IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 7 (July. 2013), ||V2 || PP 30-33

Diffie-Hellman Protocol Based on Elgamal and AES Cryptosystems

E. M. Islas-Mendoza[1], C. A. Jiménez-Vázquez[2], V. M. Silva-García[3], R. Flores-Carapia[4]
[1234]Instituto Politécnico Nacional, CIDETEC, México

Abstract : **-** This paper presents a communication scheme design for securing messages through local area networks (LAN). This scheme implements a hybrid cryptosystem which is formed by AES-256 in its symmetric part and ElGamal for encryption of keys where the prime has 400 digits and 200 digits for the alpha primitive. It also applies the Diffie-Hellman protocol for key secure distribution. This implementation is targeted at senior management members or groups of any corporate trust where the number of users is small. Key distribution requires a number equal to the number of rounds for at least one user.

Keywords: **-** AES, Diffie-Hellman protocol, discrete logarithm, encryption, Elgamal.

I. INTRODUCTION

Technology in communication networks has been increasing over the years and is the reason for the need to have security plans that protect information transmitted through these networks and especially in a business context as these provide a rapid and timely exchange of information. However, the networks have the problem of insecurity because, if they are accessed without authorization, the messages can be intercepted and / or altered. Because of this, for communication between two or more people it is necessary that a message be encrypted for secure exchange of information. Therefore, this work proposes a scheme based on hybrid cryptography because with this we bring together the strengths of symmetric and asymmetric cryptography to encrypt messages quickly using the AES-256 and encrypting its encryption key using the ElGamal asymmetric cryptosystem and distributing the key safely using the Diffie-Hellman protocol.

In literature one can find various works such as [1], which makes four proposals to increase the level of security of free license software for encryption and digital signatures. These proposals involve the incorporation of a hybrid cryptosystem, which uses Elliptic Curve and Elgamal as a basis for their different proposals for improvement. Also, works are found on modifications for standard encryption algorithms as [2] which performs an implementation of symmetric encryption algorithm AES hiding the encryption key by a combination of encryption tables with random bijections, achieving compositions instead of individual steps in the encryption process. Moreover, there are works for security analysis to cryptographic algorithms such as [3], which is divided into two sections. The first section focuses on an analysis of the current state of security for the Diffie-Hellman protocol. The second section analyzes two protocols on key exchange similar to Diffie-Hellman, which are used to generate automorphism exchanging keys.

II. PRELIMINARIES

The Diffie-Hellman protocol was developed by Whitfield Diffie and Martin Hellman in 1976 and is used for exchanging keys between the different users involved in group communication, this through an insecure channel [5]. Particularly used in order subsequently to establish a common key, this will be used as the encryption key for a period of time (Session).

The ElGamal algorithm was proposed in 1984 by Elgamal Taher, which consists of an asymmetric cryptographic scheme that is used for key generation and encrypting and decrypting messages. This scheme is based on the idea proposed by Diffie-Hellman, which also uses the discrete algorithm problem $\beta=\alpha^a \bmod p$. The primitive α is calculated using the theorem that states the following: given two integers a, b with gcd(a, b) = 1, such that a, b are relatively prime, then one can construct an infinite number of primes with the form n (a) + b [7].

The AES (Advanced Encryption Standard) is a block encryption scheme known by the name "Rijndael" by its two developers, the cryptologists Joan Daemen and Vincent Rijmen and which was sent under this name to the selection process AES. This symmetric encryption scheme was the winner announced by the National Institute of Standards and Technology (NIST) as its encryption standard (FIPS PUB 197) in 2001 [8]. Currently this encryption standard remains in effect. The AES encryption scheme has a length of 128 bits in the block cipher and the key length can be 128, 192 or 256 bits and for each of these, AES assigned 10, 12 and 14 encryption iterations respectively.

III. PROPOSED MODEL

The following describes the proposed hybrid cryptosystem for this work, which in turn employs asymmetric Elgamal and its AES-256 symmetric part of a secure key exchange protocol based on the Diffie–Hellman protocol.

1. All participants in the conversation share public keys 'p' and 'α' of 400 and 200 digits respectively. For the strength of the cryptosystem, these keys will be fixed.
2. Each participant generates its private key a.
3. The rounds of key exchange are initialized under the Diffie-Hellman protocol, sending the encrypted keys by ElGamal. The number of rounds dependent on the number of participants involving at least one communication, i.e., when n participants are involved, the number of rounds is n-1.
4. At the end of the rounds, calculating the β end or total, will be the same for each participant.
5. From the β end or total, take the first 256 bits that will be the session key with which the messages are encrypted with AES-256.
6. If a participant joins the conversation, start from step 2. And if a participant withdraws from the conversation, start from step 3.

   Fig. 1 shows how to set the session key between two participants by exchanging keys under the Diffie-Hellman protocol, sending encrypted keys with ElGamal

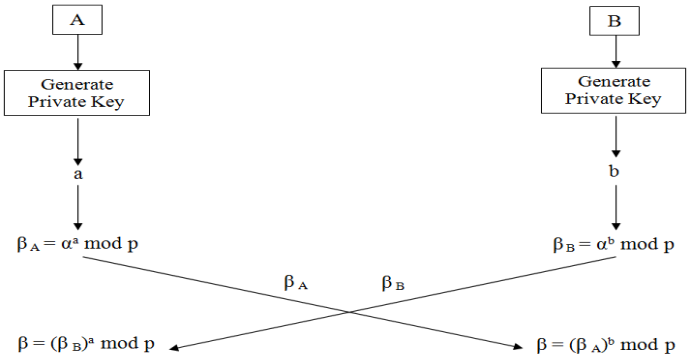

Figure 1: Communication between two participants

Fig. 2 is presented as establishing the session key for three participants under the same methodology.

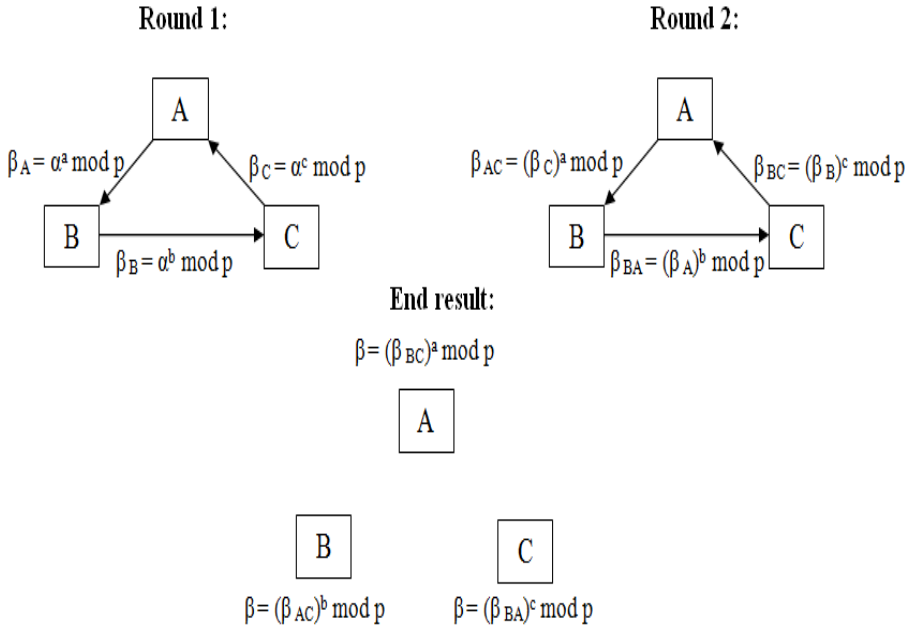

Figure 2: Communication between three participants

The implementation of the proposed cryptosystem was developed in compliance with the client-server model, where the characteristics of each process are as follows:

The client process will perform the following functions:

1. Manage User Interface
2. Interact with the User
3. Process the rounds of key exchange using Diffie-Hellman encrypted using SSL with ElGamal
4. Generate the secret key for AES-256 for encryption and decryption of messages
5. Send encrypted messages to the server
6. Receive and decode messages from the server
7. Have general messaging (for all clients) and private (for a particular client)

In addition the client must request two parameters at the beginning of each session; first ask the master key to access the group conversation, which denominate as "Session Master Key". And secondly, the user is prompted to enter the IP address of the server.

Moreover, once logged in it can be accessed by generated keys for talking, only with a second master key, which will be known as "Master Key Delta".

The server process will perform the following functions:

1. Receive messages from clients
2. Check the type of message received either general or private
3. Transmit messages to clients

This process may be performed by any member of the group when starting a chat session previously agreed by the group.

IV. EXPERIMENTAL RESULTS

In this section we present the results obtained from the tests conducted in software obtained from the implementation of the security scheme proposed in this work. The tests consisted mainly in measuring the time taken to perform key exchange between the numbers of participants that are in the conversation. Since the mathematical operations that are performed for encryption key exchange are very large, this increases if the number of participants grows, plus it increases the number of rounds to exchange keys. Table 1 provides our results.

Table 1: Results of the test.

Number of participants	Response time
3	0.47 seconds
5	1.0 seconds
10	3.5 seconds
15	5.0 seconds

The time obtained in the first test (with three participants) was 0.47 seconds, i.e., imperceptible to the user, resulting in a good time for this case. In the second test (five participants) where time obtained was 1 second, resulting in a good time.

In the case of the third test (with ten participants), the time obtained was 3.5 seconds, which is a considerable time waited by the user, unlike this one, with the fourth test (with fifteen participants) obtaining a time of 5 seconds and this can be uncomfortable for the user.

Fig. 3 shows graphically the time it takes for the software to complete the key exchange rounds based on the number of participants in the conversation, taking the results of the tests performed.

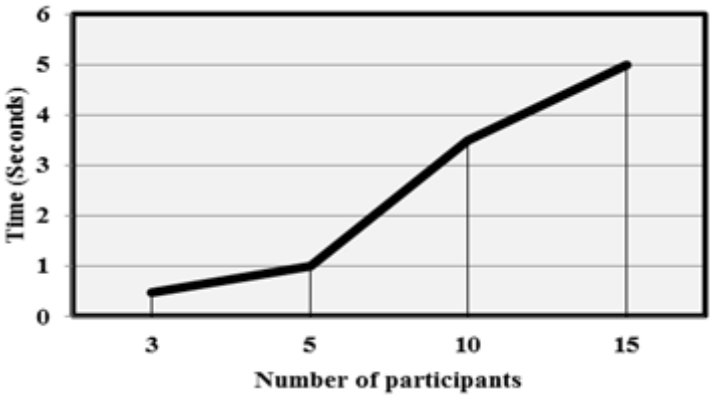

Figure 3: Graphic Behavioral of tests.

The times obtained in the tests, met the expectations of this scheme, as it is aimed at senior management members or groups of any corporate trust where the number of users is small. It is worth noting that for all cases, the time for sending/receiving messages between participants is instantaneous when encrypting and decrypting messages using AES-256 with the already established session key, i.e., the process where the system delay is in the key exchange rounds where time varies depending on the number of participants.

V. CONCLUSIONS

With the results of the tests conducted in software obtained by implementation, the performance adequately corroborates the process, since tests were applied with different amounts of users connected to the same conversation and the times obtained met the expectations raised.

Therefore, it was concluded that the design and implementation of this scheme for secure communication over networks is fully functional for senior management members or groups of any corporate trust where the number of users is small. Initially, it was expected that the maximum recommended number of users was fifteen participants, but based on the results of tests performed in section IV, it is recommended that the number of users participating in the conversation must not exceed ten for the system to provide good response times for the user.

VI. ACKNOWLEDGEMENTS

The authors would like to thank the Instituto Politécnico Nacional (Secretaría Académica, COFAA, SIP, Proyecto SIP-20130156 and CIDETEC) and the CONACyT for their economic support to develop this work.

REFERENCES

[1] S. B. Torné y R. C. Moreno, Análisis del cifrado ElGamal de un módulo con curvas elípticas propuesto para el GnuPG, Escuela Politécnica Superior, España, Reporte científico, 2007.
[2] S. Chow, P. A. Eisen, and H. Johnson, White-Box Cryptography and an AES Implementation, Cloakware Corporation, Ottawa, Canadá, Scientific report, 2003.
[3] Mahalanobis, Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups, Universidad de Atlantic Florida, Report, Agosto 2005.
[4] A. Arteaga, ElGamal, Facultad de Ingeniería - Universidad Nacional Autónoma de México, México, Reporte técnico, 2012.
[5] D. Whitfield and E. M. Hellman, New directions in cryptography, IEEE Transactions on information theory, vol. IT-22, 1976.
[6] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, vol. IT-31, 1985, 469-472.
[7] V.M. Silva-García et al, A Reinforced ElGamal Scheme Proposal Against a Pohlig-Hellman Attack, Applied Mathematical Science, Vol. 7, 2013, 2909 – 2916.
[8] Advanced Encryption Standard, FIPS PUB 197, 2001.