Improved Data Security System Using Hybrid Cryptosystem

Akshay Tarade, Prof. Ashwini Khillari.

Abstract- Cloud As information is send and receive through the planet Wide Web, it becomes subject to inspection and access by unauthorized parties from different a part of the planet since it contains vital and personal content which will be use for fraudulent purpose. As a result, data privacy requires more attention so as to scale back data loss and pilfering. Cryptography is one amongst the favored means of protecting information so as to realize data integrity, authentication, confidentiality, accountability, accuracy and digital signatures. Symmetric & Asymmetric are the 2 main categories of cryptography algorithms wont to protect data using the required key. Asymmetric algorithms are analysed by researchers to be stronger compared to Symmetric algorithms but has higher time complexity. Previous research shows that the loophole of a specific method or algorithm will be solved or minimized by another method or algorithm. Therefore, this paper proposes a technique to enhance data security and reduce the encryption and decryption speed of El-gamal algorithm for giant volume of knowledge using hybridization of El-gamal and Blowfish algorithm. The expected outcome of the proposed method is to realize a safer encryption technique to guard vital documents with faster encryption and decryption speed compare to El-Gamal algorithm.

Keywords -- Algorithm, Ciphertext, Encryption, Decryption, El-gamal, Blowfish

———————— ◆ ————————

INTRODUCTION

Cryptography may be a subject within the field of mathematics that's applied in applied science to confirm the protection primitives . it's accustomed achieve many purposes like security, data integrity, non repudiation, authentication, and digital signature. It involves encrypting the initial information to provide “cipher text” that's not easily interpreted by anyone . The aim of cryptography is to render data during a form that's unreadable by attacker or unauthorized users[1]. There are two categories of cryptography techniques which are symmetric key and asymmetric key . In symmetric key, one key called secrete key's use for data decryption and encryption operation. Some well-recognized secrete key algorithms are 3DES (Triple encryption standards), DES (Data Encryption Standard), AES aka Rijndael (Advanced Encryption Standard) , The International encryption Algorithm (IDEA), Ron's Code (RCn).

- *Akshay Tarade is currently pursuing masters degree program in Information Technology in Mumbai University, India, PH-9987506606.. E-mail: akshay- tarade4254@gmail.com*
- *Ashwini khillari is currently a head of depatment in PHCASC, Rasayan, India, PH-9860809283. E-mail: kashwini@mes.ac.in*

Some asymmetric algorithms are Pretty Good Privacy (PGP, with versions using Diffie-Hellman keys and RSA) , Rivest, Shamir and Adleman (RSA), Elliptic Curve (EC), Diffie-Hellman (DH) , SSL (used for security between an internet browser and server) and SSH (an alternative to telnet) .

Methods*:*

A. BLOWFISH ALGORITHM

Blowfish was designed by Bruce Schneier in 1993; it's one in all the accepted symmetric key block cipher and encompasses a large volume of cipher suites and encryption output. Blowfish offers a awfully good encryption performance rate and no standard cryptanalysis is successful on that [4]. It is a drop-in substitute for DES or IDEA. Blowfish algorithm has two parts , the primary part is vital expansion and also the second is encryption.

The Blowfish key expansion involves splitting the first key into series or set of sub keys. Primarily, a key of 448 bits or lesser is split into 4168 bytes. there's a P-array furthermore as four S-boxes of 32-bit each. The P-array have sub keys of 32-bit which are 18 in number and every S-box has entries of 256 .

1a. Blowfish Algorithm Encryption

The Steps involves:

I: Partition x into two equal 32-bit that is, xLH and xRH.
II: where ni = 1,2,3,4 ...., 16, perform;
xLH = xLH XOR Pni
xRH = F(xLH) XOR xRH exchange xLH and xRH
III: After the last (16th) round exchange xLH and xRH
IV: xRH = xRH XOR P I 7 xLH = xLH XOR P18
V: Finally recombine xLH and xRH.

1b.Blowfish Algorithm Decryption

The decrypt process is just synonymous to encryption process, but the P1, P2, P3, P4 ....., P18 are used starting from P18 to P1.

B. EL-GAMAL ALGORITHM

El-Gamal algorithm belongs to the category of asymmetric cryptosystem and is base on elliptic curve encryption system . it's also such as the Diffie-Hellman system and widely used for encryption further as digital signatures. Its security relies on computation of discrete logarithm finite field. The bigr feature of El-Gamal is in encryption stage, the output (ciphertext) is twofold longer compare to the related plain text. The encryption create a random N of cipher text. That is, if a specific plain text is encrypted in two different occasions; the generated ciphertext won't the identical, which renders ordinary text matching attack invalid. Its loop hole involves, long cipher text (generally twice the plain text) and this algorithm encryption operation consume time.

Encrypt message M:
Select random k such that k< Pn-1

a= gk (mod(Pn))
b = xkM(mod(Pn))

Decrypt message M

M = (b/xk)(mod(Pn)) = (b/gyk)(mod(Pn)) = (b/ay)

Message signature

Select random k that are prime with p-1
Compute b: M = (ya + kb)(mod(Pn-1))
Signature (M) = (a, b)
Confirm signature:
(xaab)(mod(Pn)) = (gm)(mod(Pn))

Results:

The strength of any information security technique like cryptography depend upon simplicity and therefore the probability to carryout it cryptanalysis. Several cryptanalys is are distributed on both symmetric and asymmetric algorithm and therefore the fact is, the loophole of a selected method or algorithm may be solved or minimized by another method or algorithm. The proposed hybrid cryptosystem is predicted to improve El-Gamal algorithm performance speed in terms of encryption and decryption for giant volume of information.

Message Size	**RSA**	**El-Gamal**
1KB	0.00326 sec	0.02697 sec
2KB	0.00346 sec	0.03959 sec
5KB	0.00829 sec	0.06758 sec
10KB	0.01669 sec	0.12194 sec
20KB	0.03186 sec	0.23498 sec
Average Time	0.01085 sec	0.06908 sec
Throughput (Mega Bytes/sec)	4.05069	0.63622

Table: Expected Results

Conclusion:

In this research, we propose a cryptography method to boost data security over a network. The network or transmission medium that's considered for communication is termed to be unsecure. The hybridize system develop by this study write of both asymmetric and symmetric cryptography technique using El-Gamal and Blowfish algorithm. In this research, Blowfish generates a secret key which is use to encrypt the message containing private data or information that the sender intends to send to the receiver and pass the key key to El-Gamal algorithm. El-Gamal algorithm continue the protection processing employing a pair of mathematically related, called private key and public key before the message is distributed to the receiver. Figure 1 shows the pictorial view.

Despite the existence of various spy applications across the web, the proposed system will enable internet users to send and receive data and knowledge during a secure way without worrying of intruder across the network.

References :

[1]. Abari Ovye John, P.B. Shola, & Simon Philip (2015). Comparative analysis of discrete logarithm and RSA Algorithm in data cryptography. International Journal of Computer Science and Information security. (ISSN 1947-5500 Volume 13– No.2, 2015)

[2]. Ankush Sharma, Jyoti Attri, Aarti Devi & Pratibha Sharma. (2014). Implementation & Analysis of RSA and ElGamal Algorithm. Asian J. of Adv. Basic Sci.: 2(3), 125-129 ISSN (Online): 2347 – 4114

[3]. Boomija M.D. & S.V. Kasmir Raja (2016). Secure data sharing through Additive Similarity based ElGamal like Encryption. International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16). 978-1-4673-9745-2 ©2016 IEEE

[4]. Chaitali Haldankar & Sonia Kuwelkar (2014). Implementation of AES and Blowfish algorithm. IJRET: International Journal of Research in Engineering and Technology. Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014, eISSN: 2319-1163 | pISSN: 2321-7308. Available @