A hybrid model to secure the exchange of DH keys

Abdellahi Ahmed
Department of Mathematics and Computer Science
FST / Cheikh Anta Diop University (UCAD)
Dakar, Senegal
abdellahiahmedcheikh@gmail.com

Mohamedade Farouk Nanne
Department of Mathematics and Computer Science
FST / University of Nouakchott Al Aasriya (UNA)
Nouakchott, Mauritanie
Mohamedade@gmail.com

Bamba Gueye
Department of Mathematics and Computer Science
FST / Cheikh Anta Diop University (UCAD)
Dakar, Senegal
bamba.gueye@ucad.edu.sn

Abstract— **The Diffie-Hellmann(DH) algorithm is an algorithm that allows the exchange of secret keys, shared via a channel that is not necessarily secure to ensure communication between two users. When exchanging DH keys, none of the users have proof that they are communicating with the right interlocutor, because the shared keys can be detected by a "Man in the middle". In this article, we propose a model called DRA which combines the three encryption algorithms DH, RSA (Rivest Shamir and Ademann) and AES (Advanced Encryption Standard), it aims to improve the security of DH key exchange especially with the evolution of computing power and computer speeds. The results obtained in this article show the efficiency of our model compared to the S-SEJAD model which itself has brought a real improvement compared to existing solutions such as S-WANE, New-Two-Pass, STS, HMQV.**

Keywords: Diffie-hellmann, RSA, AES, main in the middle

I. INTRODUCTION

Cryptography is the exchange of secret messages between two parties to secure confidentiality, integrity and authentication and involves both encryption and decryption [1]. Before the emergence of cryptography, security has always been the main concern. Symmetrical and asymmetrical encryption algorithms have provided solutions to most of the security problems, among the proven algorithms we can cite Diffie-Hellmann's algorithm which is used in several domains (DNS [2], IPV6 [3], SSH [4] ...). Our objective in this paper is to study the reliability of the DH algorithm to ensure secure transmission of encryption keys between users. Our article is based on several major points, we start with the presentation of asymmetric cryptography and a comparison between its different algorithms, the second section will be devoted to the DH algorithm and its operating steps, the third section contains a presentation of the RSA algorithm and their operating principle, the fourth section contains a presentation of symmetric cryptography and a comparison between its different algorithms, the fifth section contains a presentation of the AES algorithm and their encryption process, the sixth section contains a general presentation of the DRA model and its operating principles, and before concluding we will present the efficiency of our proposed DRA model compared to existing models.

II. ASYMMETRIC CRYPTOGRAPHY

An algorithm is said to be asymmetric if and only if it has two encryption keys, one being public, issued by the sender to allow his interlocutors to implement reciprocal operations such as encrypting messages, the other is private allowing the sender to perform operations that only he is supposed to be able to do. This method is more convenient and ensures better authentication and confidentiality of messages [5].

There are several asymmetric encryption algorithms such as, RSA, Diffie-Hellman, ECC and digital signature algorithm.

TABLE I. COMPARISON TABLE FOR DIFFERENT ASYMMETRIC KEY ALGORITHMS [5]

Method	**Rivest-Shamir-Adleman (RSA)**
Features	General form is (d, e) where d represents the private key and e represents the public key. Both encryption and decryption uses the same function.
Advantages	It is difficult to produce the private key from the public key and modulus; thus it is highly secure. Computing the reverse of e is very difficult for the attackers.
Downsides	Complexity of generating the key. The process is quite slow. It has not been proved that it is equivalent to the factorization method and factorising a large number is very difficult.
Security Solutions	Key length should be larger than 1024 bits.
Method	**Diffie-Hellmann**
Features	It is based on sharing the secret cryptographic key. This key is used for both encryption and decryption purposes. It relies on hardness of the discrete logarithms.

Advantages	As the symmetric key is of very short length (256 bits), the algorithm is quite fast.
Downsides	The longer the symmetric key is used the more attacks it will face. More vulnerable to Man in the Middle attacks.
Security Solutions	Frequent key changing is essential. Development of Station-to-Station protocol defeats Man in the Middle attacks. The development of digital signature is also a solution to the attacks.
Method	**Elliptical Curve Cryptography (ECC)**
Features	It computes the keys through elliptic curve equations.
Advantages	It can yield security using a 164-bit key and is more advantageous than RSA and Diffie Hellman algorithms. It consumes less power and provides better utilities to batteries.
Downsides	It increases the size of encrypted message and is more complex and difficult to implement, compared to RSA.
Security Solutions	Introduction of Elliptic Curve Digital Signature Algorithm (ECDSA). The Authenticated key agreement protocol, ECMQV protects against Man-in-the-Middle attacks.
Method	**Digital Signature Algorithm (DSA)**
Features	It consists of a pair of large numbers, computed based on some algorithms to authenticate data. The signatures are generated through private keys and are verified using public keys.
Advantages	It is very fast and provides non- repudiation and authenticity. It secures the data against various attacks like Man-in-the-Middle attacks and is more advantageous than other asymmetric key algorithms.
Downsides	Digital signatures have short life span. They are not compatible with each other and thus complicate sharing.
Security Solutions	Verification software is necessary. Digital certificates should be bought from trusted authorities.

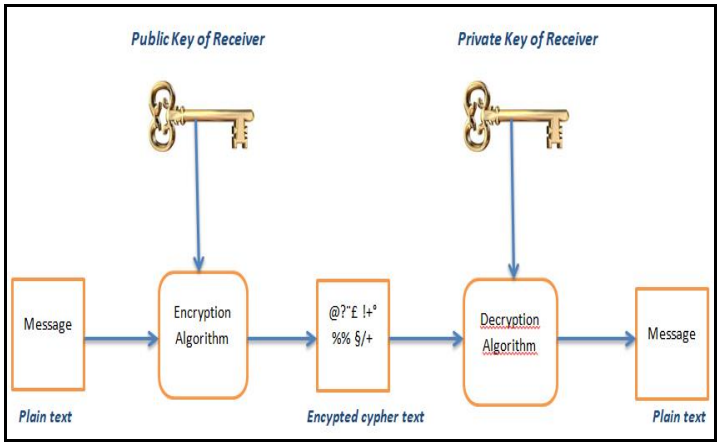

Figure 1. Asymmetric Cryptography

III. DIFFIE-HELLMANN ALGORITHM

The Diffie-Hellmann(DH) algorithm was discovered by Whitfield Diffie and Martin Hellman in 1976. The key exchange method allows two users X and Y, who do not know each other a priori, to exchange a shared secret via an unsecured communication channel.

The key exchange processes of this algorithm are summarized by the following steps:

1. X and Y choose two numbers p and g, p being a prime number and g an integer less than p.
2. X chooses a secret number a and Y chooses a secret number b.
3. X calculates the public key according to the formula $X_a = g^a \bmod p$.
4. Y calculates the public key according to the formula $Y_b = g^b \bmod p$.
5. X and Y exchange their public keys.
6. X calculates its private key according to the formula $\mathbf{k_a} = \mathbf{(Y_b)}^{\mathbf{a}}$ and Y calculates its private key according to the formula $\mathbf{k_b} = \mathbf{(X_a)}^{\mathbf{b}}$.
7. X and Y cannot communicate when they both know the number representing the value of k_s in the formula $\mathbf{k_{a=}\ k_{b=}\ k_s}$.

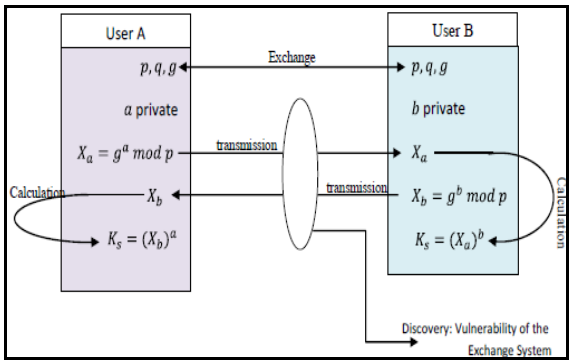

Figure 2. Diffie-Hellmann Exchange vulnirability [6]

IV. RSA ALGORITHM

The RSA algorithm is an asymmetric encryption algorithm widely used in electronic commerce, above all in the exchange of confidential data on the Internet; it was discovered in 1977 by Ronald Rivest, Adi Shamir and Len Adelman [7]. It is the first algorithm that can be used for both message encryption and digital signatures [8]. Each user has a public key used to encrypt messages, and which he can share with other users. Each user may or may not have a private key that is used to decrypt messages. The processes for exchanging keys are detailed below:

1. Random selection of two distinct prime numbers p and q, of the same bit length.
2. Calculation of the public key n=p*q.
3. Calculation of φ(n)= (p-1) (q- 1).
4. Choice of an integer e, such as 1<e< φ(n) and pgcd(e, φ(n))=1.
5. Determination of the inverse d of e according to the formula d.e≡1 (mod n).
6. The public key e and the private key d are determined from the five steps above.

V. SYMMETRIC CRYPTOGRAPHY

In symmetrical cryptography, the sender and receiver share the same key for encrypting and decrypting messages. If a middle man can intercept this key, it will be easy for him to decipher the messages.

Symmetric encryption algorithms include AES, DES, 3DES, Blowfish, and others.

TABLE II. COMPARISON TABLE FOR DIFFERENT SYMMETRIC KEY ALGORITHMS [9]

	Symmetric Encryption Algorithms			
	DES	***3DES***	***AES***	***BLOWFISH***
Block Size	64 bit	64 bit	128 bit	64 bit
Key size	56 bit	168 bit	128,192, 256 bit	32-448 bit
Created by	IBM in 197 5	IBM in 1978	Joan Da man- in 1998	Bruce Schneier in 1998
Algorith- m Structure	Fiest- el Netwo -rk	Fies tel Netw ork	Substitution Permutation Network	Fiestel Network
Rounds	16	48	9,11,13	16
Attacks	Brute Force Attack	Theoretica -lly possible	Side Channel Attacks	Not Yet

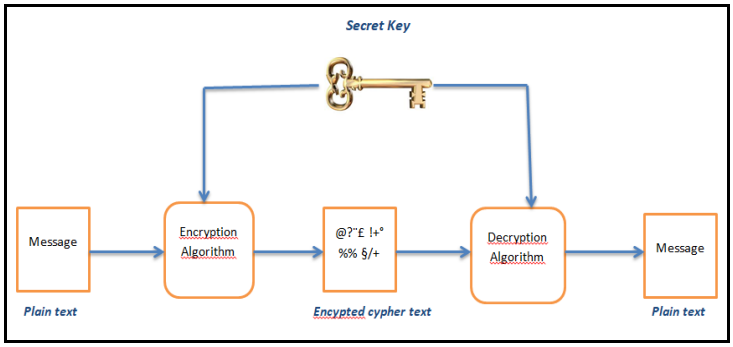

Figure 3. Symmetric Cryptography

VI. AES ALGORITHM

The AES algorithm is a block cipher algorithm, recommended by NIST (National Institute of Standards and Technology) in 2001 to replace DES which was one of the most widely used symmetric encryption algorithms in the world [10]. AES has been, and remains, widely used in many applications, including smart cards, cell phones, web servers and ATMs [11].

The AES algorithm can support any combination of data (128) and all bit-length keys 128, 192 and 256 [12]. It is an iterative algorithm, with each iteration being able to call a round whose total number of rounds is 10, 12 or 14 corresponding to key lengths 128, 192 or 256 respectively [13].

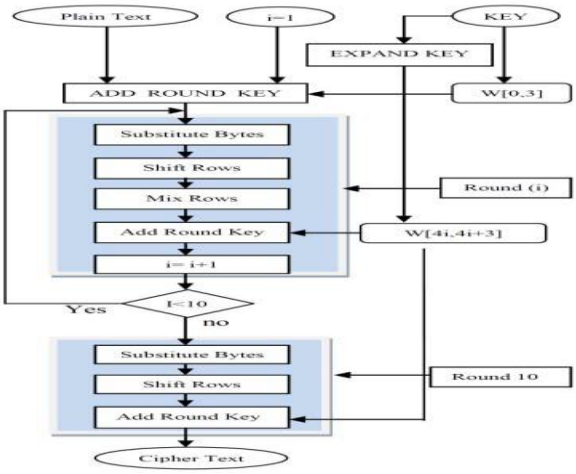

Figure 4. AES Process [12]

VII. DRA MODEL

Due to the growing increase in speed and computing power of conventional computers, and with the appearance of quantum computers with extremely powerful features, it has become necessary to find an original solution that provides maximum security for exchanging DH keys.

The main problem of the DH algorithm lies in the security of key exchange, our proposal through the DRA model consists in a solution based on the combination of the asymmetric

encryption algorithm RSA and the symmetric encryption algorithm AES.

The different steps of the DRA model are as follows:

1. Two user's X and Y share two numbers p and g, p being a prime number and g an integer strictly inferior to p.
2. User X chooses a secret number a and user Y a secret number b.
3. X calculates its public number $\mathbf{X_a} = \mathbf{g^a}$ mod **p** and Y calculates its public number $\mathbf{Y_b} = \mathbf{g^b}$ mod **p**.
4. X and Y exchange their public keys clespubRSA(X) and clespubRSA (Y) and share the numbers p and g, while keeping their private key clespriRSA.
5. . User X encrypts $\mathbf{X_a}$ with the clespubRSA (Y) public key communicated to him by User Y. User Y encrypts $\mathbf{Y_b}$ with the clespubRSA(X) public key communicated to him by User X.
6. X and Y exchange the unique key ClesAES.
7. X and Y exchange the values of the digits encrypted by the clespubRSA(Y) and clespubRSA(X) keys after encrypting them again with the unique key ClesAES.
8. each of user's X and Y decrypts the value sent to them by the other user with the unique key clesAES.
9. Each of the user's X and Y decrypts again the values thus received with the key clespriRSA.
10. This is how the shared secret value Ks can be known by both user's X and Y.

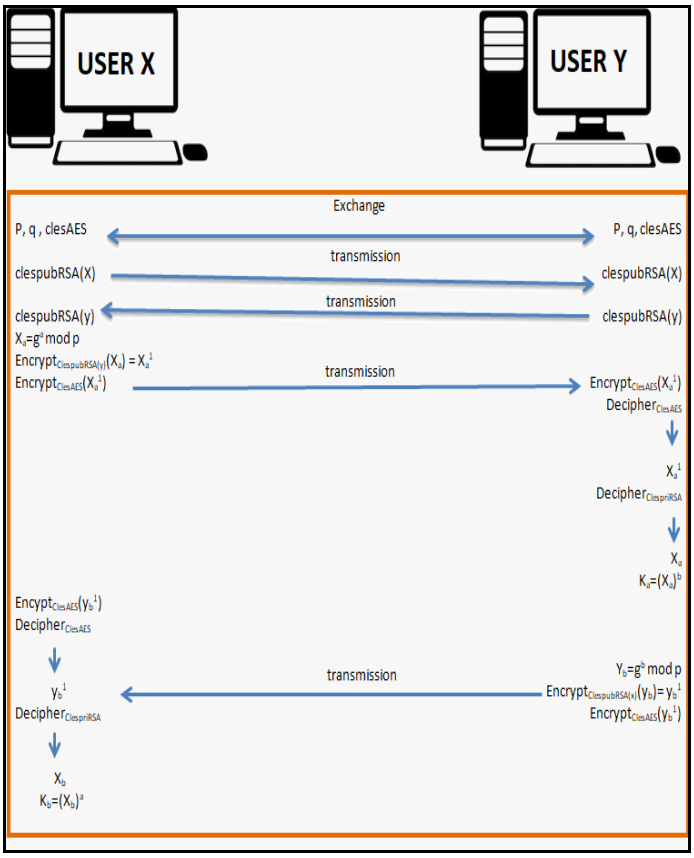

Figure 5. DRA model

VIII. COMPARISON OF THE DRA MODEL WITH PREVIOUS SOLUTIONS

Several studies have been conducted to find solutions to the problems posed at the level of the DH algorithm. These studies have led to solutions on the basis of which several protocols (including STS [14], HMQV [15], A New-Two-Pass Key Agreement Protocol [16]) and models (S-WANE [6], S-SEJAD [10]) have been developed.

TABLE III. COMPARISONS BETWEEN S-WANE AND OTHER SOLUTIONS[6]

MECHANISMS / CRITERIA	S-WANE	STS	HMQV	New-Two-Pass
Man-the-middle	Yes	Yes	Yes	Yes
Encryption of the information exchanged	Yes	No	No	No
Interception of transmitted data	Impossible	possible	possible	possible
Complexity	Less significant	significant	significant	significant
Lead-time	shorter	high	high	high

According to the results observed in the previous table, the comparison shows the security performance of the S-WANE model compared to solutions such as STS, HMQV and New-Two-Pass.

At the level of the S-SEJAD model, a clear performance in computing time is observed compared to the S-WANE model [10], even though the security problem remains the most important one. This is why all efforts must be concentrated on the means to find ever more secure models.

The S-WANE model performs its encryption and decryption processes using RSA, while the S- SEJAD model does the same via AES, and since our proposal was designed on the basis of the combination of RSA and AES, this makes our DRA model more secure than all existing solutions.

IX. CONCLUSION

In this paper we have proposed a hybrid DRA model that combines the two algorithms RSA and AES to encrypt and decrypt the keys exchanged by the DH algorithm. The keys exchanged are encrypted first by the RSA algorithm and then by the AES algorithm, and decrypted by the AES algorithm and then by the RSA algorithm.

The comparative study that we have carried out between our DRA model and the other solutions, allows us to be confident in the reliability of our solution.

The challenges posed by the growing evolution of computer speed and computing power, as well as the emergence of quantum computers, call for us to intensify our research by combining several algorithms to achieve better security.

X. REFERENCES

[1] P. Mpofu, C. Chibaya and T. Rupere, "A hybrid RSA-DH cipher for Signed Encrypted Messages," 2019.

[2] Mohammed Abdulridha Hussain; DNS Protection Against Spoofing and Poisoning Attacks, 2016.

[3] S. Deering, R. Hinden, Rfc 2460 Internet Protocol Version 6 (IPv6) Specification, December 1999.

[4] Williams S.C. (2011) Analysis of the SSH Key Exchange Protocol.

[5] Smita Paira, A comparative survey of symmetric and asymmetric key cryptography, 2014.

[6] K. W. Kelta A. Corenthin, C. Lishou, S. M. Farssi,S-wane model designed to improve Security Association negotiation process in IPv6, 2013.

[7] A. A. Hasib and A. A. M. M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," *2008.*

[8] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption,".

[9] Monika Agrawal, Pradeep Mishra, A Comparative Survey on Symmetric Key Encryption,2012

[10] A. El Emine Sejad, K. Wane Keita, K. Tall and I. Diop, "Proposal of a DH optimization model," *2020.*

[11] J. Chu and M. Benaissa, "Low area memory-free FPGA implementation of the AES algorithm,".

[12] A. K. Mandal, C. Parakash and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," *2012*.

[13] P.Karthigaikumar, Soumiya Rasheed, “Simulation of Image Encryption using AES Algorithm”, 2011.

[14] Blake-Wilson S., Menezes A. (1999) Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol.

[15] Krawczyk H. (2005) HMQV: A High-Performance Secure Diffie-Hellman Protocol.

[16] K. Al Sultan, M. Saeb and U. A. El-Raouf Badawi, "A new two-pass key agreement protocol," *2003*.