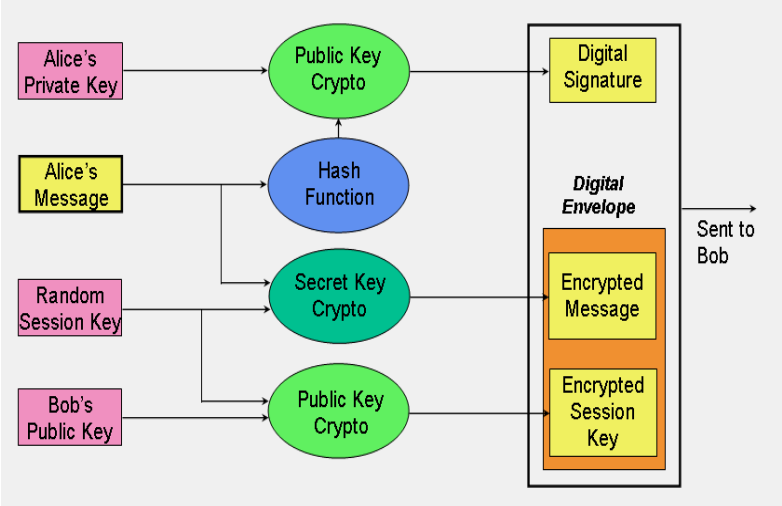

Fig. 2 Modern encryption method

In the proposed method we have a typical key among sander and recipient, which is known as private key. Essentially private key idea is the symmetric key ideas where plain content is changing over into scrambled content known as figure content utilizing private key where figure content decoded by same private key into plane content. The encryption key is inconsequentially identified with the decoding key.

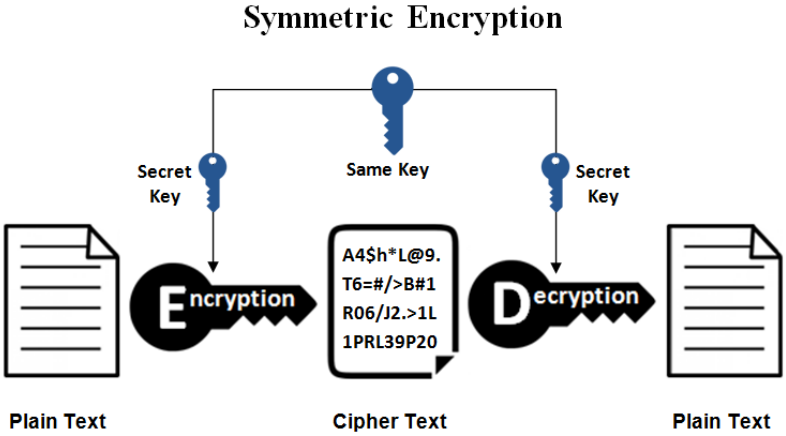

Fig. 3 Symmetric key Used

V.CRYPTOGRAPHY TECHNIQUES

There are two fundamental procedures for encoding data: symmetric encryption (likewise called mystery key encryption) and unbalanced encryption (additionally called open key encryption). Symmetric encryption is the most established and most popular strategy. A mystery key, which can be a number, a word, or only a string of arbitrary letters, is applied to the content of a message to change the substance with a certain goal in mind. Topsy-turvy encryption, in which there are two related keys- - a key pair. An open key is made uninhibitedly accessible to any individual who should send you a message. A second, private key is stayed discreet, with the goal that solitary you know it.

Symmetric Key Cryptography:

Symmetric-key cryptography alludes to encryption techniques in which both the sender and recipient share a similar key .Symmetric key figures are executed as either square figures or stream figures. A square figure enciphers

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

contribution to squares of plaintext rather than singular characters, the info structure utilized by a stream figure. Symmetric are a lot quicker than lopsided cryptography.

By utilizing symmetric encryption calculations, information is changed over to a structure that can't be comprehended by any individual who doesn't have the mystery key to decode it. When the expected beneficiary who has the key has the message, the calculation switches its activity with the goal that the message is come back to its unique and justifiable structure. The mystery key that the sender and beneficiary both use could be a particular secret word/code or it very well may be arbitrary series of letters or numbers that have been produced by a safe irregular number generator (RNG). This is the least complex sort of encryption that includes just a single mystery key to figure and decode data. Balanced encryption is an old and most popular strategy. It utilizes a mystery key that can either be a number, a word or a string of arbitrary letters.

Asymmetric Key Cryptography:

Asymmetrical encryption is otherwise called public key cryptography, which is a moderately new strategy, contrasted with symmetric encryption. Uneven encryption utilizes two keys to scramble a plain book. Mystery keys are traded over the Internet or an enormous system. It guarantees that vindictive people don't abuse the keys. Note that anybody with a mystery key can unscramble the message and this is the reason hilter kilter encryption utilizes two related keys to boosting security. An open key is made unreservedly accessible to any individual who should send you a message. The subsequent private key is stayed quiet about so you can just know. A message that is encoded utilizing an open key must be decoded utilizing a private key, while additionally, a message scrambled utilizing a private key can be unscrambled utilizing an open key. Security of the general population key isn't required in light of the fact that it is openly accessible and can be disregarded the web. Uneven key has a far superior force in guaranteeing the security of data transmitted during correspondence.

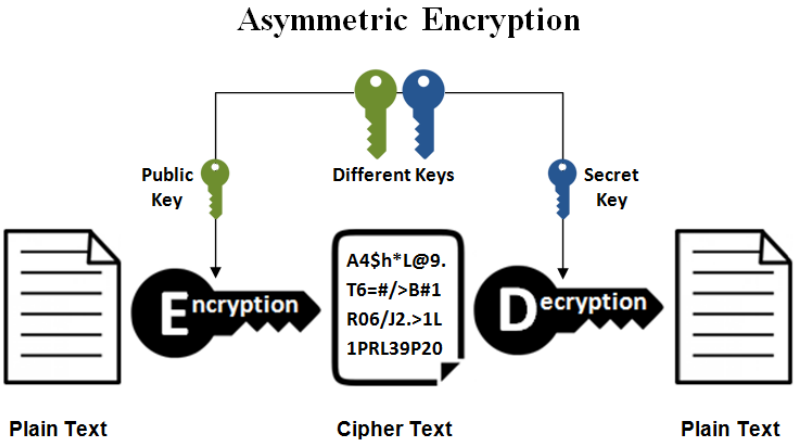

Figure 4. Asymmetric key Used

Asymmetric-key cryptography alludes to encryption strategies in which both the sender and recipient share the diverse key. One key is utilized for encryption and another for unscrambling. This gives more steadiness than symmetric frameworks. To utilize asymmetric encryption, there must be a method for finding open keys. One run of the mill system is utilizing advanced testaments in a customer server model of correspondence. An endorsement is a bundle of data that distinguishes a client and a server. It contains data, for example, an association's name, the association that gave the endorsement, the clients' email address and nation, and clients open key.

VI.RELEVANT ALGORITHMS

For cryptography strategies, various kinds of calculations are utilized for both symmetric and uneven key methods. The calculations for private (symmetric) key are DES (Data Encryption Standard), AES and so forth and for public(asymmetric)key are RSA (Rivest, Shamir, Adlemen), Diffie-Hellman: and so on.

RSA Algorithm:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

RSA represents Rivest Shamir and Adleman name of three innovators. RSA is one of the primary down to earth open key cryptosystems and is generally utilized for secure information transmission. In such a cryptosystem, the encryption key is open and varies from the decoding key which is stayed quiet. In RSA, this asymmetry depends on the down to earth trouble of considering the result of two enormous prime numbers, the figuring issue. RSA represents Ron Rivest, Adi Shamir and Leonard Adleman, who first freely portrayed the calculation in 1977.

Public key cryptography, otherwise called deviated cryptography, utilizes two unique yet scientifically connected keys - one open and one private. The general population key can be imparted to everybody, though the private key must be stayed discreet. In RSA cryptography, both people in general and the private keys can scramble a message; the contrary key from the one used to encode a message is utilized to unscramble it. This quality is one motivation behind why RSA has become the most broadly utilized topsy-turvy calculation: It gives a technique to guarantee the classification, honesty, credibility, and non-disavowal of electronic correspondences and information stockpiling.

Numerous conventions like Secure Shell, OpenPGP, S/MIME, and SSL/TLS depend on RSA for encryption and advanced mark capacities. It is likewise utilized in programming programs - programs are a conspicuous model, as they have to set up a protected association over an unreliable system, similar to the web, or approve a computerized mark. RSA signature confirmation is one of the most ordinarily performed activities in organize associated frameworks.

RSA (Rivest–Shamir–Adleman) is a calculation utilized by present day PCs to scramble and unscramble messages. It is a hilter kilter cryptographic calculation. Lopsided implies that there are two distinct keys. This is additionally called open key cryptography, since one of the keys can be given to anybody. The other key must be kept private. The calculation depends on the way that finding the variables of a huge composite number is troublesome: when the elements are prime numbers, the issue is called prime factorization. It is likewise a key pair (open and private key) generator.

To maintain a strategic distance from these issues, handy RSA executions commonly implant some type of organized, randomized cushioning into the worth m before scrambling it. This cushioning guarantees that m doesn't fall into the scope of uncertain plaintexts, and that a given message, when cushioned, will scramble to one of countless various conceivable cipher texts. The last property can build the expense of a word reference assault past the capacities of a sensible aggressor.

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

Key Generation:

```
def gcd(a, b):
    while a != 0:
        a, b = b % a, a
    return b
def findModInverse(a, m):
    if gcd(a, m) != 1:
        return None
    u1, u2, u3 = 1, 0, a
    v1, v2, v3 = 0, 1, m
    while v3 != 0:
        q = u3 // v3
```

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

```
v1, v2, v3, u1, u2, u3 = (u1 - q * v1), (u2 - q * v2), (u3 - q * v3), v1, v2, v3

return u1 % m
```

Encryption Ciphertext c comparing to determine as:

$$C \equiv m^e (mod\ n)$$

Plain content can be determined as:

$$m \equiv c^d (mod\ n)$$

Disadvantages:

In RSA encryption that is a deterministic encryption calculation (i.e., has no arbitrary part) an aggressor can effectively dispatch a picked plaintext assault against the cryptosystem. RSA has the property that the result of two figure writings is equivalent to the encryption of the result of the separate plaintexts. That is m1em2e ≡ (m1m2) e (mod n). In light of this multiplicative property a chosen cipher content assault is conceivable.

VII.CONCLUSION

Cryptography is an intriguing field with regards to PC science territory on the grounds that the measure of work done is as it were stayed quiet. There are different systems and calculation contemplated and various sorts of research have been finished. The best calculations are those which are well recorded and understood on the grounds that the calculations are very much tried and all around contemplated. This paper further considered that symmetric key cryptography are quicker than unbalanced frameworks. In any case, hilter kilter key cryptography are increasingly versatile and give more confirmation and non-renouncement effectively. Be that as it may, there us still need to grow such a calculation, that makes the encryption decoding process more simpler than RSA, DES and a lot more calculations. With the unstable advancement in the Internet, framework and data security have transformed into an unavoidable compassion for any affiliation whose inside private framework is related with the Internet. The security for the data has ended up being extraordinarily indispensable. Customer's data security is a central inquiry over cloud.

REFERENCES

[1]A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. 1996.
[2]E. Vahedi, V. W. S. Wong, and I. F. Blake, “An overview of cryptography,” in Crisis Management: Concepts, Methodologies, Tools, and Applications, 2013.
[3]R. Tripathi and S. Agrawal, “Comparative Study of Symmetric and Asymmetric Cryptography,” Int. J. Adv. Found. Res. Comput., 2014.
[4]V. Kumar and A. Sharma, “A Survey on Various Cryptography Techniques,” Int. J. Emerg. Trends Technol. Comput.Sci., 2014.
[5]G. Van Assche, Quantum cryptography and secret-key distillation. 2006.
[6]C. Paar and J. Pelzl, Understanding cryptography a textbook for students and practitioners. 2013.
[7]J. Baylis and N. Koblitz, “A Course in Number Theory and Cryptography,” Math. Gaz., 1989, doi: 10.2307/3618498.
[8]A. Young and M. Yung, “Cryptovirology: extortion-based security threats and countermeasures,” in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 1996, doi: 10.1109/secpri.1996.502676.
[9]P. Gupta and S. Kumar, “A Comparative Analysis of SHA and MD5 Algorithm,” Int. J. Comput. Sci. Inf. Technol., 2014.
[10]S. Roy and P. Venkateswaran, “Online payment system using steganography and visual cryptography,” in 2014 IEEE Students’ Conference on Electrical, Electronics and Computer Science, SCEECS 2014, 2014, doi: 10.1109/SCEECS.2014.6804449.
•Vishal Jain, Dr. Mayank Singh, “Architecture Model for Communication between Multi Agent Systems with Ontology”, International Journal of Advanced Research in Computer Science (IJARCS), Vol. 4 No.8, May-June 2013, page no. 86-91 with ISSN No. 0976 – 5697.
•Vishal Jain, Dr. Mayank Singh, “Ontology Based Information Retrieval in Semantic Web: A Survey”, International Journal of Information Technology and Computer Science (IJITCS), Hongkong, Vol. 5, No. 10, September 2013, page no. 62-69, having ISSN No. 2074-9015, DOI: 10.5815/ijitcs.2013.10.06.
•V.M.Prabhakaran ,Prof.S.Balamurugan , S.Charanyaa, “A Strategy for Secured Uploading of Encrypted Microdata in Cloud Environments”, International Advanced Research Journal in Science, Engineering and Technology Vol. 1, Issue 3, November 2014
•R Santhya, S Balamurugan, “A Survey on Privacy Preserving Data Publishing of Numerical Sensitive Data”, International Journal of Innovative Research in Computer and Communication Engineering , Vol. 2, Issue 10, October 2014

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

•BalamuruganShanmugam, Dr.VisalakshiPalaniswami, Santhya. R, Venkatesh. R.S., "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the art Survey. Aust. J. Basic & Appl. Sci., 8(15): 353-365, 2014