International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-09, Dec 2019

Review on Various Techniques of Cryptography

Seema S. Kute[1], Research Student, Dept. of CS & IT, Dr. B.A.M.U., Aurangabad, India, seemak0518@yahoo.in

Mukti E. Jadhav[2], Assistant Professor, Shri Shivaji Science and Arts College, Chikhali, India, muktijadhav@gmail.com

Chitra G. Desai[3], Professor, NDA Khadakwasala, Pune & India, chitragdesai@gmail.com

Abstract : The most important issue in network is information security. There are different cryptography techniques that provide security to our professional and personal information on top of the network. In our everyday life information sharing is needed and that data sharing is increased a lot. Many of us do online transactions in the day today life so, online transactions needed security. Likewise, many other activities performed online that also contains some information that require security for avoiding attacks that will cause misuse of knowledge, data modification and illegal access of information. So, send and receive the information in such a way that solely specific sender and receiver recognize it. It is implemented using methods of encryption and decryption. There are many techniques to do this. During this paper we are going to discuss about some such methods RSA, elliptical curve cryptography methods. Also give some brief review about the quantum cryptography.

Keywords — Conventional Cryptography, RSA, Elliptic Curve Cryptography, Quantum Cryptography.

I. INTRODUCTION

The alternative name of information security is nothing but cryptography. Cryptography word is derived from the Greek word origin in which "crypto" means hidden and "graphy" means writing that means nothing but secret writing. [1] Cryptography consists of two methods called encryption and decryption. In encryption process by using encryption algorithms converts the plain text to cipher text. In decryption process cipher text is converted into plain text only when the receiver known the encryption key which is generated during the encryption process. Public key cryptography and private key cryptography are two types of cryptography. Only one single confidential key is used in private key cryptography for both encryption and decryption. It is necessary to store this key as a confidential in the network. However, it is very difficult job to do so in the network. This algorithm is faster than the public key cryptography. In public key cryptography public and private two co relational keys are handle date encryption and decryption. In this the private key never open up in the network. A message that is encrypted by using the private key can only be decrypted by using the corresponding public key. [2]

Quantum cryptography:

The well known cryptographic difficulty is the transmission of secret messages. For solving this problem quantum cryptography is very helpful concept. Quantum cryptography is based on quantum mechanics concept which is used to do the key distribution in such a way that both parties cannot be compromised in security. This technique is called as **quantum cryptography** or **quantum key distribution.** Few years before people recognized that a quantum computer could be used to crack public key cryptography, on this problem they discovered a solution versus this quantum attack – quantum key distribution (QKD). QKD gives an unconditionally stable way to share out random keys across insecure channels. The secure key created by QKD could be further applied in the OTP system or further encryption algorithms to increase information security. [13][14]

II. LITERATURE REVIEW

The purpose of the RSA public key cryptosystem was from Diffie as well as Hellman, who initiated the technique of the exponential key exchange. Another symmetric key algorithm is Diffie-Hellman key exchange, following the RSA. However, the first ever recognized illustration of a corresponding system was made in 1973 by Cifford Cocks, a mathematician working at the GCHQ, a UK intelligence agency. The system was never set up examining the comparatively costly computers essential to execute it at the time. Since of its top-secret categorization, it was not up to, 1998 that his finding was disclosed. [3] Being the introductory specimen in history of the symmetric key cryptosystem and, worth nothing, the only type that has resisted more than three decades of attacks, the RSA has enhance the choice algorithm for tasks such as validating

 DOI : 10.35291/2454-9150.2019.0563

phone calls, encrypting credit-card , debit-card, online banking transactions over the Internet, providing Security to e-mail. The functions of the RSA sustained to improve, and to give their attempts, Rivest, Shamir, as well as Adleman got one of the highest awards in the area of mathematics. The security of RSA remains extensive center of cryptographic research, in theoretical and practical functions [4]. In this, Author differentiate the efficiency of an ECC with other cryptosystems also the homomorphism of various algorithms such as RSA, Paillier etc. [5] In this paper, Author states that an ECC is more structured than the extensive RSA based systems because ECC uses smaller key sizes for similar security. A relative analysis of ECC with RSA is made in terms of size of the key, computational potential, size of data files as well as encrypted files.[6]

III. RSA

RSA has enhance most widely utilized is because it authorizes either of the two keys to encode a message and the other key to decode it, consequently encouraging confidentiality, integrity, authenticity and non-reputability of data and e-communications [16][17]. The success of RSA algorithm comes from the fact that it's hard to computationally factor large integers into primes [15]. Multiplying the two primes is uncomplicated yet implementing the reverse in the form of factoring is actually difficult and obtains even harder as the values of p and q gets bigger [17].

RSA algorithm steps:

1. Generate two large prime numbers, p and q.
2. Let, m=pq
3. Let, m=Φ(n)=(p-1) (q-1)
4. Choose a small number e, coprime to m, with GCD (Φ(n), e) =1
5. Find d, such that de mod Φ(n)=1

IV. Elliptic Curve Cryptography

Elliptical curve cryptography (ECC) is one among the general public key encryption technique supported elliptic curve theory which will be wont to create faster, smaller, and more efficient cryptographic keys.[9]

Elliptic curves are extremely powerful new area of mathematics which has been immensely explored over the past few decades. They have shown enormous potential as a tool for solving tangled number problems and also for use in cryptography.[7]

Elliptic curve cryptography is based on the complexity of solving number problems involving elliptic curves. Elliptic curves are introduced so as they are illustrated by triple equations, similar to those used in the computations of ellipsis [10]. The general form of elliptic curve equation is:

b2 + cab + db = a3 + ea2 + fa + g

The below figure shows ECC curve:

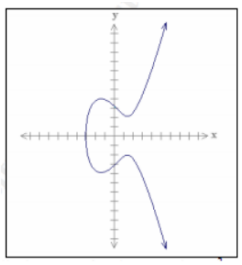

Fig 1: ECC Example
Source: sans.org

Elliptic curve cryptography was initiated by Neal Kolbitz and V Miller in 1985. Elliptic Curve Cryptography proposed as a substitute to found public key systems such as RSA and has recently acquired lot of awareness in academia as well as industry [11]. There is no sub exponential algorithm recognize to resolve the discrete logarithm problem on a suitably specify elliptic curve this is the important reason for the elliptic curve cryptography attractiveness. This signifies that essentially smaller parameters can be utilized in Elliptic Curve Cryptography than in other competitive systems like RSA but with same security extent. Elliptic curve cryptography having small key sizes key sizes includes reductions and faster calculations in storage space, bandwidth as well as processing power.[12] Elliptic curve cryptography improves the analysis and configuration of public key cryptographic designs that can be create using elliptic curves. The elliptic curve scheme analogues based on the discrete logarithm problems where the underlying group is the collection of points on an elliptic curve defined over a finite field.

There are two extensive reasons for using elliptic curves as a basis for symmetric key cryptosystems. The first causes are that the elliptic curve-based cryptosystems exist to provide better security than traditional cryptosystems for a given key size. One can take benefit of this fact is to develop security or to develop performance by lowering down the size of the key while keeping common security. The elliptic curve cryptosystem provides better security than conventional cryptosystem for a specified key size. Using this merit one can develop security or performance by reducing the key size while remain traditional security. Algebraic structure is the base of the elliptic curve cryptography that constructs cryptographic primitives which depend on a mathematical complex problem.[8]

V. CONCLUSION

In this paper reviewed all the above defined cryptography methods, it can be concluded that Elliptic Curve Cryptography is faster than RSA, because it uses smaller key. But its mathematical operation is very hard as compare to RSA. In Diffie-Hellman cryptography algorithm confidential keys are exchanged between two users. Whereas, quantum cryptography is combination with

 DOI : 10.35291/2454-9150.2019.0563

traditional secret key cryptography algorithms allow improving the confidentiality of information transmissions to a remarkable high level.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cryptography

[2] Ansah Jeelani Zargar , Mehreen Manzoor , Taha Mukhtar ,"ENCRYPTION/DECRYPTION USING ELLIPTICAL CURVE CRYPTOGRAPHY", International Journal of Advanced Research in Computer Science, Volume 8, No. 7, July – August 2017,ISSN:0976-5697

[3] Saranya, Vinothini, Vasumathi," A Study on RSA Algorithm for Cryptography ",(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5708-5709

[4] Abhijit Das, C. E. (2009). Public-Key Cryptography:Theory and Practice. Mumbai: Pearson Education India.

[5] Sigrun Goluch "The development of holomorphic cryptography" thesis presented to the Institute of Discrete Mathematics and Geometry Vienna University of Technology.]

[6] G.V.S. Raju and Rehan & bani" Elliptic Curve Cryptosystem and its Applications" published in 0-78037952-7/03/@ 2003 IEEE

[7] https://plus.maths.org/content/elliptic-cryptography Elliptic cryptography By Andrew Chambers Submitted by Marianne on July 20, 2015.

[8] Sujith Narayan," A Review On Elliptic Curve Cryptography", International Journal of Emerging Technology and Innovative Engineering Volume 4, Issue 12, December 2018 (ISSN: 2394 – 6598)

[9] H. R. Boveiri, M. Elhoseny, A-COA: an adaptive cuckoo optimization algorithm for continuous and combinatorial optimization, Neural Computing and Applications, (2018). https://doi.org/10.1007/s00521-018-3928-9.

[10] Abhijit Das," Elliptic-Curve Cryptography (ECC)", Department of Computer Science and Engineering Indian Institute of Technology Kharagpur, Second International Conference on Mathematics and Computing (ICMC 2015) Haldia, 5–10 January, 2015. https://cse.iitkgp.ac.in/~abhij/download/doc/ECC.pdf

[11]https://www.cse.iitk.ac.in/users/nitin/courses/WS2010-ref2.pdf

[12] Sneha Patil, Vidyullata Devmane," A review on Elliptic Curve Cryptography and Variant", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 05 | May-2018 , e-ISSN: 2395-0056, p-ISSN: 2395-0072.

[13] https://www.intechopen.com/books/theory-and-practice-of-cryptography-and-network-security-protocols-and-technologies/introduction-to-quantum-cryptography.

[14] C. Bennett and G. Brassard, in Proceedings of IEEE, International Conference on Computers, Systems.

[15] M. Preetha, M. Nithya, "A Study And Performance Analysis Of Rsa Algorithm", IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139, ISSN 2320–088X.

[16] Shireen Nisha, Mohammed Farik, "RSA Public Key Cryptography Algorithm – A Review", International Journal Of Scientific & Technology Research Volume 6, Issue 07, July 2017 ISSN 2277-8616.

[17] AnnapoornaShetty, Shravya Shetty K, Krithika K," A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm", International Journal of Innovative Research in Computer and Communication Engineering , Vol.2, Special Issue 5, October 2014, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 .

 DOI : 10.35291/2454-9150.2019.0563