ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Advances in Cascaded Cryptography

Harshika Rajeshkumar Rana[1]
Dept. Computer Application
Indus University
Ahmedabad, India

Prashant P Pittalia[2]
Dept. Computer Application
NICM
Gandhi Nagar, India

Abstract: ***Cryptography means protecting data from being viewed or modified over insecure channels. It is majorly done by encryption algorithms. Different research about cryptographic algorithms are going on which proves that if technology grow security should be grow security should be grow. It has been proven that cascaded cryptography is more secure than single one. Customization in cascaded cryptography for packet encryption will be value addition an advanced cryptography.***

Keywords: Cryptography; Plaintext; Encryption; Decryption; Cascaded; Transformation; Cipher text; Customization; Packet encryption.

I. INTRODUCTION

A novel bucketization and partitioning structure is proposed which then inflfenced many of the papers in literature. An algebraic framework is described for query rewriting over encrypted attributes.

The main idea is to map the plaintext values to ciphertext values by splitting the domain values of plaintexts into some partitions and giving them bucket ids. Each relation R (*A1, A2, ..., AN) is stored as an encrypted* relation: *RS (encrypted tuple, A1_S, A1_S, ... , A1_S) where the attribute encrypted tuple* is the encrypted string that corresponds to a tuple in R. Each attribute *Ai_S is the* index for the attribute *Ai. The domain of Ai is partitioned into partitions p1, p2, ..., pn such any two partitions do not overlap and the partitions taken as a whole cover* the whole domain. Different attributes may be partitioned using different partitions functions. These partition functions may be any two functions satisfying the above two conditions.

Cryptography is a process of transmitting data into a particular format so only intended persons can read and process it. The term is most often associated with transforming and substituting plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext is called encryption, then reverse process is called as decryption.

Cascaded cryptography: Multiple encryptions are the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. It is also known as cascade encryption, cascade ciphering, multiple encryption, and super encipherment. Super encryption refers to the outer-level encryption of a multiple encryption.

We can use this concept for any level of security because it can give most powerful security to network.

And fact is that when technology grow , data grow , and we need to find out most secure way for transferring data on the network.

II. LITERATURE REVIEW

Secure Distributed Computation

Secure function evaluation (SFE) is a function which allow a set of n players P ={p1, . . . , pn} to compute an arbitrary agreed function f of their inputs x1, . . , xn in a secure way. MPC: multi-party computation is in this scenario players can give input and output for many time. Example of SFE and MPC is E-voting in player's confidentiality will be maintain.[1]

Abstract Cryptography Abstract Cryptography is to achieve a highest level of abstraction. In this we have to found a way of encrypt data from generalized data with simplicity.[1]

III. Base Structure For Proposed Model

All Before In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

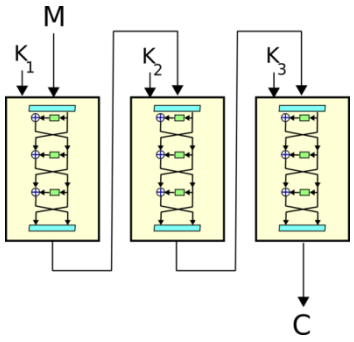

Fig.1. 3DES

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

Algorithm:

Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

I.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))

I.e., decrypt with K3, encrypt with K2, then decrypt with K1.

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3

Black-Boxes and Generic Algorithms

Algebraic structure may create complexity in cryptography and for that we have to represent them in to bit string. Algorithms that do not exploit representation that is generic. Generic can be used for two purposes first it is not important that how all structure represents and another for to give lower bound for certain computational problems.[2]

Quantum Cryptography

This method uses mechanical quantum mechanism for identifying quantum communication or break cryptography. Example: use quantum communication for sharing keys. It is mostly useful for public key encryption methods.[3]

OTP One-time password

It is new mechanism which provides authentication for one session only. In contrast of static password it provides dynamism for secure transaction. Intercepting session is very difficult without permission of authorized person.[4]

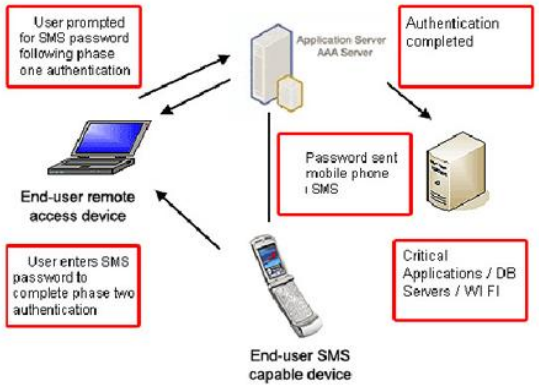

Fig.2. OTP: One-time password

IV. PRAPOSED MODEL

Customized Cascaded Cryptography: It is a mixture of two or more encryption algorithm and user can add algorithms by user requirements and they can select it as per their comfort

For Example:

- Select algorithms DES , AES , RSA
- Give them sequence number as
- 1= DES , 2 = AES , 3 = RSA
- Select one algorithm for one time = 1
- Select one algorithm for multiple time (infinity)= 1111… time
- You can merge algorithms for multiple times= 1223312312323So combinations made from these algorithms can be up to infinity

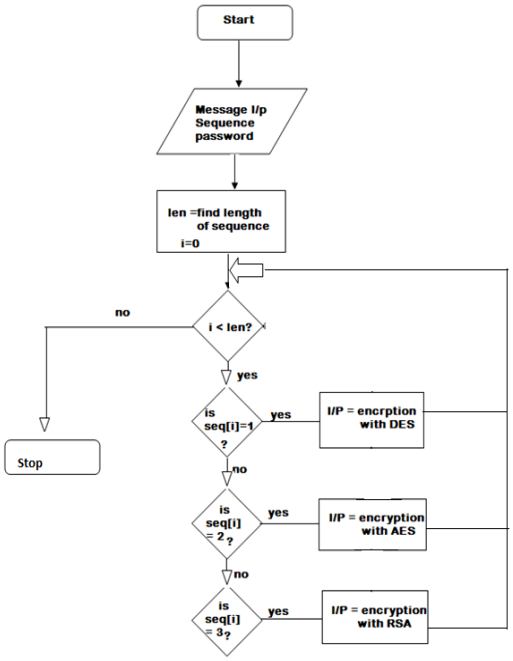

Fig.3 Customized Cascaded Cryptography

Proposed Model for Packet Encryption by routers

In current the router gives the facilities to encrypt the username and password. This can be use for transmission of packets between routers to router. It might decrease the speed but It can be the most secure way to transmit data.

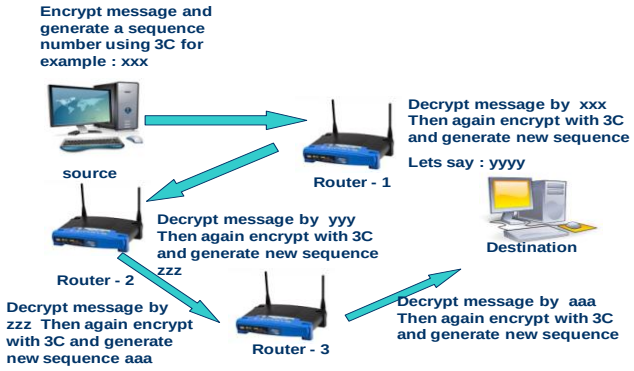

Fig.4 Proposed model for packet encryption

V. CONCLUSION

As per above literature review, It has been proven that customized cryptography is more powerful and secure than normal single encryption algorithm. This concept can be use for packet encryption which will help for value addition in the cryptographic world

References

1. www.cryptography.com
2. https://eprint.iacr.org/2007/078.pdf
3. http://arxiv.org/abs/quant-ph/0512258
4. https://eprint.iacr.org/2007/089.pdf
5. http://link.springer.com/chapter
6. http://www.crypto.ethz.ch/research
7. Computer Networks, Fourth Edition by Andrew S.
8. Network Security essentials Applications and Standards, 3rd Edition, by William Stallings, Pearson Education

AUTHOR(S) PROFILE

Harshika Rana, received the MCA degree from Gujrat Technological Univeristy in 2012. In 2013 she got admission in Indus university, Ahmedabad as a research scholar (PhD), She is also working as an Assistant Professor at Parul Institute of Computer Application, Vadodara since 2012.

Prashant P Pittalia, received the PhD degree from Bhavnagar University in 2011 and MCA degree from Gujrat Vidyapeeth in 2000. He is working as an Associate Professor at Shri Jairambhai Patel Institute of Business Management & Computer Applications (NICM Group of Institutions), Gandhinagar since 2001.

