IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115142

Various Techniques Used in Cryptography

Vishakha R. Agalawe[1], Nihal B. Jiwane[2], Ashish B. Deharkar[3]

Student, Computer Science & Engineering Department, Shri Sai College of Engineering & Technology, Bhadrawati, Chandrapur, M S India [1]

Assistant professor, Computer Science & Engineering Department, Shri Sai College of Engineering & Technology, Bhadrawati ,Chandrapur, M S India[2]

Assistant professor, Computer Science & Engineering Department, Shri Sai College of Engineering & Technology, Bhadrawati ,Chandrapur, M S India [3]

Abstract: Security plays a vital role in protecting the valuable data or information from the unauthorized access and its misuse.one of the most discussed technique for insuring data security is “cryptography”. Cryptography provides the secure communication in the presence of malicious third parties. This paper mainly focuses on the role of cryptography in data security and discussed some of the popular techniques used in cryptography.

Keywords: Cryptography , Encryption, Decryption, Data security.

I. INTRODUCTION

The term security has wide meaning. Security is nothing but a dealing with the prevention and detection of unauthorized actions by users. One of the most important method for data security is “cryptography”. Cryptography protects vulnerable data from unauthorized access. Cryptography derived from the name from a Greek word called ‘kryptos’ which means ‘hidden secrets’. Practice and study of hiding information is known ‘cryptography’. It is the technique of converting plain text into cipher text and again retransforming that cipher text into its original form.

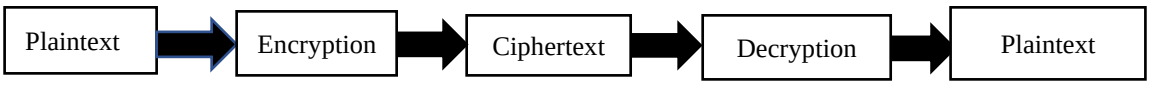

Fig 1. Cryptography

Terms used in cryptography:

1. Plain text: it is original message or the message that is not encrypted.
2. Ciphertext: it is the text that is not easily understand wihout decrypting it and is not in the easily readable form.
3. Encryption: it is the technique that is used in cryptography. Encryption is the technique that is used to convert the plain text into cipher text. It is used for keeping the senders data confidential.
4. Decryption: it is the process that converts encoded or encrypted data i.e cipher text to plain text.
5. Cryptanalysis: it is the process of understanding cipher text, cipher and cryptosystem is used for finding out the vulnerabilities or weaknesses present in them so that its key nobody should understand the plain text.
6. Key: key is a piece of information that is used to convert plain text to the cipher text .key specifies how output can be taken.

Types of cryptography:

In general there are two basics types

1. Symmetric key cryptography: for both encryption and decryption same key is used, there is a used of single common key to encrypt and decrypt messages. Symmetric key systems are faster and simpler but the problem is that sender and receiver somehow exchange key in secure manner example of symmetrical algorithm are data encryption standard (DES), triple-DES (3DES), blowfish and AES.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115142

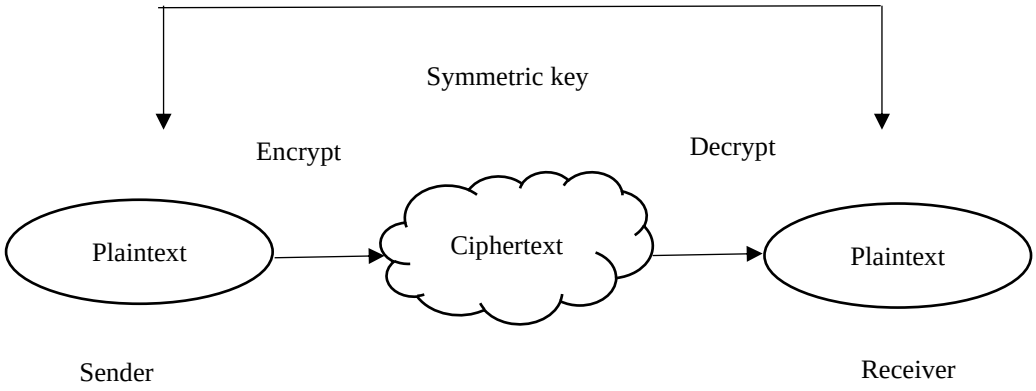

Fig 2 symmetric key cryptography

2. Asymmetric key crytography: under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encrypted plain text and a private key is used for decrypt cipher text to plain text.public key and private key both are different.even if the public key is known by third party or unauthorized person then in that case also intended receiver can only decode it because he alone knows the private key.example of asymmetric algorithm are RSA, ECC, DSA etc.

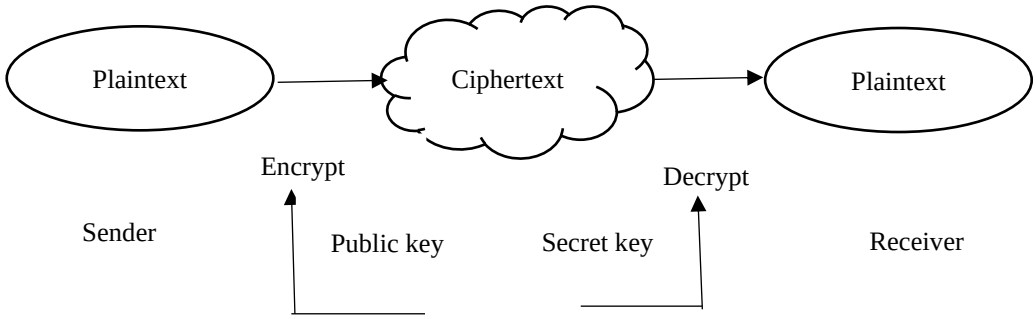

Fig 3 Asymmetric key cryptography

There are four main goals in cryptography

1. Authentication: the process of one's identity. (The primary forms of host-to-host authentication on the internet today are named-based or address-based of which are notoriously weak.)
2. Confidentiality: ensuring that no one can read the message except the intended receiver.
3. Integrity: assuring the receiver that the received message has not been altered in any way from the original.
4. Non-repudiation: a mechanism to prove that the sender really sent this message.

Symmetric key algorithm technique

1. Data encryption standard (DES): at the start of the 1970's the IBM team created a symmetric key cipher block algorithm known as DES algorithm. The DES algorithm takes the plain text of 64- bit as input and produces a ciphertext of 64-bit using a key of 56 bits. The DES was discovered vulnerable to powerful attacks and hence has slightly declined in use. Some benefits of DES are DES was developed in 1977 to run on hardware. Hence, this algorithm works fast in hardware. DES is relatively easy to implement because of its feistel structure and basic or uncomplicated logic. By reversing the order of 16 round keys the same algorithm is used for encryption and decryption. And the limitations are the total number of 16 round in DES makes the algorithm complex. DES was mainly designed for hardware so its runs

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022
DOI: 10.17148/IJARCCE.2022.115142

relatively slow on software compared to hardware. The 56-bit key length used in DES makes possible to encrypted code with modern technologies. Moreover, it can be broken using brute-force attacks and linear cryptanalysis. Hence AES (advanced encryption standard) has replaced the DES (data encryption standard).

2. Advanced encryption standard (AES): advanced encryption standard (AES) is a specification for the electronic data established by the U.S national institute of standard and technology (NIST) in 2001.AES is widely used as it is a much stronger than DES and triple DES despite being harder to implement. Advantages of AES are as it is implement in both hardware and software, it is most robust security protocol. It uses higher length key sizes such as128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking. Disadvantages of AES it uses too simple algebraic structure. Every block is always encrypted in the same way.

Asymmetric key algorithm technique

1. RSA (rivest-shamir-adleman): is a public key cryptosystem that is widely used for secure data transmission it is one of the oldest. The encryption key is public and distinct from the decryption key, which is kept secret (private). The security of RSA relies on the practical difficulty for factoring the product of two large prime number, the "factoring problem". Advantages of RSA are, it is very easy to implement, this algorithm is safe and secure for transmitting confidential data. Cracking RSA algorithm are it may fail sometimes because for complex encryption both symmetric and asymmetric encryption is required and RSA uses symmetric encryption only. It has slow data transfer rate due to large numbers involved. High processing is required end for decryption.
2. Digital signature algorithm (DSA): DSA stand for digital signature algorithm. DSA used for digital signature and its verification. It is based on mathematical concept modular exponentiation and discrete logarithm. It was developed by national institute of standard and technology (NIST) in 1991. Advantages of DSA are after signature verification, the sender cannot claim to have not sent the data. Data modification during transmission prevents final verification or message decryption. Right private /public combination help verify sender origin. Disadvantages of DSA are high cost to get started.

II.CONCLUSION

The whole point of cryptography is to secure information from third party. We use different types of algorithm to establish security services in different mechanism. The information security can be easily achieved by using cryptography techniques. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. If we want to send message quickly we use private key cryptography or public key cryptography. If we want to send message secretly we use public key algorithm. Secure communication, the most obvious use of cryptography, and the one all of us use frequently, is encrypting communication between us and another system.

ACKNOWLEDGEMENT

I would like to thank to the department of computer science & Engineering for providing guidance, useful and practical suggestions and technical support for research environment to accomplish this work.

REFERENCES

1. C.P pfleeger, S.L. pfleeger and J. Margulies, security in computing New Jersey prentice hall, 2015.
2. M. mushtaq faheem, S. Jamel,, Hassan disina, Z. A. pindar, N. shafinaz ahmad shakir, and M.. Mat deris "A survey on the cryptographic encryption algorithm", Int. J. Adv. Compute. Sci. Appl., 8(11), 2017, pp. 333-344.
3. Ashish B. Deharkar: https://ijarcce.com/papers/cloud-computing-based-on-predictive-acknowledgement-system/
4. . D. Costinela-Luminita, "Information security in e-learning platforms," Procedia - Soc. Behav. Sci., 15, 2011, pp. 2689-2693.
5. .R. Kumar, and C. C. Rabindranath, "Analysis of Diffie Hellman Key Exchange Algorithm with proposed Key Exchange Algorithm," Int. J. Emerg. Trends Technol. Compute. Sci., 4(1), 2015, pp. 40-43.
6. S. Karthik, and A. Muruganandam, "Data Encryption and Decryption by using Triple DES and performance analysis of crypto system," Int. J. Sci. Eng. Res., 2(11), pp. 24-31, 2014.
7. V. Agrawal, S. Agrawal, and R. Deshmukh, "Analysis and review of encryption and decryption for secure communication," Int. J. Sci. Eng. Res., 2(2), 2014, pp. 2347-3878.
8. V. Sukhraliya, S. Chaudhary, and S. Solanki, "Encryption and Decryption Algorithm using ASCII values with substitution array approach," International Journal of Advanced Research in Computer and Communication Engineering, 2(8), 2013, pp. 3094-3097.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022
DOI: 10.17148/IJARCCE.2022.115142

9. V. K. Mitali, and A. Sharma, "A survey on various cryptography techniques," Int. J. Emerg. Trends Technol. Compute. Sci., 3(4), 2014, pp. 307-312.
10. D. S. Abd Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," Int. J. Netw. Secur, 10(3), 2010, pp. 213-219.
11. M. A. Hameed, A. I. Jaber, J. M. Alobaidy, and A. Alaa, "Design and simulation DES algorithm of encryption for information security," American Journal of Engineering Research, 7(4), 2018, pp. 13-22.
12. .S. Ramanujam, and M. Karuppiah, "Designing an algorithm with high avalanche effect," Int. J. Comput. Sci. Netw. Secur, 11(1), 2011, pp. 106-111.
13. R. Divya, and M. Kumar, "Enhanced digital assessment of examination with secured access," International Journal of Advanced Studies in Computers, Science and Engineering, 3(10), 2014, pp. 33-37.
14. N. Singhal, and J. P. S. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," Int. J. Compute. Trends Technol., 2(6), 2011, pp. 177-181.