International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1126-1130 www.ijaem.net ISSN: 2395-5252

Hybrid Cryptographic Techniques for Information Security : A Survay

Ms. Bhavna Sahu, Mr. Vaibhav Chandrakar
Central College of Engineering & Management Kabir Nagar, Raipur
Central College of Engineering & Management Kabir Nagar, Raipur

Submitted: 25-06-2021 Revised: 04-07-2021 Accepted: 07-07-2021

ABSTRACT— Secure communication is required in order to permit sensitive data transfer between any sender and recipient. The security of shared information over an open channel has become an essential challenge, and consequently data secrecy, authentication and integrity are needed. Information protection is the way to protect information from unwanted access. Cryptographic procedures are used to ensure that data is sent securely. Almost all cryptosystems are vulnerable to various types of cryptographic assaults. Therefore, it is necessary to encrypt the gadget if you use variants of cryptographic methods. Algorithm hybridization is a valuable scheme that offers solutions to several major communication network issues. The characteristics of the algorithms used in hybrid cryptography are thus described in a thorough study of different hybrid cryptosystems suggested by various researchers.

Keywords - hybrid cryptosystem, symmetric key cryptography, public key cryptography, hash algorithm

I. INTRODUCTION

Information security research review draws many researchers because of its significance in the increasing area of electronic communications. Significant volumes of classified information are also shared between computers via public contact services, such as health and legal documents, financial transactions and credit scores, and these communications must be kept secret and secured from manipulation. Cryptography deals with the transformation of plaintext by encryption into cypher text and the transformation of cypher text by decryption back into plaintext. It guarantees anonymity, confidence, access control in e-payments, e-voting, corporate protection and in many other applications.

Symmetric and asymmetric algorithms and hash functions are all used together in the majority of cryptographic implementations of functional systems. This is known as the dual system. The explanation for the use of both algorithm families is that each has particular strengths and disadvantages. Symmetric cyphers are considerably quicker, at least 1000 times faster than asymmetric cyphers, but both parties are expected to share the key somehow.

The science and art of protecting messages is cryptography[1]. It is the analysis of mathematical methods relating to information security aspects, such as secrecy, privacy of records, authentication, and usability. During transmission or storage, it is the scrambling of the content of the data, such as text, image, audio, video and so on, to make the data unreadable or meaningless. The mechanisms used to encrypt messages represent the field of research referred to as cryptography. Cryptanalysis, on the other hand, is the science and art of cracking the cipher[2]. It is used, even though the cryptographic key is unknown, to breach cryptographic security mechanisms to obtain access to the contents of encrypted messages. In three groups, cryptographic algorithms are roughly classified:

A. Secret Key Cryptography: A single key is used in this method of cryptography technique. To encrypt a message, the sender applies a key while the recipient applies the same key to decode the message. Since only a single key is used, it is called symmetric encryption or cryptography of the private key[3].

B. Public Key Cryptography: Two keys are used in this form of cryptographic strategy. For encryption, one key is used and the other is for decryption. This method is also known as asymmetric encryption since a pair of keys is implemented here. Each party has a private key and a public key in this operation. Although the public key is exchanged with all those with whom we wish to connect, the private is kept confidential and is not exposed.

C. Hash Functions: Any function that can be used to map arbitrary size data to fixed size data is a hash function. The values that a hash function returns are called hash values, hash codes, or just hashes. A cryptographic hash function allows one to quickly check that a given hash value is mapped to any input information. But it is impossible to recreate it by understanding the stored hash value if the input data is unknown. This is used to ensure the confidentiality of the data transmitted.

II. HYBRID CRYPTOGRAPHY

Hybrid encryption is an encryption mode that merges two or more methods of encryption. To gain from the strengths of each type of encryption, it combines a mixture of asymmetric and symmetric encryption. These strengths are known as speed and defence, respectively. Hybrid encryption, as long as the public and private keys are completely secure, is considered a highly secure form of encryption. One that combines the convenience of an asymmetric encryption method with the effectiveness of a symmetric encryption system is a hybrid encryption scheme. There are different benefits of the combination of encryption techniques. Users then have the option to use hybrid encryption to connect. Asymmetric encryption will slow down the method of encryption, but all modes of encryption are improved by the simultaneous use of symmetrical encryption. The consequence is the additional protection of the transmission process along with better machine efficiency overall.

The primary purpose of this paper is to research and analyse the benefits of Hybrid Cryptography. Securing the sharing of data over the internet and the local preservation of sensitive data is essential. Authenticated correspondence over untrusted networks is enabled by cryptography, as long as the hidden keys are not exposed. Attacks by hackers and insiders, however, often reveal confidential keys. Such break-in attacks also only control the devices for a short amount of time and, thus, protection can be restored, provided that new keys can be chosen and specifically implemented. As the contamination can remain undetected, this constructive recovery operation must be invoked regularly. The advent of the era of information technology was so sudden that we have not yet been able to deal with all the changes or with many of the ramifications. More and more people are concerned about the issue of privacy in an age in which virtually everything we do is recorded somewhere in a computer system and communicated through some electronic means. Fig. 1 depicts the basic model of a hybrid cryptosystem.

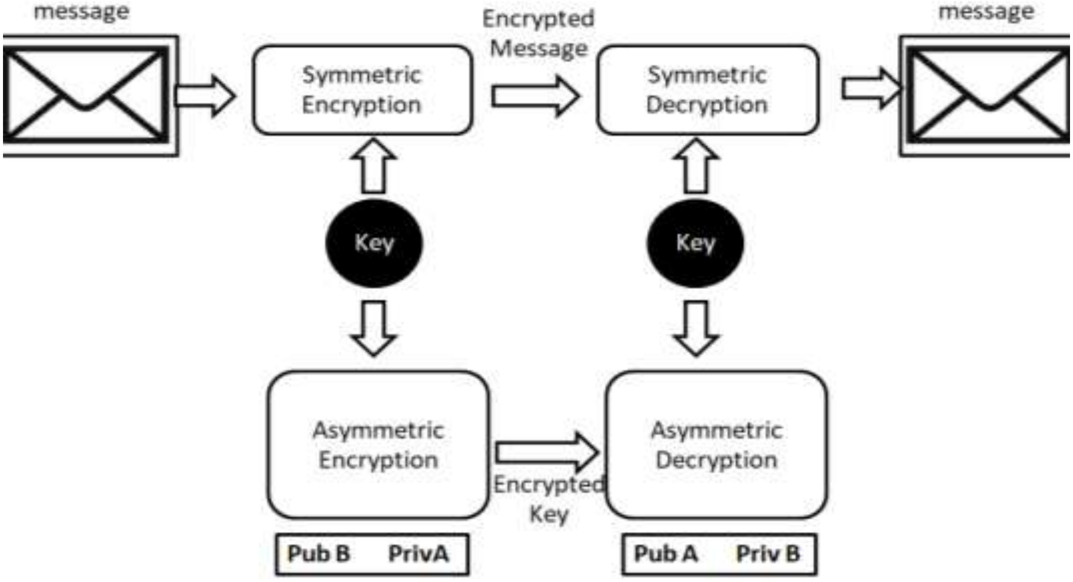

Figure 1- Hybrid Cryptosystem

III. SOME IMPORTANT ALGORITHMS USED IN HYBRID CRYPTOGRAPHY

A. DES (Data Encryption Standard)

One of the first commercially developed cyphers is the Data Encryption standard. DES is a block cypher that encrypts 64-bit data blocks, and a 56-bit secret key[4] is used to encrypt the data. DES is consisting of sixteen rounds and two layers of permutation. A mutual key is used by DES both to encrypt and decode the message. The method of decryption is the opposite of the process of encryption. DES has a potent Avalanche effect and is robust as it runs in CBC, ECB, CFB and OFB modes. DES is prone and comparatively sluggish to Blunt Force attack.

B. AES (Advanced Encryption Standard)

The 128 bit data block can be processed by AES and uses main lengths of 128, 192, or 256 bits. AES can be referred to as AES-128, AES-192, and AES-256 for the key lengths of 128,192 and 256 bits, respectively. AES, unlike DES, does not have a group system. The number of rounds in AES depends on the key length, i.e. the number of rounds is 10 with a key length of 128, and equally for 192 and 256 bit keys, 12 and 14 respectively. AES promises resistance, easy architecture and good processing speed against all established threats.

C. RSA (Rivest, Shamir and Adleman)

In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman developed a public key encryption algorithm. It was the first algorithm proven to be sufficient for both signing and encryption, and one of the first significant developments in the encryption of public keys. It is also commonly used in protocols for electronic commerce, and its protection is believed to rely on the complexity of large numbers decomposing. RSA is protected because it is capable of overcoming concerted assault.

D. Diffie-Hellman Key Exchange Algorithm

In 1976, Whitfield Diffie and Martin Hellman discovered the first public key algorithm ever developed, the Diffie-Hellman (DH) algorithm. Diffie-Hellman creates a mutual secret key that can be accessed when sharing data over a public network for secret communications. Before communication starts, the Diffie-Hellman algorithm does not require any known key and the Discrete Logarithm problem makes it incredibly difficult to crack. The algorithm of Diffie-Hellman is vulnerable to a man-in-the-middle attack.

E. Elgamal Algorithm

Taher El-Gamal, which is based on the Discrete Logarithm Problem and Diffie-Hellman key exchange, invented the Elgamal algorithm. Elgamal can be used both for encryption and digital signature purposes. It supplies a separate ciphertext if the same plaintext is encrypted. Elgamal has the downside of making the plaintext double the size of the ciphertext.

F. DSA (Data Signature Algorithm)

David Kravitz invented the Data Signature Algorithm. In 1991, the National Institute of Standards and Technology (NIST) adopted the Digital Signature Standard (DSS) using DSA. DSA protection is focused on the complexity of overcoming discrete logarithms. DSA has been popularly embraced. More efficient and quicker than RSA is DSA.

G. ECC (Elliptic Curve Cryptography)

Koblitz and Miller independently introduced the use of elliptic curves in public key cryptography in 1985, and since then, a significant amount of work has been performed on elliptic curve cryptography. Point addition and point doubling are the basic EC operations. It was not possible to find simple multiplication in the case of elliptic curves. A single point implies that A(x,y) on the elliptical curve will produce a resulting point B(x',y ') by adopting a sequence of adding points and doubling points instead of multiplying point A directly with a scalar, thus A=zB, where z is a multiple scalar. In reality, symmetric key algorithms and algorithms for public key cryptography are typically mixed together. For the sake of greater efficiency and accuracy, integrating the functionality of two algorithms is known as Hybrid cryptography.

Algorithm hybridization is a valuable scheme that offers solutions to several major communication network issues. A modern hybrid cryptographic algorithm can result in the deployment of the positive points of an algorithm into other less powerful algorithms. An overview and study of various algorithms used in hybrid cryptography is carried out by evaluating research papers by different scientists and provided in Table 1.

IV. ANALYSIS OF DIFFERENT ALGORITHMS AND THEIR ADVANTAGES

TABLE 1 Analysis of algorithms used in hybrid cryptography

Reference	Hybrid Method	Remark
[4]	Huffman coding, hierarchical encryption technique	high robustness, low computation time, high data embedding capacity
[5]	AES, LSB	Increased security as text embedded in the wavelet transformed image
[6]	ECC, AES, XOR Dual RSA, MD5	Better security, reduced processing overhead, lower energy consumption

[7]	Caesar Cipher, DES	More secured, maintaining the confidentiality of data
[8]	Enhanced symmetric key algorithm	More efficient for large data, better speed, less overhead
[9]	DES, RSA	Two levels of security i.e. hybrid cryptography and steganography are combined together. BPCS approach is used to decide embedding byte positions.
[10]	DES(Triple DES with 168bit key) with RSA and SHA-1 with DSS	Triple DES for confidentiality, RSA for key management and SHA-1 for data integrity.
[11]	RSA cryptography	Transformation of personal information from plaintext to cipher text can be done and client's privacy is preserved.

V. CONCLUSION

One of the main problems faced by information protection is secrecy. Via cryptographic encryption techniques, during signal transmission, one may prevent a third party from understanding transmitted raw data over an unsecured channel. Through analyzing different algorithms that make use of the idea of hybrid cryptography, this paper attempted to add to the general body of knowledge in the field of cryptography. It can be argued that cryptographic aims such as secrecy, transparency and authenticity can be accomplished using hybrid cryptographic techniques, considering the increased computational complexity.

REFERENCE:

[1] B. Forouzan, Cryptography and Network Security. McGraw-Hill, 2007.

[2] C. Paar and J. Pelzl, Understanding Cryptography. Berlin Heidelberg: Springer-Verlag, 2010, pp. 3-9, 30-31.

[3] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. Wiley, 1996, pp. 233-263.

[4] N. Tayal et al., A Novel Hybrid Security Mechanism for Data Communication Networks, Multimed Tools Appl, vol. 76, no. 22. Springer, 2017, pp. 24063-24090.

[5] M. Indra et al., "Secured data transmission using wavelet based steganography and cryptography by using AES algorithm, procedia," Comput. Sci. Elsevier, vol. 85, pp. 62-69, 2016.

[6] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," J. Electr. Syst. Inf. Technol., vol. 2, no. 3, pp. 296-313, 2015 [doi:10.1016/j.jesit.2015.11.005].

[7] K. Goodarzi and A. Karimi, "Cloud computing security by integrating classical encryption, procedia," Comput. Sci. Elsevier, vol. 42, pp. 320-326, 2014.

[8] K. K. Pandey et al., "An enhanced symmetric key cryptography algorithm to improve data security," Int. J. Comput. Appl., vol. 74, pp. 29-33, 2013.

[9] S. P. Bansod et al., "Modified BPCS steganography using Hybrid cryptography for Nishtha Mathur and Rajesh Bansode, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, Procedia," Comput. Sci. Elsevier, vol. 79, pp. 1036-1043, 2016.

[10] L. D. Singh and K. M. Singh, "Implementation of text encryption using elliptic curve cryptography,procedia," Comput. Sci. Elsevier, vol. 54, pp. 73-82, 2015.

[11] improving data embedding capacity Intl. Conf. on Commun., Information & Computing Technol. (ICCICT), vol. 2012, 2012, pp. 1-6.

[12] L. Wang and Yonggui Zhang, A New Personal Information Protection Approach Based on RSA Cryptography. IEEE, 2011.

[13] "Shankar Dhakar, Ravi & K. Gupta, Amit & Sharma, Prashant, modified RSA encryption algorithm (MREA)" 2nd Intl. Conf. on Adv. Comput. and Commun. Technol.(ACCT), vol. 2012, 2012, pp. 426-429.

[14] A. Abdul-Aziz Gutub and F. Abdul-Aziz Khan, "Hybrid crypto hardware utilizing symmetric-key & public-key cryptosystems"

Intl. Conf. on Adv. Comput. Sci. Appl. and Technol. IEEE, 2012, pp. 116-121.

[15] S. Gupta and J. Sharma, “A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman” Intl. Conf. on Comp. Intell. and Comput. Res. IEEE, 2012.

[16] J. Zhang and Xuling Jin, “Encryption system design based on des and SHA-1” 11th Intl. Symp. on Distrib. Comput. and Appl. to Bus., Engineering & Science. IEEE, 2012, pp. 317-320.