2019 IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E)
Bali, Indonesia, November 13-15, 2019

2019 IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E) | 978-1-7281-3134-4/19/$31.00 ©2019 IEEE | DOI: 10.1109/TIME-E47986.2019.9353292

Hybrid Algorithm Combining Modified Diffie Hellman and RSA

Junnel E. Avestro
Technological Institute of the Philippines- Quezon City
Quezon City, Philippines
javestro.it@tip.edu.ph

Ariel M. Sison
Emilio Aguinaldo College
Manila, Philippines
ariel.sison@eac.edu.ph

Ruji P. Medina
Technological Institute of the Philippines- Quezon City
Quezon City, Philippines
ruji.medina@tip.edu.ph

***Abstract*—The Classic Diffie-Hellman (CDH) algorithm encounters several security problems. The algorithm security depends on the complexity of solving the discrete logarithm and the integer factorization problem. The security also depends on the length of bits keys used. In this paper, we proposed a hybrid algorithm, the combination of Modified Diffie Hellman (MDH) with the Rivest, Shamir, and Adelman (RSA) algorithm. The MDH will not use primitive root (g). Instead, it will use two prime numbers (P and Q) for key exchange. It reduces the possibility of a man-in-the-middle attack. Furthermore, the MDH has an authentication mechanism. If both shared keys are equal, the communication will continue. Otherwise, it will stop because it is compromised. Also, the RSA algorithm will use the two prime numbers generated by MDH (P and Q). The RSA algorithm will perform the encryption and decryption message. The Diffie Hellman (DH) and the RSA Algorithms are the basis of several security standards and services on the internet, especially TLS and SSL. If the security of both algorithms is compromised, such systems will collapse. In this proposal, the combined cryptography system aims to achieve secret message exchange; it uses random prime numbers after multiplication and eventually shared with the other end of a communication. The proposed algorithm secretly generate a value so that the security level increases**

Keywords— Diffie Hellman, RSA, Public Key Pair Based Authentication.

I. INTRODUCTION

In the smart digital environment, data security plays a prominent role in data transmission through communication channels. To make the data secure, the information should not be available or disclosed to unauthorized individual's confidentiality, it should be protected from unauthorized modification, and available to authorized individuals as per requirement. The data security considers the confidentiality, availability, and integrity of the data. Cryptography, which is also termed as "secret writing," is the science and art of converting messages into secret texts that are insusceptible to attacks by an unauthorized user. The proliferation of computers and communications systems in the early years has brought with it the means to protect the information in digital form and to provide security against security attacks. [1]

Security is a prime concern when data is transmitted through a wired or wireless communication network. Generally, the operation of cryptography is performed before any transmission, and this involves the action of encrypting the data before sending and then decrypting on receiving. Encryption involves scrambling of data with the use of a particular key and then decrypting it using either the same key or another key, which produces the same effect as inverting the effect of encryption and getting back the original data. [2][3]. DH cryptography is based on the key exchange. Both parties need to exchange secrets key to encrypt the message. Based on the difficulty of computing discrete logarithms. DH is based on symmetric key exchange for both encryption and decryption. DH algorithm does not provide strict authentication. The security of the DH cryptography system completely depends upon the random prime number selected by the user. Finding private keys after accessing public key and prime number P is a logarithmic problem to solve. [4]. The RSA is a form of public-key cryptography that creates a public and secret key using different procedures. RSA is the most common standard of encryption in the computer world. It is most widely used in a web browser, such as net space to email encryption programs. The main purpose of RSA, it was not being proven that breaking the RSA algorithm is equal to factoring large numbers, but neither has been proven the factorization is not equivalent. The different types of attacks on RSA are private key guessing, message space searching, low exponent, cycle attack, final factoring variable N, and common modular, which is factoring the public key and it is the best way to crack RSA[3].

The proposed algorithm is to modify Diffie-Hellman to provide authentication and avoid primitive root generation steps to achieve speed and authentication to prevent key exchange with the unauthenticated user and also aims to make secret message exchange. RSA uses random prime numbers P and Q, which after multiplication, value N is shared to another side of communication. Besides, the security of RSA is dependent on the prime factorization of N, and the proposed algorithm secretly generates a value of N so that the security level increases in the new RSA based cryptography system.

II. LITERATURE REVIEW

A. Diffie Hellman Algorithm

The purpose of the DH protocol is to enable two users to exchange a secret key securely that can be used for subsequent encryption of messages. The protocol itself is limited to the exchange of the keys. But because of having no entity authentication mechanism, DH protocol is easily attacked by the man-in-the-middle attack and impersonation attack in practice. The DH key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to establish together a shared secret key over an insecure communications channel. Then they use this key to encrypt subsequent communications using a symmetric-key cipher.

The scheme was first published publicly by Whitfield Diffie and Martin Hellman in 1976, they use this key to encrypt subsequent communications using a symmetric-key cipher. The DH key arrangement is a non-authenticated key arrangement protocol and considered as one the basis of authenticated protocols. It also used to have perfect forward secrecy in Transport Layer Security's short-lived modes [5].

1. Communication takes place through an insecure channel.
2. The sender and receiver have no prior knowledge of each other
3. Provide a new DH key is very fast
4. Secret key sharing is safe
5. Used Secure Socket Layer (SSL) and Transport Layer Security (TLS)
6. Used in the card payment system
7. Used in ATM network management
8. Used in Secure Shell (SSH)
9. Used in Internet Protocol Security (IPSec)
10. Used in Public Key Infrastructure (PKI)

Fig 1. DH Hardware and Software supported components [9][10].

Figure 1 shows the DH numerous internet applications and how is implemented.

B. RSA Algorithm

The Rivest, Shamir, and Adelman (RSA) is the most widely used cryptosystem around the world. The RSA used in digital signatures, keys exchange, and encrypting data. Many security protocols depend on RSA, such as the TLS protocol, which is used in Internet-based e-commerce. Also, it is used for protecting emails and traffic of the web, and it is used for securing some of the wireless devices and network resources. If there is any leak in the security of RSA, the vulnerability to attacks is higher and it will lead to security breaches in the Internet applications [14][15] [16][17].

RSA_Key_Generation ()
INPUT: Select two random distinct prime numbers a and b.
OUTPUT: Find Public Key (p), Private Key(q), and Modulus (x).
Begin
Procedure (a, b, p, q and x)
1. $x \leftarrow a * b$
2. Calculate Euler Ø () of x Ø (x) $\leftarrow (a-1) * (b-1)$
3. Generate a public key p, such that, gcd (p, Ø (x)) = 1, $1< p < Ø (x)$
4. Calculate the private key q, such that,$q \leftarrow p-1 \bmod (Ø (x))$
End Procedure
RSA_Encryption ()
INPUT: Select Plain text (T), Public key (p) and Modulus (x).
OUTPUT: Find Ciphertext (C).
Begin
Procedure (T, p, x and C)
$C \leftarrow TP \bmod x$
End Procedure
RSA_Decryption ()
INPUT: Select Cipher text (C), Private key(q) and Modulus (x).
OUTPUT: Find Plain text (T).
Begin
Procedure (T, p, x and C)
$T \leftarrow Cq \bmod x$
End Procedure

RSA is a "public key" cryptosystem originated from some mathematical operation. This algorithm used the variable *x,* which is the multiplication of two large prime numbers *a* and *b* [18][19][20].

RSA Supported Software and Hardware
1. Securing electronic communication and online data storage.
2. Provide a method of assuring confidentiality, integrity, & authenticity of electronic communication
3. Use to ensure internet, social media, online shopping & secure personal information
4. It is used in security protocol like IPSEC/IKE, TLS/SSL, PGP, SSH, SILC
5. Used in government and military to secure communication.
6. Used for signing a digital signature
7. Used in a website and web-based application
8. Very fast & simple encryption
9. Easier to implement and understand
10. Widely deployed, better industry support & prevents the third party from intercepting the message.

Fig 2. RSA Hardware and Software supported components [9][11] [12] [13].

Figure 2 shows that RSA has widely used cryptography in a network environment, and it supports the software and hardware.

RSA and DH are the two most important algorithms. This approach will provide more communication security. The RSA algorithm can be used for public-key encryption and digital signature. The DH algorithm is used as a key exchange method that allows two parties that have no proper knowledge of each other to share a secret key jointly. In this approach, the RSA keys were taken as input for DH. The required keys are generated using the RSA algorithm. The DH is used for generating a more secure cipher-text. [6][7][8].

III. Modified Diffie-Hellman Algorithm And RSA Algorithm

The proposed integration of the modified Diffie-Hellman(MDH) algorithm with the RSA algorithm is

divided into two parts. The first part of the MDH algorithm key exchange. The second part is it uses the RSA algorithm to encrypt and decrypt the message, but both sides two keys are generated with the RSA approach, and keys are called as sender key for encryption and receiver key to decrypt incoming message.

First part: Secret key generation

Secret key generation is using the MDH algorithm. These are the steps:

1. User A generates a random prime number (P), and then it will be multiplied by 2 (Pn).

Therefore Pn = P * 2 (to avoid using primitive root, the value of P will be twice) and sends it to User B

2. The User B receives Pn and calculate it as P = Pn/2 (to return the User A original prime number (P). After this, User B also generates a random prime number (Q).

User B makes Q as Qn = P + Q (to add P to Q) and send it back to User A

3. User A received the number from User B and subtracted P to Qn

User A get Q = Qn-P and assign this value of Qn to Q

B. Authentication process

4. User B Authenticates and Send Public key to user A and receive the value of Qn

Q' = Qn-P and then compare with the value of Q

If Q'==Q are equal, it will continue. Otherwise, it will stop to avoid compromised conversation.

If the value of Q matches then User B generate this public key (PubB)

Select Random Private Prime Number Pb.

PubB = P^{Pb} mod Q

PubB sent to User A

5. User A receives Public Key of User B, and then User A also generates a public key (PubA).

Select Random Private Prime Number Pa

PubA = P^{Pa} mod Q

PubA sent to User B

6. User B receives the Public Key of User A and Secret Key Generation process

SecKb = $PubB^{Pa}$ mod Q

7. User A Secret Key Generation Process

SecKa = $PubA^{Pb}$ mod Q

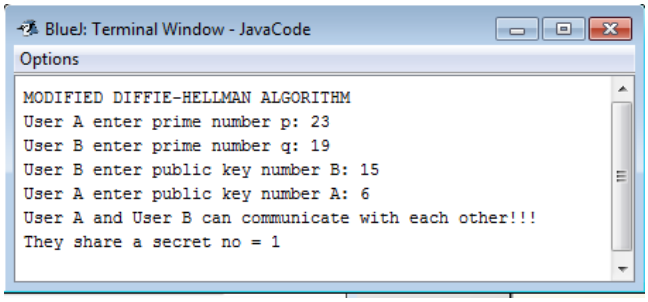

Fig 3. The MDH Algorithm Simulation.

Figure 3 shows the simulation of MDH using Java programming. It allows the user to input two prime numbers, public keys, and generates secret keys. If the secret key is equal, the communication will continue. Otherwise, it will stop the conversation.

Second Part: Sender key and Receiver Key Generation

The sender key will be used for message encryption while the Receiver key will be used for decryption to the receiver message.

8. Calculate the new Prime number (Pnew)

For User A

Pnew = P x SecKa (the value P originated from step 1, and SecKa)

Find next prime of Pnew & which new value of P of User A

P = next prime(Pnew)

For User B

Pnew = P x SecKb (SecKb originated from step 6)

Find next prime of Pnew & which new value of P of User B

P = next prime(Pnew)

Notice that equation 3.1 and 3.2 are the same value because the secret key must identical in both User A and User B

9. Calculate new Q

For User A

Qnew = Q x SecKa (the value of Q originated from step 2 and SecKa)

Find the next prime of Qnew, which the new value of Q at User A

Q = nextPrime(Qnew)

For User B

Qnew = Q x SecKb (SecKb originated from equation 1)

Find the next prime of Qnew, which the new value of Q at User B

Q = nextPrime(Qnew)

The RSA Algorithm

The values of Prime number P and Q respectively originated from MDH to avoid RSA to generate random prime numbers to increase security.

10. Calculate the value of N and φN

N = P x Q

φN = (P-1)x(Q-1)

11. Choose e such that 1 < e <φN and e and N are co-prime

12. Compute the value for d such that d x emodφN = 1

13. Sender key is (e, N); Receiver key is (d, N)

14. The Encryption of message (m) is

c = m^emod N

15. The Decryption of message (c) is

m = c^d mod N

It completes the process of a hybrid cryptosystem. In this process, the MDH performs key exchange to establish communication on both parties and also provides authentication. The next step is the RSA receives the prime number values (P and Q) from MDH. In this way, RSA will no longer generate prime numbers (P and Q). It also increases the security to encrypt and decrypt messages.

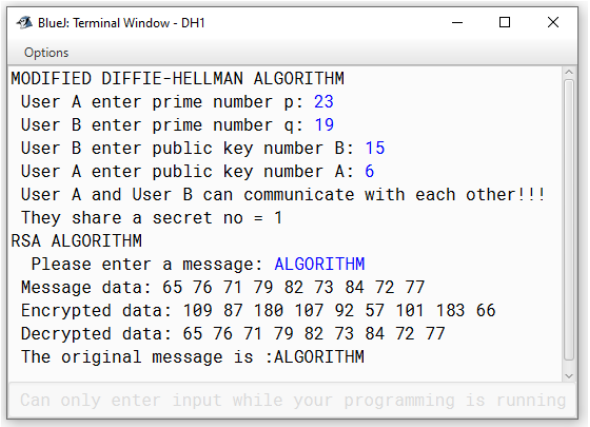

Fig 4. Integration of MDH and RSA algorithm

Figure 4 shows the MDH and RSA algorithms. The first part is the MDH. It allows the user to input two prime numbers, public keys, and generates a secret key. The second part is the RSA algorithm uses the two prime numbers (P and Q) generated by MDH. The program allows the user to compose message data, encrypt, decrypt, and return the original message.

IV. Performance Analysis

The MDH and CDH algorithm comparison based on the following criteria: using 64-bits,128-bits, 1024-bits, and 2048-bits symmetric keys lengths

TABLE I. MDH AND CDH COMPARISON

Symmetric key	**MDH**	CDH	Time Difference
64 – bits	**27.72387 sec**	88.58767 sec	68.70 %
128– bits	**66.71367 sec**	165.552 sec	59.70 %
512– bits	**271.9631 sec**	603.8776 sec	54.96 %
1024– bits	**1722.826 sec**	2450.669 sec	29.70 %
2048– bits	**18551.22 sec**	23352.92 sec	20.56 %

Table I shows the comparison of the performance of MDH and CDH. The result MDH much faster among symmetric keys.

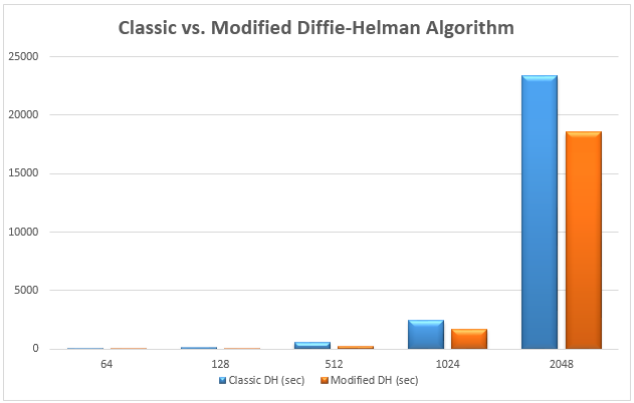

Fig 5. MDH and CDH Graph Comparison

Figure 5 shows the performance comparison of the classic and the modified algorithms in terms of run time. It indicates that MDH is faster in all symmetric key length ranging from 64-bits up to 2048 bits since the modified DH does not require to generate primitive root. The time needed is significantly shorter compare with CDH in different symmetric key lengths. Since RSA choose two big prime number (P and Q), the key generation is slow. To increase the speed of the key generation, the manufactures need to design devices with a faster processor so that the key generation is fast and is reliable. It will also solve the problem of slow signing and decryption. Another option would improve the speed of the key generation would be doing some modification to two big prime numbers. By selecting a random big number could increase the speed of key generation. The proposed algorithm will use the two prime numbers generated by MDH to speed up the keys needed by RSA. In that way, it gets faster key generation, encryption, and decryption of messages. The throughput in the actual scenario gets better. More transactions will be accommodated

V. Conclusion And Recommendation

The proposed algorithm is a secure and detail process of a cryptosystem. It is easy to understand and more secure as the complexity of the algorithm is a logarithmic problem to solve. Security of RSA depends on the prime factorization of N. The proposed algorithm authenticates a user as shown is the first part of the algorithm by exchange value of random P and Q. Another strength of the hybrid algorithm, it will not generate primitive root (g). Then generate secret keys at both sides. Secret keys not known or not sent over a communication channel, so eavesdropper has no chance to get the value of the secret key. The secret key is multiplied to P, and hence new P will be not identifiable to attacker though the value of P gets compromised. This value of P and Q is generated secretly at the user side, and this valued is not shared through the communication channel, so we claim that the proposed method is more secure than the original RSA. The disadvantage of the proposed algorithm has extra steps that mix symmetric key and asymmetric key cryptography. The time required for this integration steps is disadvantageous of this proposed method. But we can achieve better security

The proposed algorithm is secure. It encrypts and decrypts the message with secretly generated sender key and receiver key, which is known to the sender and receiver. Two-level of securities are implemented. The algorithm is based on hybrid cryptography as it uses asymmetric that is the sender and receiver key and symmetric key that is both the user A and use B uses the same key pair for encryption and decryption.

References

[1] W. Stallings, Network Security Essentials, 4th ed., New York: Pearson Education, Inc, 2011.

[2] Stallings, W., "Cryptography and Network Security Principles and Practices Fourth Edition," Prentice-Hall, New Jersey, 2005.

[3] Rajeshwaran et al., 2017. Secured Cryptosystem for Key Exchange.2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)

[4] Mogos, G., 2016. Use Quantum Random Number Generator in Diffie-Hellman Key exchange protocol.2016 IEEE International Conference on Automation, Quality and Testing, Robotics(AQTR)

[5] Nilesh Lal. 2017.A Review of Encryption Algorithms RSA and Diffie Hellman. International Journal of Scientific & Technology

[6] Nan Li. 2010. Research on Diffie-Hellman Key Exchange Protocol. 2nd International Conference on Computer Engineering and Technology

[7] David Adrian et al., 2015. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, CCS'15, October 12–16, 2015, Denver, Colorado, USA. ACM 978-1-4503-3832-5/15/10.

[8] Nilesh A. Lal 2017, A Review Of Encryption Algorithms RSA and Diffie Hellman, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 07, JULY 2017, ISSN 2277-8616.

[9] E. E. Classes, "Diffie Hellman Key Exchange in Hindi for Symmetric Key Encryption System –With Example," 2016. [Online]. [Accessed 24 03 2017]. Available: https://www.youtube.com/watch?v=_M2Ea_3DRGA.

[10] K.Suganya, "Performance study on Diffie Hellman, "International Journal for Research in Applied Science, vol. 2, no. 3, pp. 68-75, 2014.

[11] F. H. a. F. R. Michael Cobb, "RSA algorithm (Rivest Shamir Adleman)," 2014.[Online].Available:http://searchsecurity.techtarget.com/definition/RSA. [Accessed 24 03 2017]

[12] H. M. J. Ali Makhmali, "Comparative Study On Encryption Algorithms," International Journal of Scientific & Technology Research, vol. 2, no.6, p. 44, 2013.

[13] D. Chauhan, "RSA and Diffie Hellman Algorithm," 2016 [Online].Available:https://www.slideshare.net/daxeshchauhan/rsa and Diffie hellman algorithms 64170629. [Accessed 24 03 2017].

[14]. A. Karakra and A. Alsadeh, "A-RSA: Augmented RSA," 2016 SAI Computing Conference (SAI), London, 2016, pp. 1016-1023.

[15]. N. M. S. Iswari, "Key generation algorithm design combination of RSA and ElGamal algorithm," 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, 2016, pp. 1-5.

[16]. B. J. S. Kumar, A. Nair, and V. K. R. Raj, "Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2017, pp. 1057-1060.

[17]. A. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms," 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), Baghdad, 2016, pp. 1-6.

[18]. A. Chaouch, B. Bouallegue and O. Bouraoui, "Software application for simulation-based AES, RSA and elliptic-curve algorithms," 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Monastir, 2016, pp. 77-82.

[19]. P. K. Panda and S. Chattopadhyay, "A hybrid security algorithm for RSA cryptosystem," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-6.

[20]. P. M. Aiswarya, A. Raj, D. John, L. Martin, and G. Sreenu, "Binary RSA encryption algorithm," 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, 2016, pp. 178-181.