Implementation of Blowfish Algorithm and Exploring Key Management & Authentication in Cryptography

[1.]S.Uma Mageshwari,Research Scholar, R& D Centre, Bharathiar University , Coimbatore.

[2.]Dr. R.Santhi,Research Supervisor, Bharathiar University, Coimbatore.

Abstract

In this IT scenario, there is an increase in the malware, spyware and malicious software (or applications) in the network by the attackers, such things need to be sensed and secured by adopting the mechanism to ensure confidentiality, authentication, integrity and availability. The number of Cryptography algorithms has been devised to develop the secret messages. The security attacks encountered essential to be resolved with key management, public key cryptography, protocols and authentication. This paper enlightens the Key distribution, Authentication, Security focuses in the Network and Blowfish algorithm. The implementation of the Blowfish algorithm is done in Netbeans 8.1.

Keywords: Authentication, Blowfish, Key distribution and Security.

I.INTRODUCTION

The direct transmission of message over the network give away the attackers to gain access of the information. Therefore, the original text is converted into ciphertext by using various cryptography algorithms. The security of the network structure be determined by the algorithm with key. The key is the most precious thing for safeguarding the information as well as thwarting the hackers for unapproved access. The keys have to be retained and circulated in a proper secure channel. The access privilege to be given only to the legal person. These tasks are achieved with Key distribution and Authentication methodology. As well as, the Blowfish algorithm is discussed in this paper with sample output.

II. LITERATURE REVIEW

[1] **Youssouf Mahamat koukou et.all**.: This paper deals with the comparison of algorithms such as AES, Blowfish, CAST-128 and DES. The performance analysis is done using Crypto tool.

[2] **Manisha Yadav, Karan Singh, Ajay Shekhar Pandey**: The overhead problem of communication and storage in the network is carried out using key management technique as well as implemented in Network Simulator(NS2).

[9] **Hasen Nicanfar et.all.:** For HAN(Home Area Network) attacks has been resolved with proposed key management and authentication structure.

III. METHODOLOGY

A.PUBLIC KEY CRYPTOGRPHY

To ensure confidentiality for the information the concept of public key cryptography is adopted. The asymmetric key cryptography or Public key cryptography needs the following mechanisms such as,

- M : PlainText

- EKRa(M) : CipherText
- Keys : Private[KR_a] & Public [KU_b])
- E : Encryption algorithm
- D : Decryption algorithm

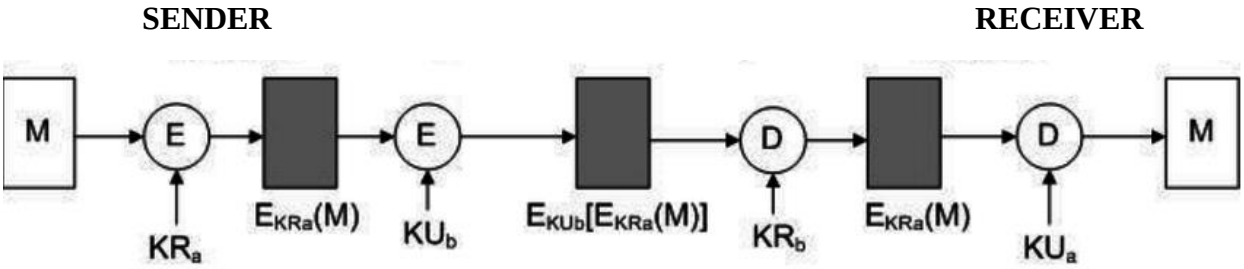

Fig 1: [3] Public Key Encryption

B. KEY MANAGEMENT

Asymmetric key encryption requires pair of keys namely, private (confidential) and public (revealed to all) key. Such public keys are distributed by the sender in a secure channel to the recipient. To achieve confidentiality and authentication to the information in a network, all the users' keys need to be stored and maintained.

Key Distribution

The public keys can be distributed in the following ways [6],

- ***Public Announcement***

  The Key will be announced to all the users. These keys can be forged.

- ***Publicly available directory***

  The registered users can store their public keys in the directory. The keys will be distributed to the communicating parties through directory. If the directory password is revealed, then there is no security to all the users' public key.

- ***Public key authority***

  The public key authority maintains all the users' public key. The key will be issued after proving the authentication of the users. Every time all the users have to get the key of communicating party from public key authority. So, the system speediness become slow.

- **Public key certificates**

  The certificate authority will issue a certificate to the user that need to be decrypted by using authority's public key. Then, the user's certificates will be exchanged between the parties.

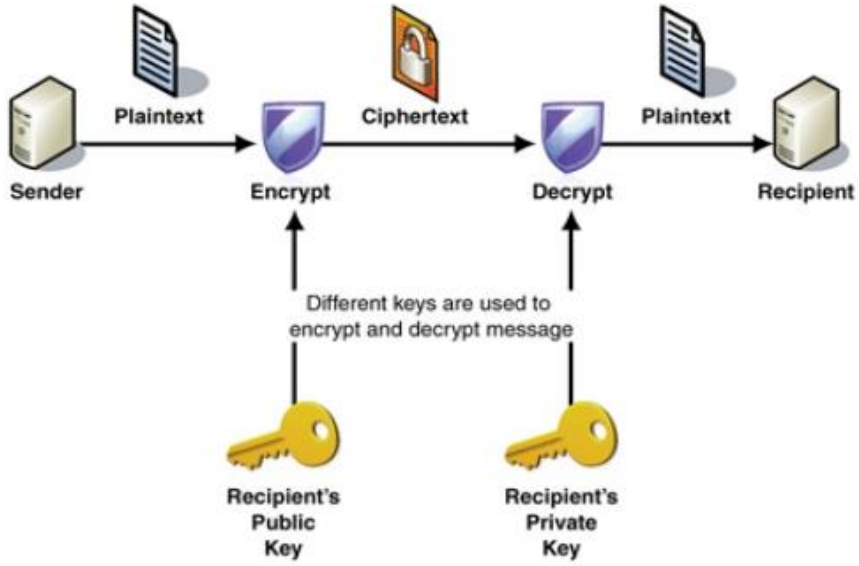

Fig 2: [8] Public Key Cryptography

C. AUTHENTICATION

The authentication confirms the user identity. So, the message will be forwarded only to the authorized person. The authentication method can be shown as below [6],

- ***Password based Authentication***

  The password (secret code) has been used to guarantee user's identity. The password can contain special characters, alphabets and numbers. The currently entered password will be compared with the stored value. If it matches, then the authentication is done successfully. In this approach, if the password is stolen by the attacker then there is no security to the system.

- ***Two factor Authentication***

  The security is accomplished using two aspects namely, identification and authentication. The good example of this methodology is ATM card issued by the bank. For online transactions, OTP (One Time Password) has been used widely. The Man –in-the middle attack and Trojan horse (malicious application/software) is the weakness of this technique.

- ***Biometric Authentication***

  The person is authorized with biometric impression such as fingerprint, iris, face, tongue or voice. If there is any physical injuries caused to a person, then the impression won't match with the stored template. This is the difficulty of this methodology.

- ***Extensible Authentication Protocol***

  The communication between the server and client is done using EAP. The EAP identifies the users and transfer the messages to the right authenticator. The applications of EAP are Smart Card, Online Transactions for producing OTP and Digital Certificate.

D.BLOWFISH ALGORITHM

[6] The Blowfish is a block cipher symmetric encryption algorithm. The algorithm is developed by Bruce Schneier in the year 1993. The algorithm operations can be described as Key expansion, Encryption and Decryption. For Decryption process, the subkeys are used but in the converse order of Encryption. The 16 rounds , 4 s- boxes and use of round keys makes the algorithm to be robust as well as produces the result faster.

PlainText	64 bits
CipherText	64 bits
Key size	32 to 448 bits
Rounds	16
Subkeys	18
S-boxes	4 (Each convert 8- bit to 32 –bit)

Table 1: Blowfish Algorithm

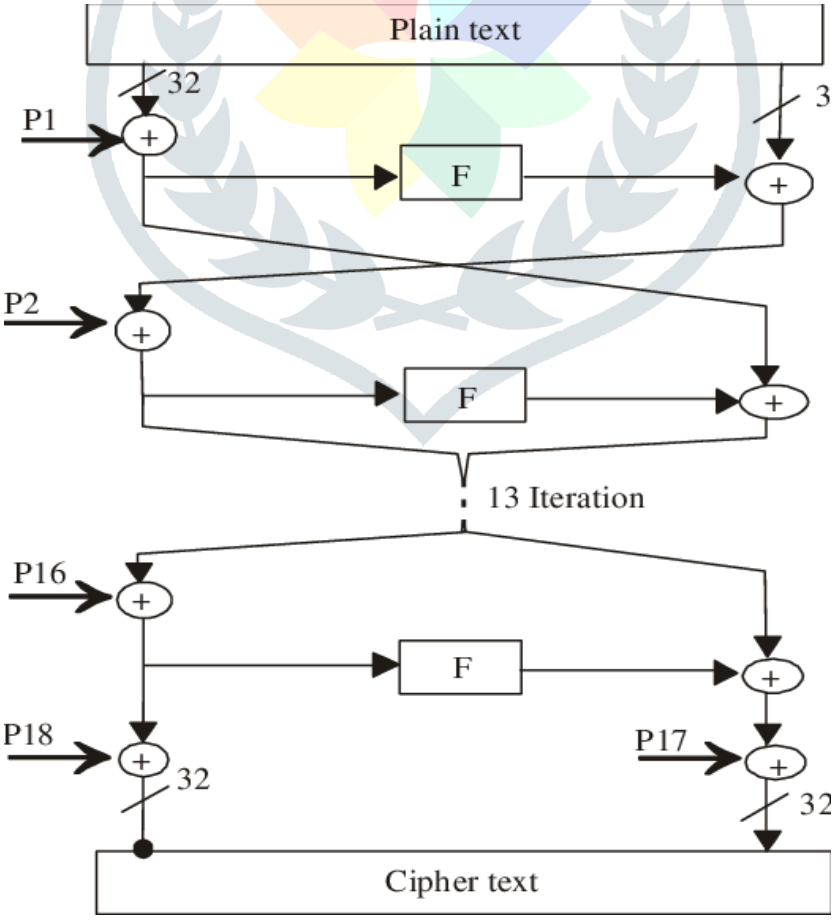

Fig 3: [4] Blow Fish Architecture

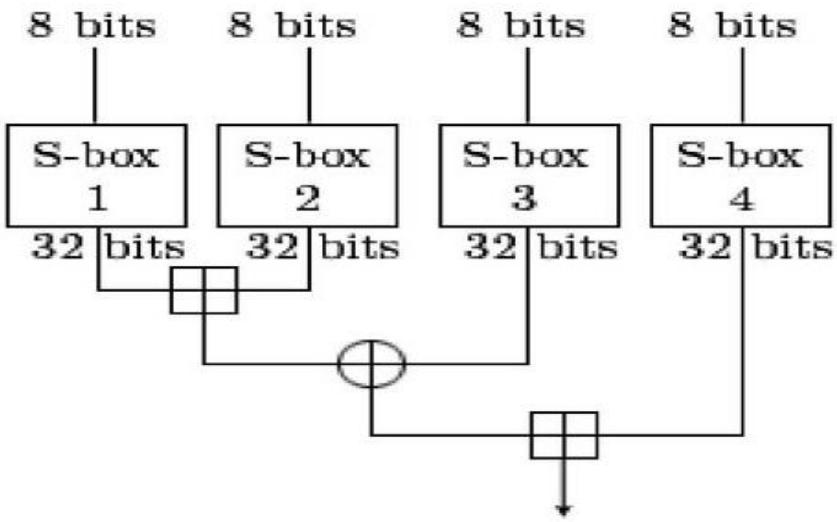

Fig 4: [5] "f" function Blowfish Algorithm

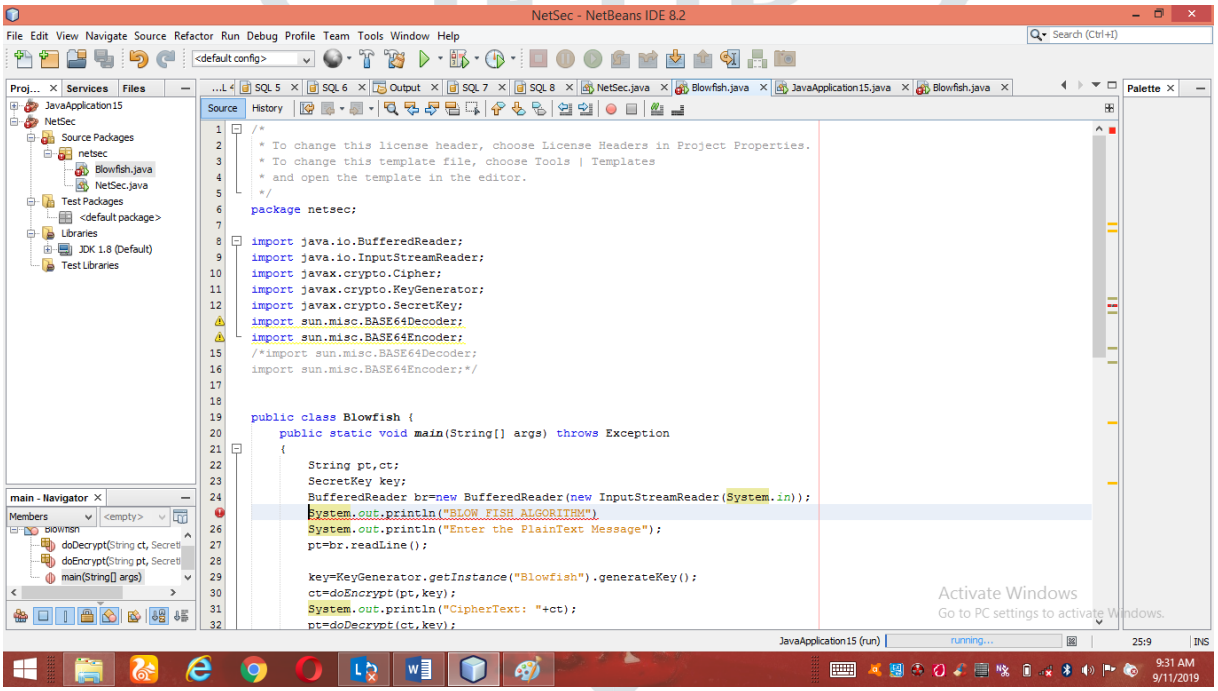

Fig 5: Implementation of Blowfish Algorithm

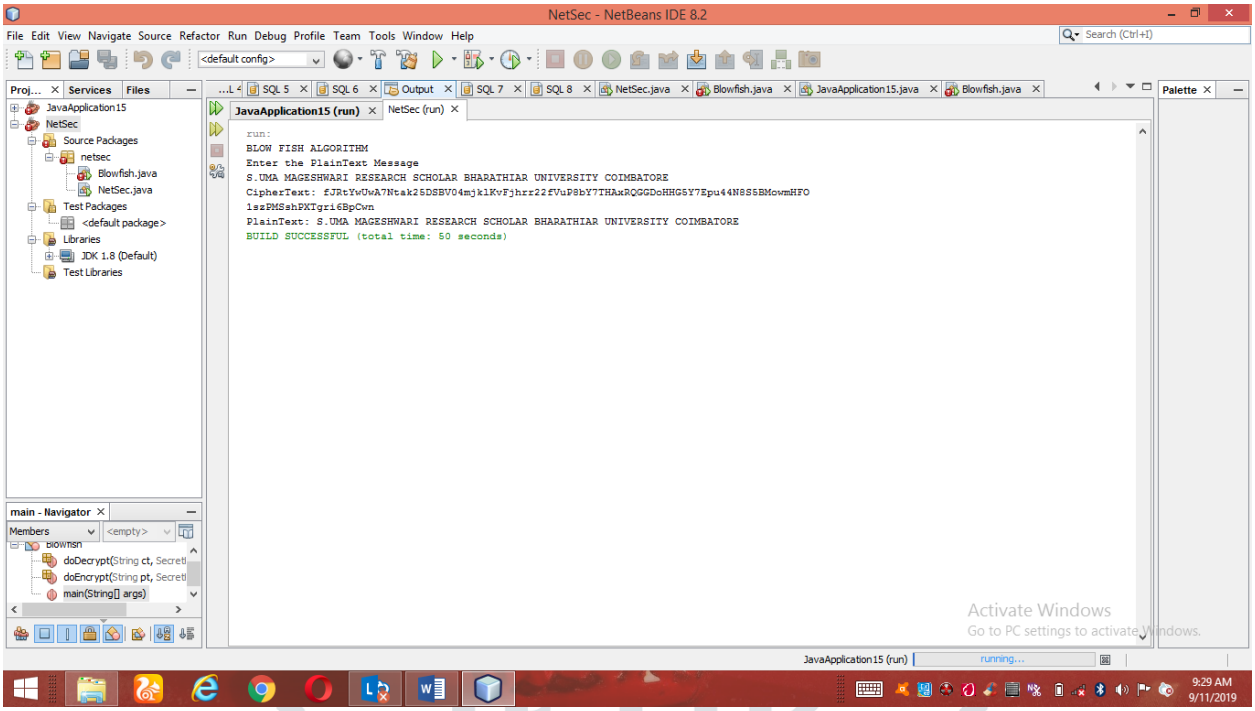

Fig 6: Sample Output of Blowfish.

IV. SECURITY FOCUSES

A. WEB SECURITY

[6] Web security is achieved through SSL (Secure Socket Layer). SSL protocol is established by Netscape. The TCP/IP (Transmission Control Protocol/ Protocol) is responsible to send and route the data over the Internet. The SSL protocol act over the TCP/IP. SSL be responsible for the security from server to client by providing certificate. The client is authenticated with id and password then secured key and certificate will be issued by SSL.

B. EMAIL SECURITY

The Email communication between the sender and receiver can be secured with the methodology such as PGP (Pretty Good Privacy), MIME (Multipurpose Internet Mail Extension) and S/MIME (Secure/ Multipurpose Internet Mail Extensions).

C. IP SECURITY

The network structure should be secured from unauthorized access of information. The IP security can be carried out by making use of the techniques such as IPv4, IPv6, ISAKMP (Internet Security Association and Key Management Protocol) and VPN (Virtual Private Network).

V. CONCLUSION

In this digital world, all the important transactions and messages are communicated through Internet. Such, information are to be kept secret and the hackers accessing methods to be prevented. The impact on security threats and authentication system must be controlled in a proper way for better security. Thus, the paper identifies the glimpses of Blowfish algorithm, management of keys and public key cryptosystem.

REFERENCES

[1] Youssouf Mahamat koukou et al., "Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm", IOSR JEN,Vol: 06. Issue: 06, June 2016, V1, PP 01-07.

[2] Manisha Yadav, et al., "Key Management in Efficient and Secure Group Communication", ICETEESES-16,IEEE, 2016.

[3] https://www.researchgate.net/figure/Public-Key-Encryption-Confidentiality-Authentication-and-Signature_fig3_256542207

[4] https://www.researchgate.net/figure/Fiestal-structure-of-blowfishcipher_fig1_278671149.

[5] https://www.splashdata.com/splashid/blowfish.htm

[6] V.K.Pachghare, "Cryptography and Information Security", PHI Learning Private Limited 2009.

[7] William Stallings, "Cryptography and Network Security", Prentice Hall of India, 2008.

[8] https://www.slideshare.net/Indra97065/public-key-cryptography-and-rsa-algorithm- 65491226

[9] Hasen Nicanfar, et al., "Efficient Authentication and Key Management for the Home Area Network", IEEE ICC 2012,IEEE.

[10] B.T.Geetha, Dr.M.V.Srinath, "A study on various Cryptographic Key Management and Distribution system in Secure Multicast Communicatios", 2012, IEEE, DOI:10.1109/MNC Apps.2012.18.

[11] ShraddhaM.Gurav, et al., "Graphical Password Authentication",2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, IEEE, DOI: 10.1109/ICESC.2014.90.

[12] Fadi Aloul, Syed Zahidi, "Two Factor Authentication Using Mobile Phones",2009, IEEE.

[13] Chao Lv et al., "A Security Authentication and Key Distribution Protocol for Wireless Networks", IEEE Globecom 2010 Workshop on Web and Pervasive Security, IEEE.

[14] Samir Kumar Bandyyopadhyay et al., "User Authentication by Secured Graphical Password Implementation", 2008 IEICE.

[15] C.Y.Chen et al., "A Fair and Dynamic Password Authentication System", 2011, IEEE.

[16] Wenjian Luo et al., "Authentication by Encrypted Negative Password", DOI: 10.1109/TIFS. 2018.2844854, IEEE.

[17] Krishna Dharavath et al., "Study on Biometric Authentication Systems, Challenges and Future Trends: A Review", 2013, IEEE.

[18] Sunyanan Choochotaew, Krerk Piromsopa, "An Analysis of Authentication Models for MANETs", 2014, IEEE.