Online Employee Assessment System using Cryptography

S. Seerarutselvi[*1], R. Soubarnica[*2], K. Suba Nandhini[*3]
[*]*Department of Information technology, Sri Krishna College of Engineering and Technology,*
(An Autonomous Institution affiliated to Anna University,Chennai.),Coimbatore, TamilNadu, India.

***Abstract*— A communication is said to be completely secure when two parties are communicating and a third party does not listen to them, such that the communication is not susceptible to eavesdropping. Security has become a major concern after the advent of internet. There are many cryptographic algorithms but the security is still under threat. This paper enlightens the study of usage of Vernam cipher in encrypting the message. Vernam cipher is applied to Online employee assessment system in encrypting the personal details of an employee for assessing the employees, thereby achieving ultimate security.[**

Index Terms— decryption, eaves dropping, encryption, Online employee assessment system, Vernam cipher.

I. INTRODUCTION

In today's world information rules the world. Living without the access to information is practically impossible nowadays. With upgrading technology everyday, security is equally threatened on the other side. The malicious activity from a hacker could possibly corrupt the data and make it irrecoverable resulting the system in a dormant state. So having a security system can result in authorization for read /write access.

Most of the data that we transmit might be for communication purpose but there are some data that need to be kept confidential. These data require at most protection against the unauthorized.

The term "Cryptography" finds its origin from a Greek work which means secret writing. It is the science of transforming the original message into an intermediate format which is more secure. With cryptography, we can ensure security for the communication. There are several techniques and algorithms used for securing like AES (Advanced Encryption Standard), DES (Digital Encryption Standard), etc. .,. Not all cryptographic algorithms are 100% effective, which then results in the use of a special expensive hardware. In case of smaller companies, this may not be a good solution. A survey according to the BLI (Breach Level Index) identity that the theft type breaches were about 73% of all incidents, which is almost 50% increase in comparison to the previous survey. So there is a huge demand for an algorithm that provides a very high level security.

Our proposed system uses vernam cipher for encrypting the personal information of employees for assessment in the Online employee assessment system. The proposed algorithm illustrate tremendous security against security threats.

II. GUIDELINES FOR MANUSCRIPT PREPARATION

A. TDES (Triple Data Encryption Standard)

[3] uses Triple DES (Data Encryption Standard) algorithm to provide effective security and performance from the attackers. DES increases the size of the key which increases the protection of the system against illegal access. DES is the widely used symmetric key algorithm. TDES is a slight variation of traditional DES, which uses three times the application of traditional DES and it involves usage of two independent keys to produce a key length which is of 168 bits.

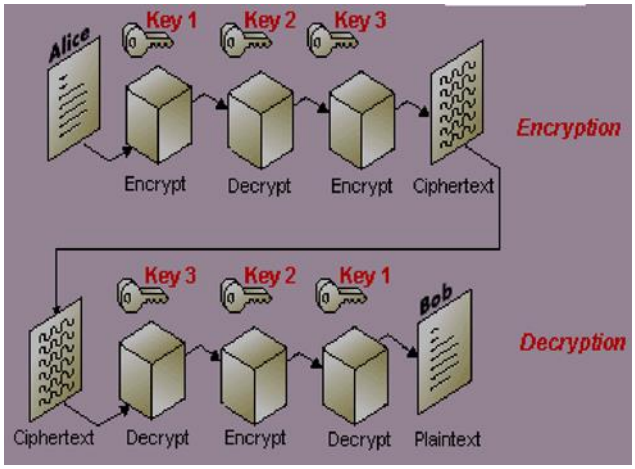

Fig. 1. DES Encryption and Decryption

It will make sure enhanced security through its encryption capabilities. It is a 64 bit of data block. It exhibits three keying techniques:

All keys are independent, the first key and the second key are independent and all the keys used are the same. It contains the usage of three iterations of common DES involving three steps:

- Encryption using the first secret key
- Decryption using the second secret key
- Encryption using the third secret key

The highlight of this method is the significantly sized key length, which is longer than most key lengths affiliated with other encryption modes.

B. AES(Advanced Encryption Standard)

[2],[4] proposes a system that uses Advanced Encryption Standard for enciphering and deciphering of data. AES contains three different sizes of keys – AES 128, followed by AES 192, and finally AES 256 bit with each cipher having each block 128-bit of size.

It explains the crucial features of AES and provides a comparison with algorithms like DES, Double DES, Triple

DES, Blowfish, etc., AES deals with a plaintext which is of fixed block whose size is about 128 bits.

The 16 bytes is represented in a 4 row and 4 column matrix (4X4) and so AES operates on the bytes composed as matrix.

The usage of this algorithm is much quicker than TDES. It performs its computations in units of bytes. The encryption process involves three process, starting with shifting of rows, then mixing the columns, finally adding the required round key.

The decryption process is same to the encryption followed in reverse order.

The advantage of AES is that it has built-in adaptability of size of the key, which ensures high level security against security threats.

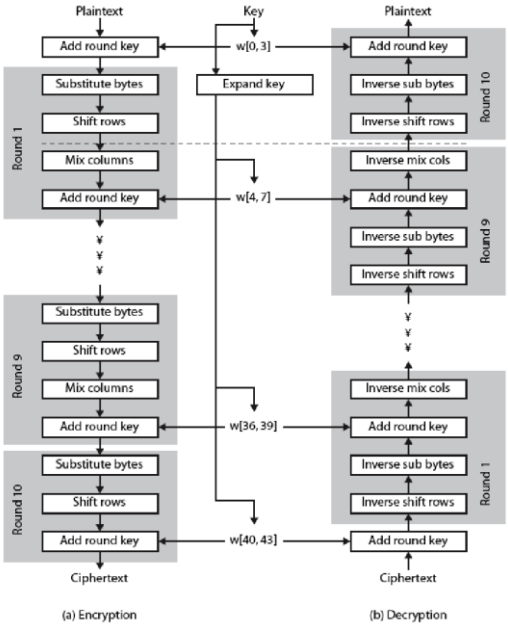

Fig. 2. AES Encryption Decryption process

C. *Password-based Authentication key exchange*

[7] proposes Password-based Authentication key exchange which is the widely used protocol in the modern network communication. It is said to provide a greater security against password guessing. The password here is not shared with others, it is shared with a third party who can be trusted (Trusted Third Party TTP). Here two participants are allowed to achieve authentication of their identity with the exchange of a simple password, and with the assistance of trusted third party a session key is shared where only the two participants have the knowledge of the session key. It provides high efficient, reliable, scalable key for data communication [8].

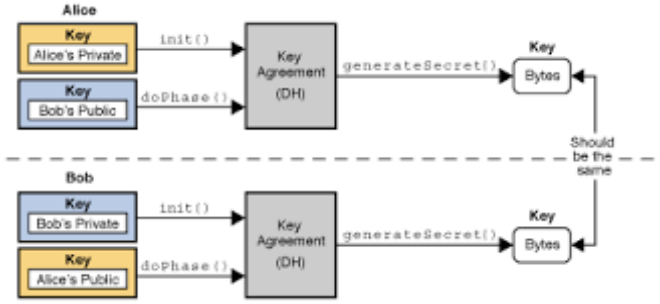

Fig. 3. Password-based Authentication key exchange process

It produces high throughput, producing a total of 40 sessions in key exchange process. So users can create up to 40 individual channels for their communication.

Thus the computational cost is greatly reduced due to the multiple keys used for sessions in the key exchanging process.

III. STATISTICAL ANALYSIS

There are several factors based on which an algorithm's performance can be analysed [5].

A. *Throughput*

The maximum time taken to process the data that is delivered over a medium. It is damaged by different components such as end user behavior, processing power, medium etc.,

B. *Encryption and Decryption speed*

The register size of CPU determines the speed of the enciphering and deciphering to fulfil the necessary requirements.

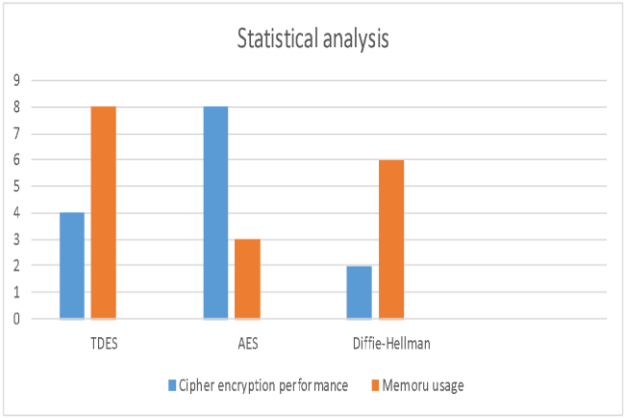

Fig. 4. Comparative analysis of algorithms

TABLE I
COMPARATIVE ANALYSIS OF VARIOUS ALGORITHMS

Algorithm parameters	**DES**	**AES**	**Diffie-Hellman**
Throughput	lower than AES	high	low
Complexity	More	Less	Less
Encryption speed	Very slow	Faster	Slow
Security against	Brute-force attack	Chosen plaintext, known plaintext	Eavesdropping
Rounds	16	10/12/14	56
Block size (bits)	64	18	56
Application	Smart card	Password manager	Protocols like SSL, SSH, IP sec.

C. *Key length*

This is the most important parameter when it comes to data encryption. The usage of different key length in symmetric algorithm takes longer time than

asymmetric key algorithms. So, managing the key becomes a great aspect when encryption is concerned which determines the cipher's control operation.

D. Levels of security

Any cryptographic algorithm should be secured against all the known attacks so far, such as, statistical attack, brute force attack, chosen plaintext, chosen ciphertext attacks. This is a prime aspect for an algorithm to satisfy the cryptographic security.

E. Encryption and Decryption time

The algorithm's complexity and the processor speed determines the time taken in enciphering and deciphering. The less time the algorithm consumes, the more enhanced is the complete operation of the system.

F. Encryption ratio

It can be defined as the ratio of measurement of encrypted data to that of the whole data. For each algorithm, the division of plaintext into megabyte takes place which is encrypted on total encryption time.

IV. Conclusion

The communication lies entirely upon the encryption algorithms. Every algorithm has its unique nature and its application differs based on the application. It has been found that AES is the most secure and efficient algorithm. The speed and power consumption of AES is also better in comparison to others. DES can be used for financial applications for the protection of classified information. Diffie-Hellman plays a role in securing internet services.

REFERENCES

[1] Shilpi Banerjee.(2016,Dec.).,OAES: Scalable and Secure Architecture Online Assessment and Evaluation System, Conference Paper.

[2] Daniyal M. Alghazzawi, Syed Hamid Hasan and Mohamed Salim Trigui**,** "Advanced Encryption Standard – Cryptanalysis Research**",** 2014 ICCSGD (INDIACom).

[3] Karthik .S, Muruganandam .A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System", IJSER www.ijser.in ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014.

[4] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security, IJCA, 67(19).

[5] Gaurav Yadav, Mrs.Aparna Mejame, "A Comparative Study of Performance Analysis of Various Encryption Algorithms", ICEMTE-2017 ISSN: 2321-8169 Volume: 5 Issue: 3.

[6] Mansoor Ibrahim, Sujaar Khan, Umer Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis", IJCA (0975 – 8887) Volume 61– No.20, January 2013.

[7] Eun-Jun Yoon 1 and Kee-Young Yoo 2, "Cryptanalysis of a simple three-party password-based key exchange protocol", IJCS Int. J. Commun. Syst. 2011; 24:532–542 Published online 12 July 2010 in Wiley Online Library (wileyonlinelibrary.com). DOI:10.1002/dac.1168.

[8] Md Imran Alam*, Mohammad Rafeek Khan," Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", Volume 3, Issue 10, October 2013, ISSN: 2277 128X , IJARCSE.

[9] Vekariya Meghna, "Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms", IJCES,August- 2014.

[10] Ajin P Thomas1, Sruthi P.S2, Jerry Rachel Jacob3, Vandana V Nair 4, Reeba R 5," Secret Data Transmission Using Combination of Cryptography & Steganography", Volume 4, Issue 5, May-2017, pp. 171-175 ISSN (O): 2349-7084,IJCERT.