A Survey Paper on Secured Email Server using 3DES

Nandkumar Bhimnath, Rohan Yemul, Manisha K. M

[1,2]Student: Computer Science & Engineering Department, Sanjay Ghodawat Group of Institutions
[3]Assistant Professor: Computer Science & Engineering Department, Sanjay Ghodawat University

---***---

Abstract: *Any network is vulnerable to malicious use and accidental damage unless it's properly secured. Hackers, disgruntled members, or poor security practices within the organization can leave private information exposed, including trade secrets and customers private details. Losing confidential research such as, the potentially cost an organization millions of dollars by taking away competitive advantages it paid to gain. While hackers stealing customers' information, and selling them to be used in fraud, creates negative publicity and public misuse of the organization. So security is a must to keep data safe.*

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are used for three times to every data block. The key size is increased in Triple DES to check additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are mentioned as bundle keys with 56 bits per key. Here the user entered key is distributed to receiver or sender via SMS or EMAIL.

Keywords: 3DES algorithm, SSL Security, 3DES Encryption, OTP Authentication, 3DES Decryption

1. Introduction

Email It's in common use to share data with help of server offering services with other users, friends etc. E.g. such sharing the data or vice versa (e.g. Profile information, health or property records, etc.). It's always the users responsibility to safeguard own data and avoid misuse of it. It becomes a challenge for user to protect self-data on email network, to overcome this scenario it is important to design and allocate secured access control to the data until the expiry period. Basic can be to store the data in encrypted format but disadvantage with classic encryption is the owner should know what information the users wants to share and with whom this makes the process to sharing the data to many a bit hectic. To overcome this disadvantage we have Triple DES encryption which enables one to many encryptions Triple DES has the ability to provide data security as well as access control to the minimum level.

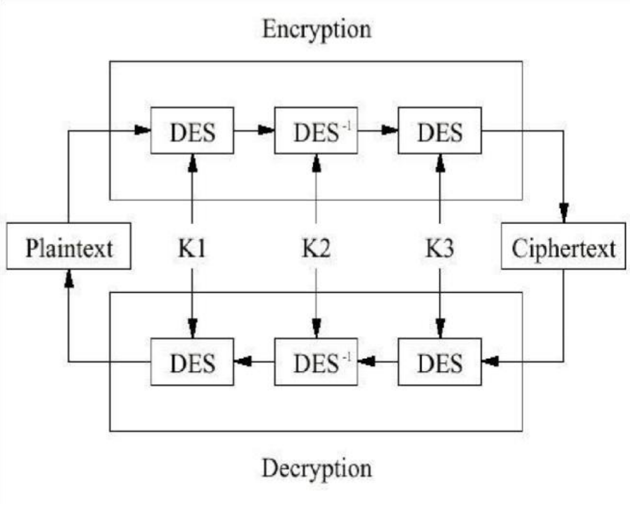

Fig 2: General Depiction of 3DES

2. Literature Survey

In order to know in detail about this survey the previous research work done in this direction, several studies dedicated to the topic were referred. The literature survey is done in chronological order from 1996-2016.

Chris J. Mitchell in 2016, [1] has stated that an encryption technique that remains widely used despite recently being de-standardised and constituting the first advance in cryptanalysis of 2-key triple DES since 1990. They give future attack enhancements that together implies that mostly used estimate that 2-key 3 DES provides 80 bits of securities can no more be regard as conservativation. Finally whilst not completely broken, the margin of safety for 2-key triple DES is slim, and efforts to replace it, at least with its 3-key variant, should be pursued with some urgency.

Mohamed hamdy Eldefrawy, khurram Khan has used Two-factor authentication (2FA) provides protection, since cutomers are encouraged to provide something they observe and something they have it. That technique deliver a higher-level of authentication assurance, which is easy for online banking securities. They presented a two-factor authentication scheme whereby a user's device produces multiples OTPs from an initial seed using the proposed scheme. The initial seeds is produced by the communications partners' unique parameters. They applied many from one function to a certain seed removes the requirement of sending SMS-based OTPs to users, and reduces the restrictions caused by SMS.

D. Coppersmith and D. B. Johnson proposed a next mode of multiple encryption 3-DES external feedback cipher block chaining including output feedbacks masking. They provided protection against certain attacks which exploit the short message-block size of DES. They implemented secret mask value which is derived from a fourth encryption operation per message block, in addition to the three used in previous mode. The new mode is part of encryption mode proposed in the ANSI X9.F.1 #-DES draft standards (X9.52).

Devashish Kumar Amit Agrawal they shown that the OTP which was developed as a part of two factor authentication is weak point to attacks. In this paper, they represented a new framework for improving authentication during online transaction which secures our OTP.

3. Triple DES(3 DES)

3DES is a symmetric-key block cipher, inherited from the DES and it make use of three different keys that means which applies the DES three times to every data block. Uses a 56-bit key and is not view as sufficient to encrypt sensitive information. 3-DES simply increase the key size of DES by applying the algorithm three times in succession with three different keys. The grouped key size is 168 bits because of 56 bit with 3 times.

Table 1.1Comparasion between DES and 3DES Encryption

Factors	DES	3DES
Key Length	56 bits	112 bits(2 key) 168 bits(3 key)
Block Size	64 bits	64 bits
Possible key	2^56	2^112
Cipher type	Symmetric Block	Symmetric Block
Weakness to hacking	• Cryptanalysis • Brute Force • Linear	• Cryptanalysis • Brute Force • Linear
Security	Weak	Strong
Keys	1	2 or 3
Rounds run through algorithm	16	48

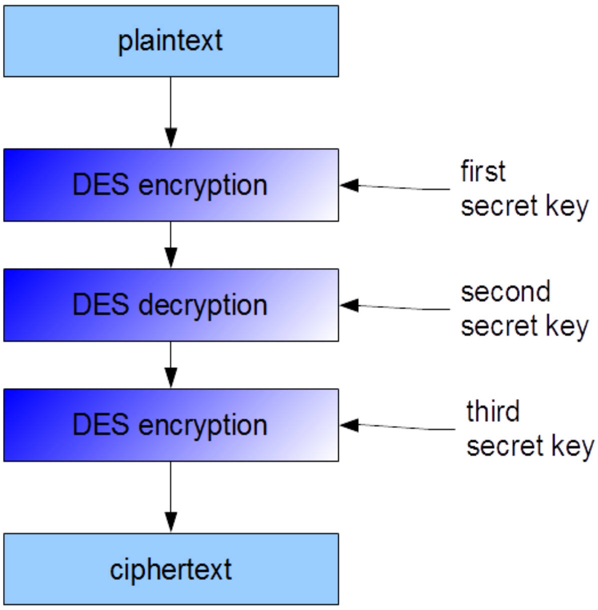

Figure 3.2.1 3DES Encryption

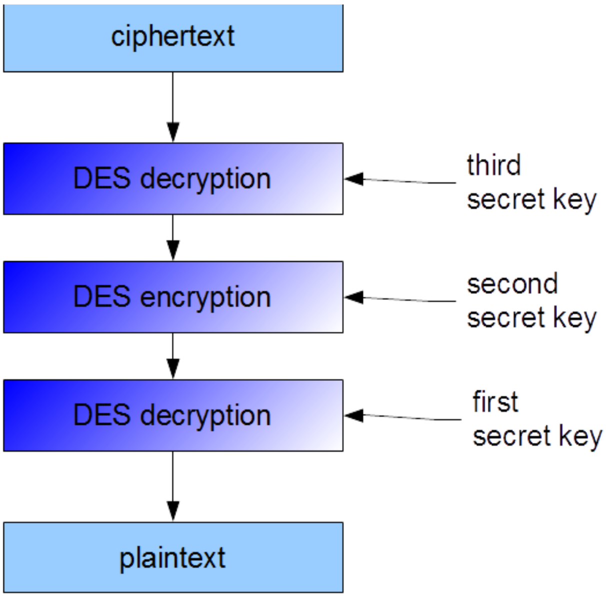

Figure 3.2.2 3DES Decryption.

4. CONCLUSION

The main aim of this tool is to provide security. This tool can be best used at the organizational level. It provides high level security wherein even if the data is hacked; the hacker will not be able to access the account because of the Triple DES technique used. Hence, this tool is the best to be used for security. To prevent the users of Gmail, rapid share, PayPal, eBay, etc. getting hacked. To prevent the users loss of data in Internet. The two factor authentication gives boost to the security.

5. References

1) “A proposed mode for triple-DES encryption” by D. Coppersmith, D. B. Johnson and S. M. Matyas.

2) “On the Security of 2-Key Triple DES” by Chris J. Mitchell.

3) “OTP-Based Two-Factor Authentication Using Mobile Phones” by Mohamed Hamdy Eldefrawy, Khaled Alghathbar and Muhammad Khurram Khan.

4) “Efficiently improving the security of OTP” by Devashish Kumar, Amit Agrawal and Puneet Goyal

5) Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish

6) Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science

7) Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud,"Performance Evaluation of Symmetric EncryptionAlgorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

8) Electronic Frontier Foundation. Cracking DES: Secrets of encryption research, wiretap politics and chip design. O’Reilly and Associates,