Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Cryptographic Technique

[1]Mayank Jain, [2]Raghvendra Gupta, [3]Pinku, [4]Sudha Senthil Kumar, [5]Brindha K

[1, 2, 3] MCA VIT University, Tamil Nadu, India

[4, 5] SITE VIT University, Tamil Nadu, India

Abstract-- Cryptographic technique is used to secure data while sending and receiving data among users.It is an effective way to secure the data as it is very dangerous to send or receive data because to increasing cases of data loss, theft and hacking.While exchangingconfidential information on networks, this technique is used to encrypt the data and decrypt at the receiver's end which enhances authentication.The plain text is encrypted using algorithms at the sender's end which is ciphered text and the ciphered text is decrypted at receivers end. In this paper, we have used the Cryptographic ULS algorithm to encrypt and decrypt the data. Cryptographic ULS algorithmprovides the process of converting a maximum file size of 20 Mb into an encrypted text and is being decrypted at receivers end. Also a random password is generated with it which is also being written during encryption and the receiver receives the file and decrypt it. Also the password should not be less than 8 bytes and it can be maximum of 32 bytes.

Keywords:Encryption, Decryption, Symmetric, Cryptographic ULS, Symmetric Key

I. INTRODUCTION

Cryptography is a method of encrypting and decrypting data so it provides authenticity and confidentiality to the data to maintain security so it cannot be read and accessed by any unauthorised person. By encrypting the data we getoutput in the form of ciphered text which is unique. The opposite is decryptionwhich is used to decrypt the ciphered text and derive the original text. Many algorithms have been proposed like DES, RSA etc. but they are less efficient than Cryptographic ULS algorithm as Cryptographic ULS algorithm focus on encrypting the file and add a random password generated with it which is being sent to the sender. Further the receiver checks whether the random number it has received is the original number generated or not.

Symmetric key technology is a technique in cryptography which encrypt plain text and convert it into ciphered text. Then the ciphere text is decrypted and plain text is obtaine at the receiver end.Both the sender and receiver have to agree upon sharing secret key to encrypt as well as decrypt data which is one of the drawback of symmetric key algorithm compared to public key encryption. This algorithm is of two types: **stream ciphers and block ciphers**.

II. LITERATURE REVIEW

1. [1]DES Algorithm: This is a symmetric key algorithm to encrypt data which was famous during its time for academic purpose and was designed by IBM. This algorithm is considered to be insecure because it uses 56 bit key. This algorithm was believed to be secure in form of Triple DES but there are some theoretical attacks. It has the block size of 64 bits but only 56 bits are used by the algorithm. The rest eight are used for checking parity, so they are discarded.
2. [2] AES Algorithm: This is a symmetric key algorithm established in 2001. It has block size of 128 bits and three different key lengths: 128,192 and 256 bits. It is based on substitution-permutation network andfast in both hardware and software. It operates on 4*4 column-major order. AES algorithm has 10 cycles for 128 bit keys, 12 cycles for 192 bit keys and 14 cycles for 256 bit keys. Each round consists of multiple steps and has four similar but different stages and reverse rounds are performed to convert ciphered text into plain text. This is the reason this algorithm supersedes DSA Algorithm.

III. CRYPTOGRAPHIC ULS ALGORITHM

A. STEPS FOR ENCRYPTION

- A file is taken which is to be encrypted.
- The file could be of any size up to 20mb.
- Once the file is encrypted a random password is generated.
- The encrypted file with the random number generated is sent to the sender.

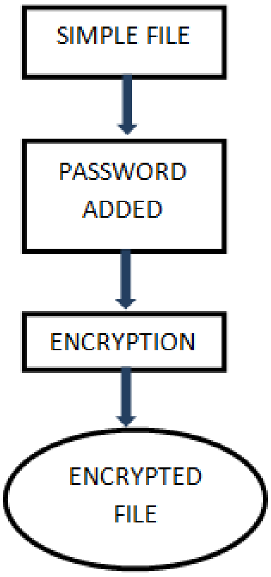

Fig.1: Architecture for encryption

B. STEPS FOR DECRYPTION

- The decrypted file is received.
- The random password is checked by the receiver.
- If the password it receives is matched it goes for further process
- The file is then decrypted.

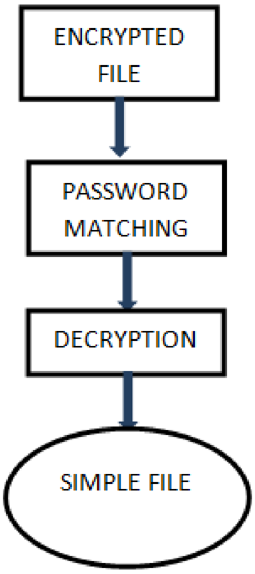

Fig.2: Architecture for decryption

IV. COMPARATIVE ANALYSIS

Algorithm	File Size	Time (In Sec. approx.)	Performance
DES	4 MB	1.5	Low
CRYPTOGRAPHIC ULS (176- Bit)	4 MB	1	Medium
AES	4 MB	0.5	High

Algorithm	File Size	Time (In Sec. approx.)	Performance
DES	10 MB	3	Low
CRYPTOGRAPHIC ULS (176- Bit)	10 MB	2	Medium
AES	10 MB	1	High

Algorithm	File Size	Time (In Sec. approx.)	Performance
DES	20 MB	5	Low
CRYPTOGRAPHIC ULS (176- Bit)	20 MB	3	Medium
AES	20 MB	1.5	High

V. SECURITY ANALYSIS

This algorithm provides security by encrypting a file of maximum size upto 20mb. Also a random password generated is being added with the encrypted file. The password shouldn't be less than 8 bytes and it could be maximum of 32 bytes in size. All of this is then sent to the receiver and once the receiver receives it, it first matches the password with the original password and then decrypts the file.

A. Brute force attack

Cryptographic ULS uses the 176 bit key size which makes it impossible for hackers to crack 2^{176} in a short period of time. DES uses 56 bit key which is much easy to be cracked as compared to Cryptographic ULS algorithm. Therefore, Cryptographic ULS is secured against DES.

B. Avalanche effect

The avalanche effect comes when an input is changed to some part, the output changes. In any kind of ciphered method, small amount of change in either key or the plain text could make a change in the ciphered text. In Cryptographic ULS algorithm it's been proved in the results that ciphered output changes more drastically as compared to DES. So Cryptographic ULS have more avalanche effect than DES.

C. Key Management & Complexity

176 bit key securely changed with help of Diffie-Hellman key exchange algorithm reduces the risk of key losss or hackers cracking the key during the data transfer. Cryptographic ULS provides more complexity as we used a secret key as well provided it with a password at the users end.

We have increased the security by providing a secured password which would be known only to receiver. It helps in preventing data loss as if the hacker hacks the encrypted data, he wouldn't beknowingpassword to decrypt it which maintains the integrity of the data. One of the key advantage of Cryptographic ULS is, the random password generated. The receiver has to match the password with the original password in order to check whether the file has been tampered in between or not.Also, our key is 176 bits which is very much efficient as compared to DES algorithm which use only 56 bit key.

VI. CONCLUSION

Security is very important nowadays as the cases of hacking are increasing. In order to save the data from any kind of loss, theft or hijacking, cryptographictechnique is usedwhich uses technique of encryption and decryption of information. In this we have used the Cryptographic ULS Algorithm to secure the information by encrypting a file of maximum size 20mb. Also a random password is generated which is being added with the encrypted file and is being sent to the receiver. The receiver after receiving the file, matches the password with the original random password. If it matches then it further goes on with the process of decrypting the data. After the correct password has been input, the receiver can access the data. This provides more integrity and security to the data as if the data gets lost or hacked, then the hacker wouldn't be able to access the data as he wouldn't be aware of the password and hence the data would be secured from getting leaked.

VII. FUTURE WORK

This algorithm has various benefits and can be used in multiple applications. We are planning to work on cloud computation by using Cryptographic ULS algorithm. We are planning to upload files and information on the cloud like images, audio files, video files, very large amount of documentation and folders on the cloudwhich would make them secured. Also, we have planned to improve the algorithm by encrypting data in such a way that the sender also wouldn't be knowing what is the content of data, which enhances the level of security. This would help in critical situations when the owner of the data sends the data with the help of a cyber expert and he doesn't want to disclose it to sender. This would make the information highly confidential to the outside world and only the owner and the authorised receiver would be granted all permission to access the data which would prevent data from any kind of leakage. Also it maintains integrity of all information which is the most important aspect of data encryption.

REFERENCES

[1] Sombir Singh, Sunil K Makkar, Dr.Sudesh Kumar "Enhancing the security of DES algorithm Using Transposition Cryptography Techniques", IJARCSSE, Vol. 3, June 2013.

[2] Bin Liu, Bevan M. Baas "Parallel AES Encryption For many Co-Processor Arrays, IEEE, Vol.62, No. 3 March 2013

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh,M.A.Mallik, Proceedings ofInternational conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244

[4] Data Hiding and Retrieval, A.Nath,S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Cryptography and Network, William Stallings, Prectice Hall of India

[6] Data Hiding and Retrieval, A.Nath,S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.