IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138
INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A BREIF STUDY ON VARIOUS CRYPTOGRAPIC ALGORITHMS FOR DATA SECURITY

Mr.Shivansh Mishrar
B.Tech CSE, Department of CSE, CAET, Chandra Shekhar Azad University of Agriculture & Technology, Kanpur, Uttar Pradesh

Dr.J.Mahalakshmi
Assistant Professor, Department of Computer Technology, PSG College of Arts & Science , Coimbatore -14

Abstract- In today's era of digital world most of the activities and exchange of information are being carried out on the digital platforms. The factor jeopardizing on such platforms is the Data security while exchange done in open communication channel. One better solution for the issue is altering the data to unintelligible format. Cryptography can be defined as the method of protecting the data/information, using the codes so that the information can only be understood by the person to whom it is sent. Encryption and decryption is the process, where the data is converted and reverse to its original state using various algorithms and modes. It is categorized into two types: Asymmetric encryption and Symmetric encryption. The main difference between them is that in symmetric encryption the message is encrypted and decrypted using the same key, whereas in asymmetric encryption for encryption of message public key is used and for decryption of message private key is used. This article, covers the review of the Encryption algorithms advantages and limitations, so that the researchers may avail, the suitable algorithm for their research work

Keywords – Cryptography, Encryption, Decryption, Algorithms, Data Security, Data Breach.

I. INTRODUCTION

Cryptography ensures the security of the data, by converting it into some inarticulate form and protect the data from the intruders. Encryption is the process of converting the original message or data into another form so that the people with authorized access to that data can only access the information of that data. The original data or message is called plaintext and the converted data is called ciphertext. The process of converting the ciphertext back to plaintext is called decryption. For the process of conversion, a key is used which can be either public key or a private key.

Cryptography has three types, Asymmetric cryptography, Symmetric cryptography and Hash function. In asymmetric cryptography a pair of public and private keys are used for encryption and decryption of messages respectively. Elliptic, (Rivest, Shamir, Adleman)RSA algorithm, Diffie-Hellman key exchange, Digital Signature Algorithm (DSA) are some algorithms used for asymmetric encryption.

In symmetric cryptography only a single key also known as secret key is used for both encryption and decryption of messages. AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish are some algorithms used for symmetric encryption. Considering both asymmetric and symmetric encryption, it is seen that Asymmetric encryption is safer than symmetric encryption but the later seems to be faster.

Hash function is another type cryptography used in almost all security applications. Hash function is a mathematical algorithm that coverts data of arbitrary size into unique string of text of a fixed size. In hash function, there is no use of key instead a hash value with fixed length is calculated as per the length of pain text which is used for the recovery of the pain text.

This paper consists of an abstract, introduction, implementation and conclusion.

II. LITERATURE REVIEW

Table 1. provides a review of the research conducted in past five years based on algorithms used in the symmetric and asymmetric cryptography.

Table 1: Pros and cons of algorithms used in cryptography

S.No.	Year	Author	Proposed Algorithm(s)	Pros	Cons
1.	2016	Kumar &Ragupathy	Symmetric and Asymmetric cryptography	Concentrates on the key selection for the encryption and decryption of the text.	Though key section plays a vital role in cryptography but the selection of a robust algorithm that consumes less memory is also important.
2.	2016	Patil et.al.	DES, 3DES, AES Blowfish and RSA	Concentrates on the analysis of the different algorithms so that they find the most suitable ground of implementation.	Though the blowfish algorithm requires less memory but it is not strong enough to provide authentication as well as non-repudiation as two people have the same key and AES algorithm, being very easy to implement is not robust as it uses too simple algebraic structure.
3.	2016	Senthilkumaran et.al.	Elliptic Curve Cryptography (ECC) and Identity-Based Cryptography (IBC)	Concentrates to find the effective implementation and fix the problems of asymmetric key cryptography in wireless sensors network.	Though attempts are made to create a strong encryption, but the use of IBC is not robust because if the key generator is compromised then the entire security is at risk.
4.	2016	Sghaier et.al.	Elliptic curve cryptography (ECC)	Concentrates on the hardware building for the implementation of modular multiplication and inversion in order to reduce the encryption time of ECC.	Though the encryption time is bit reduced but the memory consumption is high because of the increased size of the ciphertext than that of plaintext.
5.	2017	Henriques&Vernekar	Symmetric and Asymmetric cryptography	Concentrates on small size of the ciphertext and consumption of less memory by making a combination of the concepts of symmetric and asymmetric cryptography.	Though the combination of the concepts of symmetric and asymmetric cryptography decreases the size and memory consumption of the ciphertext but it may case the high loss in case the key is decoded.
6.	2017	Luo et.al.	Modular multiplication algorithm (MMA)	Concentrates on the most efficient utilization of the memory so that high density data can accurate with zero leakage and also to accelerate the modular multiplication.	The use of MMA is made due to which the output polynomial is in different redundant representation than the inputs, which makes it inefficient for modular acceleration.
7.	2017	Mahagaonkar&Dongre	Elliptic Curve Discrete logarithm Problem (ECDLP)	Concentrates on making a secure and well organized, systematic communication model for Vehicular AdhocNetworks.	Although there exists some computational complexity.
8.	2017	Maqsood et.al.	DES, AES, RSA and Elgamal	Concentrates on the performance of the algorithms to find the most robust algorithm.	Though the Elgamal algorithm provides security but the ciphertext is too long as compared to the plaintext, i.e., twice the length of the plaintext.
9.	2017	Sa'adah et.al.	RSA algorithm	Concentrates on the security scheme that can provide the secure multi-antenna transmission in fading channel by the implementation of Multiple Input Multiple Output– Orthogonal Frequency Division Multiplexing (MIMO-OFDM) system that is synchronized with RSA algorithms.	Though with the use of RSA algorithm the performance of MIMO-OFDM, do not degrade but it can be very slow when the large amount of data is needed to be encrypted by the system.

10.	2017	Sharma & Gupta	RSA algorithm	Concentrates on the analysis of the RSA algorithm so that a stronger encryption system can be build.	Though RSA algorithm provides a strong encryption system, but it is very slow when a large amount of data is to be encrypted.
11.	2017	Sridhar &Smys	Lattice-based cryptography	Concentrates on building a secure encryption system that can be protected from the quantum algorithm attacks.	Though the system uses fake packets in order to protect from quantum attacks, but it made the computation speed much slow.
12.	2017	Timothy &Santra	Blowfish, RSA, and SHA-2 algorithms.	Concentrates on building a strong encryption system by making a combination of Blowfish, RSA, and SHA-2 algorithms.	Though making a combination of Blowfish, RSA, and SHA-2 algorithms makes a robust encryption system, but using SHA-2 leads to the compatibility problems as many OS don't support SHA-2 algorithms.
13.	2017	Zhao et.al.	RSA algorithm	Concentrates on overcoming the problems of optical asymmetric cryptosystem with the implementation of modified RSA algorithm.	The use of the modified RSA algorithm leads to the requirement of third party for the verification of public key, which may lead to insecurity of public key.
14.	2018	Khan et.al.	RSA algorithm	Concentrates on the authentication and the confidentiality of the information during its transportation by using the private key as well as the public key and implementing the RSA algorithm.	Inspite of the implementation of the RSA algorithm, it is still not safe enough as first the use of private key is made for encryption and then the public key, and the disadvantage of using the private key is that it requires anyone new to gain the access to the key which makes it insecure.
15.	2018	Li et.al.	Elliptic curve cryptography (ECC)	Concentrates on the reduction of the computation time of the machine by the use of the tag radio frequency identification (RFID).	Though the computation time is being reduced by the used of tag RFID but using the RFID is very expensive which will also increase the cost of the system.
16.	2018	Santoso et.al.	BlowFish, DES AES, RSA, DSA and Diffie-Hellman	Concentrates on the comparison of the different cryptographic algorithms in order to find the most effective algorithm.	In the algorithm used, the DSA and Diffe-hellman lacks in authentication process which makes it not strong enough.
17.	2018	Su et.al.	Phase-truncated Fresnel transform (PT-FrT) and discrete wavelet transform (DWT)	Concentrates on the greyscale image encoding and a watermarking scheme - as the greyscale watermark is first encoded into a noise like pattern by using PT-FrT and then is embedded into the greyscale host image's texture by DWT fusion approach.	The use of DWT may lead to high computational complexity and time consumption because in DWT, the main problem is choosing the right mother wavelet and the number of decomposition levels.
18.	2019	Almajed&Almogren	Elliptic Curve Cryptography (ECC)	Concentrates on providing secure and efficient encoding scheme for wide range of devices by using ECC to prevent them from several encryption attacks.	Though ECC consumes less power, but it is not strong enough as its implementation is complicated and tricky mainly the standard curves and the public key operations are slow with it.
19.	2019	Easttom	NTRU encryption, The GoldreichGoldwasserHalevi (GGH) and Learn with Error (LWE)	The use of NTRU, GGH and LWE algorithms are made for the Lattice-based cryptography, hence providing a strong security due to the presence of the algorithms like LWE and NTRU.	Though the algorithm used are robust but the GGH algorithm is not much secure and it requires more comparative study of lattice-based algorithms of the existing cryptanalysis data.

20.	2019	Panhwar et.al.	The Advanced Encryption Standard (AES), The Data Encryption Standard (DES), and 3-DES	Concentrates on the implementation of the AES over the DES and 3-DES on the basis of speed, computation time and the memory consumption.	Though the AES provides good speed, less memory and computation time but still it is not a robust encryption as is uses very simple algebraic structure and flows the same encryption pattern.
21.	2019	Uppu et.al.	Asymmetric cryptography	Concentrates on making a unclonable key in order to achieve a high security cryptography.	Though making a unclonable key increases the security but it also increases the computation time for the bulk messages.
22.	2019	Verma et.al	phase-retrieval algorithm and phase- truncated Fourier transforms (PTFT)	Concentrates on the authentication of the person who receives the ciphertext to decrypt the input information by use of biometric key. It also generates the decryption key during the PTFT encryption which is not related to any visual input information that is carried out.	Though the use of biometric key will help in decryption by the authenticate person, but still the algorithm is not strong enough to protect the data, as the attacker can alter the pixel pattern or and alter with the biometric key pattern.
23.	2020	AlMajed&AlMogren	Elliptic curve cryptography (ECC)	Concentrates on the establishing a secure WSN in IOT by the use of ECC encryption encoding.	Though ECC is used for providing a secure encryption but is increased the size of the encrypted message and ECC being complex, its implementation is not easy which causes error implementation.
24.	2020	Saho &Ezin	Elliptic Curve Integrated Encryption Scheme (ECIES), Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Nyberg-Rueppel (ECNR) and RSA.	Concentrates on finding the effective alternative of RSA that uses shorter key size and provides the same level security.	Though it provides security but it takes time for the authentication of the user as the use of ECDSA is made which requires a lot of time for authentication and the verification process.
25.	2020	Singh & Sharma	Elliptic curve cryptography (ECC)	Concentrates on the effective use and performances of the elliptic curve cryptography by involving the algebraic mathematics.	The implementation of ECC is complicated and tricky specially for the standard curves and also increase the size of the encrypted message.

III.CONCLUSION

In this paper, we study about the pros. and cons. of the various algorithms used for data encryption. Using these algorithms, we can attain a highly security to our data and will also choose the algorithm that is fast enough for encryption and decryption of the data. This paper will be beneficial for the beginners and help the new researcher for their research work.

Acknowledgement:

The Author expresses their gratitude to the MentX Summer Internship Offered by the Young Academy of India, to carry out the Research Work.

REFERENCES

[1] AlMajed, H. N., &Almogren, A. S. (2019). SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography. IEEE Access,7. doi:10.1109/access.2019.2957943.

[2] AlMajed, H.N., &AlMogren, A.S. (2020). A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things. Sensors, 20(21), 6158. MDPI AG. Retrieved from http://dx.doi.org/10.3390/s20216158

[3] Easttom, C. (2019). An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives, 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0811-0818, doi: 10.1109/CCWC.2019.8666459.

[4] Henriques, M. S., &Vernekar, N. K. (2017). Using symmetric and asymmetric cryptography to secure communication between devices in IoT, 2017 International Conference on IoT and Application (ICIOT), pp. 1-4, doi: 10.1109/ICIOTA.2017.8073643.

[5] Khan, A., Basharat, S., &Riaz, M. (2018). Analysis of asymmetric cryptography in Information security based on computational study to ensure confidentiality during information exchange. International Journal of Scientific & Engineering Research, 9(10). 10.13140/RG.2.2.30495.61602.

[6] Kumar, M.V., &Ragupathy, U.S. (2016). A Survey on current key issues and status in cryptography. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 205-210.

[7] Li, Z., Zhao, H., Su, X. & Wan, C. (2018). Asymmetric Cryptography Based Unidirectional Authentication Method for RFID. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 374-3743, doi: 10.1109/CyberC.2018.00073.

[8] Luo, T., He, B., Zhang, W., &Maskell, D. L. (2017). A novel two-stage modular multiplier based on racetrack memory for asymmetric cryptography. IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 276-282, doi: 10.1109/ICCAD.2017.8203789.

[9] Mahagaonkar, S. V. &Dongre, N. (2017). TEAC: Timed efficient asymmetric cryptography for enhancing security in VANET. International Conference on Nascent Technologies in Engineering (ICNTE), pp. 1-5, doi: 10.1109/ICNTE.2017.7947968.

[10] Maqsood, F., Ahmed, M., Mumtaz, M., & Shah, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080659.

[11] Panhwar, M.&AliKhuhro, S.,Panhwar, G., & Ali, K. (2019). SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms. International Journal of Computer Science and Network Security, 19(1)

[12] Patil, P., Narayankar, P., Narayan D.G., &Meena S.M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science, 78, 617–624. doi:10.1016/j.procs.2016.02.108

[13] Sa'Adah, N., Astawa, I. G. P., &Sudarsono, A. (2017). Asymmetric cryptography for synchronization on MIMO-OFDM system, 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), pp. 57-62, doi: 10.1109/ELECSYM.2017.8240379.

[14] Saho, N.J.G. &Ezin, E.C. (2020). Survey on Asymmetric Cryptographic Algorithms in Embedded Systems. International Journal of Innovative Science and Research Technology, 5(12)

[15] Santoso, P.P., Rilvani, E., Trisnawan, A.B., Adiyarta, K., Napitupulu, D., Sutabri, T., Robbi, R. (2018). 2nd Nommensen International Conference on Technology and Engineering IOP Conf. Series: Materials Science and Engineering, 420, 012111. doi:10.1088/1757-899X/420/1/012111

[16] Senthilkumaran, U., Nallakaruppan, M., &Senthilkumar, M. (2016). Review of Asymmetric Key Cryptography in Wireless Sensor Networks. International Journal of Engineering and Technology (IJET), 8(2).

[17] Sghaier, A.,Zeghid, M.,Massoud, C. &Machhout, M. (2016). Proposed unified 32-bit multiplier/inverter for asymmetric cryptography. 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 109-112, doi: 10.1109/SETIT.2016.7939851.

[18] Sharma, S.& Gupta, Y. (2017). Study on Cryptography and Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 02(01).

[19] Singh, S., & Sharma, A. (2020). Cryptosystems in Asymmetric Cryptography for Securing Data at various Level. Journal of Technology and Engineering Sciences, 4(2), 3-15.

[20] Sridhar, S.&Smys, S. (2017). Intelligent security framework for iot devices cryptography based end-to-end security architecture. International Conference on Inventive Systems and Control (ICISC), pp.1-5, doi: 10.1109/ICISC.2017.8068718.

[21] Su, Y., Tang, C., Li, B., Qiu, Y., Zheng, T., & Lei, Z. (2018). Greyscale image encoding and watermarking based on optical asymmetric cryptography and variational image decomposition. Journal of Modern Optics, 1–13. doi:10.1080/09500340.2018.1530387

[22] Timothy, D. P. &Santra, A. K. (2017). A hybrid cryptography algorithm for cloud computing Security. International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), pp. 1-5. doi: 10.1109/ICMDCS.2017.8211728.

[23] Uppu, R., Wolterink, T. A. W., Goorden, S. A., Chen, B., Škorić, B., Mosk, A. P., &Pinkse, P. W. H. (2019). Asymmetric cryptography with physical unclonable keys. Quantum Science and Technology, 4(4), 045011. doi:10.1088/2058-9565/ab479f

[24] Verma, G., Liao, M., Lu, D., He, W., Peng, X., & Sinha, A. (2019). An optical asymmetric encryption scheme with biometric keys. Optics and Lasers in Engineering, 116, 32–40. doi:10.1016/j.optlaseng.2018.12.010

[25] Zhao, T., Jiang, Y., & Liu, C. (2017). Demonstration and a practical scheme of the optical asymmetric cryptosystem. Optik, 138, 509–515. doi:10.1016/j.ijleo.2017.03.013