Improving the Diffie-Hellman-RSA-AES model

ABDELLAHI AHMED

FST / University of Nouakchott Al Alasriya (UNA)

Abstract

With the emergence of quantum computers with very powerful capabilities, the security of the exchange of shared keys between two interlocutors poses a big problem in terms of the rapid development of technologies such as computing power and computing speed. Therefore, the Diffie-Hellmann (DH) algorithm is more vulnerable than ever. No mechanism guarantees the security of the key exchange, so if an intermediary manages to intercept it, it is easy to intercept.

In this regard, several studies have been conducted to improve the security of key exchange between two interlocutors, which has led to interesting results. The modification made on our model Diffie-Hellman-RSA-AES (DRA), which encrypts the information exchanged between two users using the three-encryption algorithms DH, RSA and AES, by using stenographic photos to hide the contents of the p, g and ClesAES values that are sent in an unencrypted state at the level of DRA model to calculate each user's public key.

This work includes a comparative study between the DRA model and all existing solutions, as well as the modification made on this model, with an emphasis on the aspect of reliability in terms of security. This study presents a simulation to demonstrate the effectiveness of the modification made on the DRA model. The obtained results show that our model has a security advantage over the existing solution, so we made these changes to reinforce the security of the DRA model.

Keywords - DH, DRH, RSA, AES

1. INTRODUCTION

The fundamental security need is to hide information from public or malicious attackers. This requirement has given rise to different types of cryptographic primitives, including symmetric and asymmetric cryptography, hash functions, digital signatures, message authentication codes, etc. [1].

Security and confidentiality are ensured using cryptographic protocols [2]. Security protocols are communication rules between users that use cryptographic primitives such as encryption to provide a guarantee of data security and confidentiality.

The issue of the security of exchanged information between two interlocutors is a real concern and a major focus for scientific research. In a globalized world, marked by the new demands of interlocutors, addressing security needs is a significant challenge. The use of the DH algorithm as a means of communication between two interlocutors on a not necessarily secure channel raises serious security problems, such as [3] [4]:

- The absence of an authentication procedure.
- The use of this algorithm at the level of symmetric key exchange only.
- It is vulnerability to man-in-the-middle attacks since there is no authentication involved.
- Encryption of the information exchanged cannot be performed using this algorithm, and digital.
- Signatures cannot be signed.

The main purpose of this work is to contribute to the strengthening of the security of key exchange of the DH algorithm in the face of the increasingly growing security requirements. In particular, with the risk that the data sent between the two interlocutors can be intercepted by a "middle man".

Through our research on the most important problems of the DH algorithm, we discovered that there are some flaws, especially at the level of key exchange. The results of this work have led to a solution that can offer greater guarantees of security regarding key exchange.

During the research, we proposed a modification to the DRA model [5] that was suggested to replace the DH algorithm and to reduce the risk of interception of data sent between two users by a communicating third party. Therefore, this change maintains secret communication between the transmitter and the receiver throughout the process of calculating the shared secret key.

The proposed modification to the DRA model shows strong resistance against attackers and an ability to securely calculate the shared secret key. In this work, we demonstrate how to secure the key exchange of the DH algorithm by using RSA encryption algorithms, AES, and stenographic images to hide the content of the values exchanged in clear text at the DRA model level.

2. PRESENTATION OF THE DRA MODEL

The hybrid DRA model is the result of one of several studies conducted in this context to find adequate solutions to the various safety problems encountered at the DH level. The DRA model secures the DH key exchange using RSA and AES encryption algorithms.

The DRA model [6] combines the three the different stages of the operation of encryption and decryption of the information exchanged between two users at the level of the DRA model are presented in the following tfigure1: encryption algorithms to encrypt and decrypt the exchanged keys of the DH protocol. The exchanged DH keys are encrypted first by the RSA algorithm and second by the AES algorithm, and they are decrypted first by the AES algorithm and then by the RSA algorithm.

The DRA model is the only hybrid model that uses three encryption algorithms (DH, RSA, and AES). It is used to encrypt and decrypt the keys of the information exchanged between two interlocutors, which further reinforces its reliability in terms of security compared to existing solutions.

The different stages of the operation of encryption and decryption of the information exchanged between two users at the level of the DRA model are presented in the following table 1:

Table 1: The stages of DH algorithm

1	Two users X and Y share two numbers p and g, p being a primenumber and g an integer strictly less than p.
2	user X chooses a secret number a and user Y selects a secret number b.
3	X calculates its public number **Xa** = $\mathbf{g^a}$ mod **p** and Y calculates its public number **Yb** = $\mathbf{g^b}$ mod **p.**
4	X and Y exchange their public keys RSApub(X) and RSApub(Y)and share the numbers p and g, while each keeping their private key RSApri.
5	User X encrypts Xa with the public key **RSApub(Y)** given by user Y. User Y encrypts Yb with the public key **RSApub(X)** given byuser X.
6	X and Y exchange the unique key **CléAES**.
7	X and Y exchange the values of the digits encrypted by the keys RSApub(Y) and RSApub(X) after having encrypted them againwith the unique key CléAE.
8	each of the users X and Y decrypts the value sent by the other userwith the unique key **CléAES**.
9	Each of the users X and Y decrypts the values received againwith the key RSApri.
10	This is how the shared secret value Ks can be known by bothusers X and Y.

Figure 1 below represents the encryption and decryption key exchange process between two X and Y users and shows how both users can calculate the Ks value.

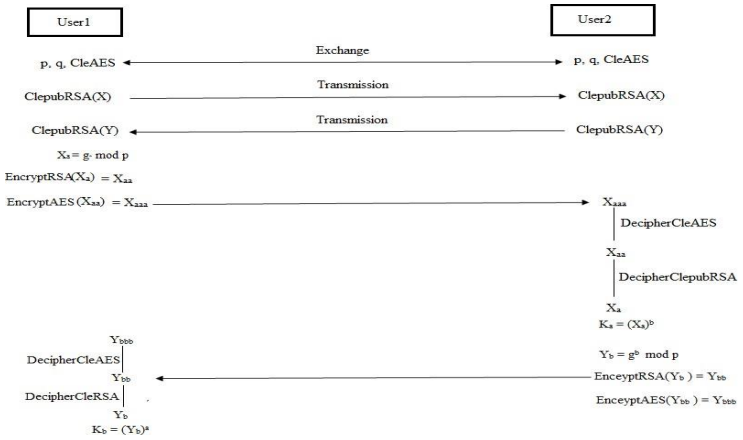

Figure 1: DRA model

This figure represents the DRA model, which offers a very powerful reduction of security vulnerability using the three DH, RSA and AES algorithms.

3. COMPARATIVE STUDY BETWEEN DRA AND EXISTING SOLUTIONS

The comparison between the DRA model and the five existing solutions is based on the following criteria:

- The attack of communicating third parties. This is an important parameter, which consists in assessing the position of the solution in relation to this type of attack, which is a major issue.
- The encryption of the data exchanged. This parameter avoids the possibility of interpreting the data in case it happens to be intercepted.
- The complexity of the mechanisms used. This parameter consists of the ease of implementation related to the number and complexity of the mechanisms used.
- Robustness. This parameter guarantees greater reliability in terms of security.

This comparison will be carried out between the DRA model and each of the five solutions (STS [7], HMQV [8], NEW TWO-PASS AGREEMENT PROTOCOL [9], S-WANE [10] et S-SEJAD [11]).

3.1 DRA vs STS

The DRA model and STS protocol were created to reduce vulnerability at the DH protocol level. Each of them has its own characteristics.

According to the DRA model, the data is encrypted by one of the users before being sent to the other party, which makes it almost impossible to interpret if it can be intercepted by a third party. whereas the STS[12] protocol imposes mutual authentication before the data is exchanged, which makes it possible to identify the communicating third parties before this exchange and thus limit the risks of their interception.

The DRA model encrypts the exchanged data using three encryption algorithms. While the STS protocol does not encrypt the exchanged data, this makes its interpretation possible.

Because complexity is measured by the number of mechanisms used. The two solutions, DRA and STS, each using three-encryption mechanisms, can be said to be equal in terms of complexity.
The DRA model supports two security problems considered major in terms of security (the attacks of the middle man and the interpretation of the data), which demonstrates the robustness of this model (DRA) compared to the STS protocol.
Table 2 below presents details of the comparison between the two DRA and STS solutions:

Table 2: DRA vs STS

Protocol Criteria	DRA	STS
Middle man	Yes	Yes
Data encryption	Yes	No
Risk of data interpretation	Impossible	Possible
Complexity	Lower	Lower
Robustness	Very high	Very high

3.2 DRA vs HMQV

According to the HMQV protocol [13], which uses digital signatures, each user can receive these signatures to identify his interlocutor, but interpretation of the information exchanged remains possible. This is not the case for the DRA model, which uses encryption algorithms.
The HMQV [14] protocol does not encrypt the data exchanged, which makes it possible to interpret them as in the STS solution, while the DRA model encrypts the data exchanged during the transfer, which makes it impossible to interpret them if they are intercepted. The HMQV protocol, which uses four mechanisms, is more complex than the DRA model, which uses only three.
Table 3 below shows the difference between the DRA model and the HMQV protocol inmore detail.

Table 3: DRA vs MMQV

Protocol Criteria	DRA	STS
Middle man	Yes	Yes
Data encryption	Yes	No
Risk of data interpretation	Impossible	Possible
Complexity	Lower	Lower
Robustness	Very high	Lower

3.3 DRA vs New-Two-Pass Prtocol

The New-two Pass Agreement protocol [15] does not encrypt the information exchanged before it is sent, but provides an agreement and secret information allowing each user to identify their interlocutor. This is not the case for the DRA model (see Table 4 below).

Table 4: DRA vs New-Two-Pass Prtocol

Protoc olCriteria	DRA	New-Two-Pass Prtocol
Middle man	Yes	Yes
Data encryption	Yes	No
Risk of data interpretation	Impossible	Possible
Complexity	Lower	Lower
Robustness	Very high	Lower

3.4 DRA vs SWANE

The DRA model, which uses three encryption algorithms, offers greater security in the face of the considerable development of technology compared to the SWANE model [16], which uses only two encryption algorithms. Both models use both DH and RSA encryption algorithms, but the DRA uses, in addition to these two algorithms, the AES algorithm, which demonstrates its robustness in terms of security compared to the SWANE solution [17].

The difference between the two solutions is presented in Table 5 below in more detail:

Table 5: DRA vs SWANE

Protoco lCriteria	DRA	SWANE
Middle man	Yes	Yes
Data encryption	Yes	yes
Risk of data interpretation	Impossible	Low
Complexity	Lower	Lower

Robustness	Very high	High

3.5 DRA vs S-SEJAD

The S-SEJAD [18] model is a hybrid model using two encryption algorithms (DH and AES) to encrypt DH keys before they are transferred and decrypt them at their destination. The DRA solution uses, in addition to the two-encryption algorithms used by S-SEJAD, the RSA encryption algorithm. This illustrates its robustness in terms of security compared to the S-SEJAD model.

At the level of the S-SEJAD model, security is limited to two encryption algorithms (DH and AES). It is sufficient for a communicating third party to decrypt AES in order to be able to interpret the key of the data exchanged using a high-quality modern computer to access the secret. On the other hand, the communicating third party can only obtain the information exchanged via the DRA solution after decrypting the RSA and AES encryption algorithms, which is practically impossible.After a comparative study of this model with all existing solutions, we observed the security performance of the S-WANE solution compared to the following solutions: STS, HMQV, and New-Toc-Pass. We also noticed in the S-SEJAD model a clear performance in the calculation time compared to that of the S-WANE and greater security compared to the three above protocols (STS, HMQV, and New-Two-Pass). Since the problem of security is of the utmost importance in terms of communications and the exchange of information, all efforts must be concentrated on finding ever more secure models. The S-WANE model performs its encryption and decryption processes using DH and RSA, while the S-SEJAD model performs these processes via DH and AES. Given that the proposed DRA model was designed based on the combination of DH, RSA, and AES while circumventing the weaknesses of the SWANE and S-SEJAD models, we confirmed that it is the most secure compared to all existing solutions.

Table 6: Here is the difference between the DRA model and the S-SEJAD model:

Table 6: DRA vs S-SEJAD

Protocol Criteria	**DRA**	**S-SEJAD**
Middle man	Yes	Yes
Data encryption	Yes	Yes
Risk of data interpretation	Impossible	Low
Complexity	Lower	Lower
Robustness	Very high	High

After a comparative study of this model with all existing solutions, we observed the security performance of the S-WANE solution compared to the following solutions: STS, HMQV, andNew-Toc-Pass. We also noticed in the S-SEJAD model a clear performance in the calculation time compared to that of the S-WANE and greater security compared to the three above protocols (STS, HMQV, and New-Two-Pass). Since the problem of security is of the utmost importance in terms of communications and the exchange of information, all efforts

must be concentrated on finding ever more secure models. The S-WANE model performs its encryptionand decryption processes using DH and RSA, while the S-SEJAD model performs these processes via DH and AES. Given that the proposed DRA model was designed based onthe combination of DH, RSA, and AES while circumventing the weaknesses of the SWANE and S-SEJAD models, we confirmed that it is the most secure compared to all existing solutions.

4. THE MODIFICATION MADE ON DRA MODEL

The DHA model uses the DH protocol, the RSA algorithm, and the AES algorithm to encrypt and decrypt the information exchanged and authenticate the middle men by combining the two algorithms to ensure better security of the DH keys. One of the limitations of this model is that the values exchanged p, g, and ClesAES are not encrypted and used to calculate the Xa and Xb values. Their interception and possibly their interpretation by a third party are always to be feared. The modification made to this model to improve the security of information exchange between two communicators is to encrypt the exchanged values (p, g, and ClesAES) in such a way that third parties cannot use them to calculate users' public keys.

The various steps of the proposed model to improve the security of information exchange at the level of the DRA model are as follows:

1. Both users X and Y agree on two numbers p, g and ClesAES that are sent in a photo to conceal their contents, such as, p being a prime number and g<p.
2. User X selects a secret number a, Y selects a prime number b.
3. X calculates its public key $X_a = g^a \bmod p$ and Y calculates its public key $Y_b = g^b \bmod p$.
4. X and Y exchange their public keys clePubRSA(X) and clePubRSA(Y), by keeping each its RSApri private key.
5. X encrypts its X_a public key with the public key PubRSA(Y) and Y encrypts its Y_b public key using the public key PubRSA(X).
6. The two users X and Y exchange the values of the digits encrypted by the cleRSApub(Y) and cleRSApub(X) keys after they have been encrypted again with the unique CleAES key.
7. Each user decrypts the value sent by the other with the CleAES key.
8. Each user decrypts the values received with the RSApri key again.
9. X calculâtes $k_a = (Y_b)^a$ et Y calculâtes $k_b = (X_a)^b$
10. According to the laws of algebra, $k_a = k_b = k_s$. X and Y both know the secret value “k_s”.

Figure 2 below demonstrates the encryption and decryption key exchange process between two users X and Y.

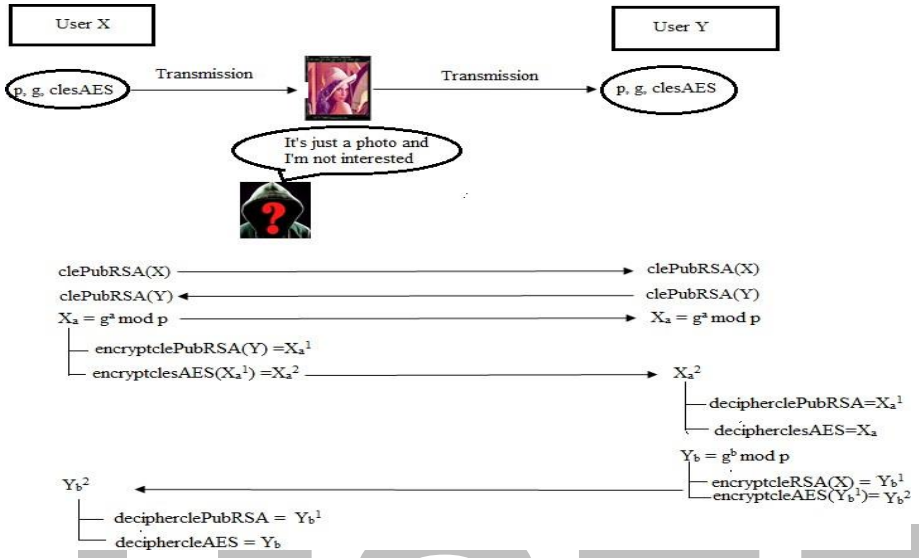

Figure 2: modification made on DRA model

5. EXPERIMENTAL PARAMETERS

The objective of the simulation program [17] is to test the DRA model in terms of time. This test was conducted according to the following criteria:

- The attack of a communicating third party.
- Encryption of information exchanged.
- Interception and interpretation of information exchanged.
- Robustness.
- Execution time.

It must be noted that we were able to give a formal opinion on the first four criteria. However, the fifth criterion, namely time of execution, could only be supported by tests. In fact, these tests will help quantify these time limits. They will produce results leading to a better appreciation of this criterion.

This is how we turned to the simulation of these mechanisms by writing a program in MATLAB. It should also be noted that times of execution (lead times) are defined in ms.

For the first graph, we vary the size of the key from 0 to 320 and we observe the evolution of the time (ms) according to these values. This evolution is shown in Figure 3 below.

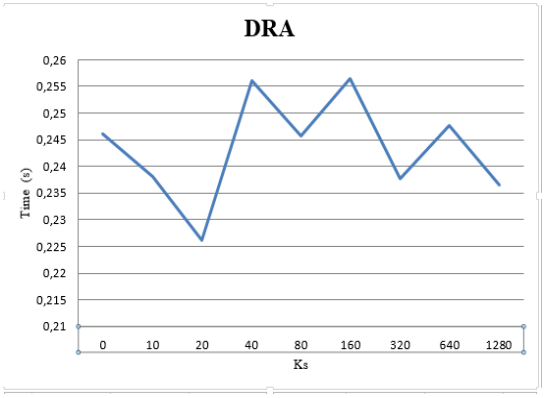

Figure 3: Time based on to the Ks values of "DRA"

There is a noticeable decrease in execution times as the size of the keys increases to a few spikes. For the construction of Figure 4 below, the size of the key was varied from 0 to 1280, and the evolution of the execution times (ms) was measured according to this variation.

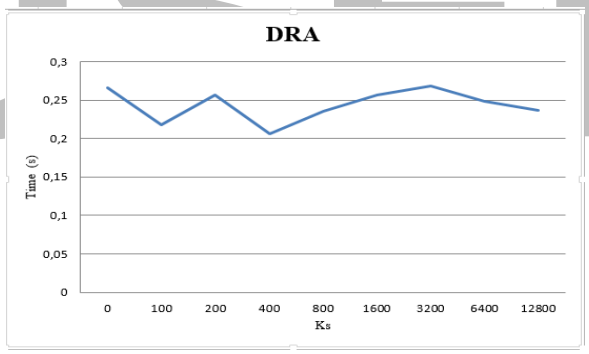

Figure 4: execution time based on Ks values of "DRA"

In Figure 4 above, there is a significant decrease in execution time when increasing the size of the keys.

Reading these graphs allows one to notice a reduction in the DRA deployment time according to the order of magnitude of the keys. A few peaks are noted in Figures 4 and 5. The curve changes from stationary to decreasing. The advantage is that we control the lead-time, which shows a strong downward trend when the size of the keys increases.

The simulation was performed on a computer with the following characteristics:

- CPU: Intel(R) Core (TM) i3-2350M CPU @ 2.30GHz (4 CPUs), ~2.3GHZ.
- RAM: 4GB.
- OS: Windows 8.1 Professional.

6. CONCLUSION

The aim of this work was to contribute to optimizing the security of the DRA model. To attain this goal, we carried out a critical study of the security of this model.

Through this study, we can see that the limits of the security of the DRA model are centered on the values p, g and ClesAES that are shared between the two users X and Y with no encryption.

The results obtained from this study showed its strengths in relation to the initial concerns associated with a certain limit linked to the deployment time. To validly assess this model, simulations were implemented. To achieve this, a simulation program was produced and the following reports were obtained:

- The reliability of the DRA model and the effectiveness of the modification carried out on this model.
- Reduction of DRA time depending on used key sizes.

This study also shows that the DRA model, resulting from the combination of DH, RSA, and AES encryption algorithms, is more robust than all existing solutions because it has considerably reduced the risk of attacks by the men in the middle and made it impossible to interpret the data in case it is intercepted. This is why the DRA model appears as an alternative solution to the DH protocol. Indeed, with the enhanced security of our DRA model, we offer greater reliability for these systems.

REFERENCES

[1] H. A. A and H. M, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," 2008.

[2] Ş. Ciobâcă, "Verification and composition of security protocols with applications to electronic voting," École normale supérieure de Cachan - ENS Cachan.

[3] B. P, D. M and O. H, "Improving the Diffie-Hellman secure key exchange," International Conference on Wireless Networks, 2005.

[4] K. S. McCurley, "The discrete logarithm problem," vol. 42 of Proceedings of Symposia in Applied Mathematics, p. 49–74, 1990.

[5] Abdellahi Ahmed, M. F. Nanne and B. Gueye, "A hybrid model to secure the exchange of DH keys," 2021 International Conference on Computer Communication and Informatics (ICCCI -2021), 2021.

[6] A. Ahmed, M. F. Nanne and B. Gueye, "The effectiveness of a hybrid Diffie-Hellman-RSA-AES model," 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022.

[7] Blake-Wilson S and Menezes A, "Unknown Key- Share Attacks on the Station-to-Station (STS) Protocol," Public Key Cryptography, vol. 1560. , 1999.

[8] K. H, "HMQV: A High-Performance Secure Diffie-Hellman Protocol," Advances in Cryptology – CRYPTO 2005, vol. 3621, 2005.

[9] K. Al Sultan, M. Saeb and U. A. El-Raouf Badawi, "A new two-pass key agreement protocol," 46th Midwest Symposium on Circuits and Systems, 2003 .

[10] Khadidiatou Wane Kei"ta and Claude Lishou, "The Impact of Model S-Wane on IPv6," 2014.

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

[12] S. BLAKE-WILSON and A. MENEZES, "Authenticated Diffie-Hellman key agreement protocols," Fifth Annual Workshop on Selected Areas in Cryptography (SAC '98) (1999), p. 339–361, 1999.

[13] Menezes A and Ustaoglu B, "On the Importance of Public-Key Validation in the MQV and HMQV Key Agreement Protocols," Progress in Cryptology - INDOCRYPT 2006, vol. 4329, 2006.

[14] K. H, "HMQV: A High-Performance Secure Diffie-Hellman Protocol," dvances in Cryptology – CRYPTO, vol. 3621, 2005.

[15] S. Blake-Wilson, D. Johnson and A. Menezes, "Key exchange protocols and their security analysis," 6th IMA International Conf, 1997.

[16] K. W. Keita, B. Bodian, I. Diop, C. Lishou and S. M. Farssi, "The S-WANE model, a real alternative of DH system," 5th International Conference on Multimedia Computing and Systems (ICMCS), 2016.

[17] K. W. Keita, "CONTRIBUTION A L'AMELIORATION DE LA SECURITE DANS L'ENVIRONNEMENT IPv6 : Modélisation et simulation d'un système d'échange des, clés S-WANE,," THESE DE DOCTORAT, 2015.

[18] A. El Emine Sejad, K. W. Keita, K. Tall and I. Diop, "S- SEJAD versus DH," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021,pp.

Authors' background

Your Name	Title*	Research Field	Personal website
Abdellahi Ahmed	Assistant professor	cryptography	