Enhanced Multistage RSA Encryption Model

Mays M. Hoobi\textsuperscript{1}, Sumaya S. Sulaiman\textsuperscript{2}, Inas Ali AbdulMunem\textsuperscript{3}

Department of Computer Science, College of Science, Baghdad University, Baghdad, Iraq

\textsuperscript{1}Mays.m@sc.uobaghdad.edu.iq, \textsuperscript{2}sumasaad@uobaghdad.edu.iq, \textsuperscript{3}inas.ali@uobaghdad.edu.iq

Abstract:
Digital data amounts are expanding quickly every day over the Internet. Security plays an essential role in the advancement of communication systems, particularly with confidential material transmitted over a network because of the continuous availability of digital data and effective attackers try to access these data. Cryptography becomes one of the most major fields used, and necessary fields for achieving a high level of protection between distinct individuals. Efficient and new editions of cryptography algorithms can help decrease security risks, any type of data has its own confidentiality, so new algorithms should be used to protect confidential data toward unauthorized access. After reviewing the RSA and attacking it, it would appear that a new model should be improved to mitigate this attack and improve the security of the RSA algorithm. In this research, increasing the complexity and search space of RSA algorithm against brute force attack in addition to security enhancement was satisfied by applying four cases with using different cryptography algorithms. This four cases included:

- Case 1: Enhanced the security of RSA by using Optimal Asymmetric Encryption Padding (OAEP),
- Case 2: Combining of the two most important algorithms RSA and Diffie-Hellman (D-H),
- Case 3: For increasing complexity and obtaining high level of security, the two above cases (case 1 & case 2) were concatenated, finally for most complexity and obtained highest security level with increasing search space of RSA case 4 was applied.
- Case 4: Contained implementation of case 3 in addition to apply new level of security by adding another cryptography algorithm called HiSea algorithm.

The results of using multiple cryptography algorithms in each case of the above four cases respectively improved security level by increased the complexity and key search space that lead to protect the security goals against the attackers. Case 4 is the best case because it provides most efficient complex and accurate encryption system that used the processing of encryption data multiple times using different strong algorithms.

Keyword: Brute force attack, Cryptography, D-H, HiSea, OAEP, RSA, Security.

1. Introduction:
Securing of data is a complicated task in data communication today that influences many areas; therefore, security is still one of the major methods of protecting information by transferring undefined and encrypted information not permitting unauthorized persons to obtain it. A full data protection solution needs to have confidentiality, integrity, and authenticity. Cryptography is the process of designing procedures that enable information to be transmitted securely such that the intended recipient is the only person capable of obtaining this information [1]. The basic cryptographic principle is described as: A text to be sent is identified as plaintext, then encrypted using an encryption algorithms, this process is known encryption. The encrypted text produced is known as ciphertext, and the decryption process turns them back into plaintext. Graphical presentation in figure (1) shows conventional encryption as well as decryption process [2].
The cryptography's main aim is not really to provide secrecy only, it also to provides solutions to other issues such as: integrity of data, authentication and non-repudiation. Many algorithms are developed and designed to ensure security for most information that travels across the universe via networking. In algorithms the main emphasis is depend on the key. There are two main types of key, symmetrical: use one key to encrypt and retrieve message, Whilst we use various keys in asymmetric form, one being “public” and others one is “private” for decryption and encryption. It is necessary to choose the accurate and appropriate algorithm to ensure a secure connect that adds more effective and appropriate system for encryption [3]. The principle of multiple encoding can be represented as a multilayer and multilevel protection technique. Multiple encryptions are the method of encrypting an already encrypted text more than one time, using same or different algorithm [4]. This research uses multiple efficient encryption algorithms, which uses the same structure of encryption and decryption procedure. This research is distributed in six sections, section1 presents introduction to data security algorithms and cryptography, in section2, research on security using various cryptographic algorithms is described, section3 explains the using of efficient cryptography methods, section4 describes proposed enhanced model, section5 and 6 present result analysis and conclusion respectively.

2-Related Work:

This section lists a number of related works, In [5], Diffie and Hellman (D-H) proposed in this work for key exchange, some drawbacks to this algorithm against. The suggested methodology has identical purposes with the D-H algorithm, and a new method is being used to exchange session keys that resolve the D-H algorithm’s time-complexity limit. The proposed "Multiplicative Key Exchange Algorithm" produces and uses simple arithmetic equations to exchange and generate keys over unsafe connection. In [6], A polyVernam cryptosystem proposed and adapted to operate with the keys, that were very difficult and complex to implement to use. When coupled with modern monoalphabetic cipher algorithms, it is possible to manipulate data using key generation algorithm and also can be constantly used as a simplistic password. In [7], The One Time Pad (OTP) technique was suggested as a combination of certain cryptographic primitives to implement diffusion and a simple form of randomized steganography to conceal where the encryption starts. The result of the enhanced OTP technique was appropriate to allow the same key unlimitedly used to encrypt different plaintext without disclosing any pattern. In [8] A modern Vernam cipher-based algorithm updated by adding 2’s complement to improve the algorithm’s complexity. The key used was optimized using a genetic method to develop the power and complexity from key dedication and displayed a low score for the avalanche effect.
3-Algorithms:
Multiple encryptions with the same or different algorithm can be illustrated as a repetitive single encryption process. To recognize the basic idea for every encryption algorithm used in this research, the process of (RSA, OAEP, D-H, HiSea) algorithms was considered as illustrated in following subsections:

3.1 RSA Algorithm:
RSA, the Advanced Encryption Standard, is a standard for symmetric key encryption that is commonly used to protect data where confidentiality is a crucial and significant problem. The security of algorithm is depending on the hardness of factoring a large number of composites and a composite number for a specified odd integer e computing eth roots modulo. Public key of RSA consists of integer pair (n, e). The modulus n is a large number of composites while the public exponent ‘e’ is normally a small prime. The modularity is the result of multiplying 2 primes. Using the main advantage of RSA, variable size key and encryption block to improve security [9][10]. To illustrate RSA encryption and decryption show figures (2), (3), and (4) in addition to table (1).

![RSA Algorithm Diagram](image)
3.2 Optimal Asymmetric Encryption Padding (OAEP) Algorithm:
OAEP is a message encoding process. The process is done by encoding a message once with OAEP, then encoding it again with RSA this means that if hash functions are very random, an opponent who retrieves this message must be able to break the RSA algorithm. The encoded OAEP message is a concatenation of a string of "masked data" with a "masked random number". Masked data is formed in the simplest form of OAEP by taking the result of XOR of plaintext message M and hash G of a random string r. While the masked random number is the XOR of r with the hash H of the masked data. An OAEP has several variants which has a component called "plaintext-awareness". This means an opponent has to know the original plaintext to construct a valid encoded OAEP message. To achieve this, first, the plaintext message M is padded (e.g. with zeroes string) then the masked data is calculated[10][11]. For clear idea of OAEP see figures (5), (6), and table (2).

Figure (5): OAEP Encoding Operation
3.3 Diffie-Hellman (D-H) Algorithm:

Whitfield Diffie and Martin Hellman identified what the Diffie-Hellman (D-H) algorithm is now known as. D-H key exchange is a systematic approach for the exchange of cryptographic keys, this algorithm generates the sender's and receiver’s secret key. The D-H key exchanging method enables two parties without previous knowledge of each other to create a mutual secret key.
together with an insecure channel of communication. Then, the key is used to encrypt the communications messages using a symmetric key cipher [12]. For more illustration about D-H show algorithm (1), figure (7), and table (3).

Algorithm (1): D-H Algorithm

| Step No. | Step Calculation |
|----------|------------------|
| 1        | Two numbers ‘R’ (is a prime) and ‘G’ (is called as base) are selected. |
| 2        | A secret numbers ‘A’ and ‘B’ are selected. |
| 3        | A public numbers ‘X’ and ‘Y’ are calculated where X = G^A mod R And Y = G^B mod R |
| 4        | Public numbers are exchanged |
| 5        | First session key is computed as K1, K1 = Y^A mod R |
| 6        | Second session key is computed as K2, K2 = X^B mod R |
| 7        | Here K1 = K2 = K |

![D-H Algorithm Diagram](image)

Figure (7): D-H Algorithm

| Symbol   | Mean                                      |
|----------|-------------------------------------------|
| A, B     | Random Number                             |
| R        | Prime number                              |
| G        | Integer number and primitive root of R    |
| K1, K2   | Keys generated by D-H algorithm          |

Table (3): Symbol meaning of D-H

3.4 Hisca Algorithm:

Hisca is an encoding for antisymmetric block, using an integer for the encryption and decryption of plain text. For the encryption process, message is a 64-byte ASCII, where Hybrid Cube (HC) depends on multiplication the layer matrix of magic cubes (MC) [13].
In a similar way, we finish the remainder of a layers before a new HC cube is built based on MC layers, the sophistication may be expanded by combining many HC layers of input to build complex coding and decoding algorithms. Figure (8) show the HiSea's overall design, where keys, plain text, and encrypted text are structured in matrix 4 order in encryption method. HiSea encryption text, that is defined by protection and wide space and also has complex keys to guess or measure or time-consuming for attacker, this is added to enhance the encryption difficulty [14]. Algorithm(2) illustrates the steps of HiSea Algorithm.

Algorithm(2): HiSea steps

| Step No. | Step Calculation |
|----------|------------------|
| 1        | ASCII symbols is used to format the plain text as 64 characters and four arrays of plain text are created as P1-P4. The output (P1) is used as the intermediary for the P2 encryption process and the P2 result as the intermediary for the P3 encryption process. Until we get to P4. |
| 2        | P1’ is the encrypted text formed by mixing P1 with the primary matrix (IM) and so on until P4 is reached. Then P1’ is added with Session Key 1 (K1). Use the Mix Row and Mix Col function to create a post in Cipher text 1 (C1). |
| 3        | C2 is formed by adding plain text which is P2 where it is mixed with P1’ to produce P2’ and then compiled with K2 which is session key 2 and produced by Mix Row and Mix Col Previous operations are repeated depending on P3 and P4 to create 3 (C3) and 4 (C4). |
| 4        | Repeat previous operations depending on P3 and P4 to create 3 (C3) and 4 (C4) |

Figure(8): Diagram of HiSea Algorithm

The HC matrix of the 4x4 command is defined as Hi, j, i {1, 2, 879} and j {1, 2, 3, 4} as follows:

Hij = MCi,j MCi, j, where the MCi, j is a jth layer of ith magic cubes. Assume we have coordinates x = {1, 2, 3, 4} where we multiply with the matrix of the MC 1 layer to produce HC 1 and then we generate HC 2 by multiplying the coordinates of the MC 2 layer with X = {1, 2, 3, 4}

In a similar way, we finish the remainder of a layers before a new HC cube is built based on MC layers, the sophistication may be expanded by combining many HC layers of input to build complex coding and decoding algorithms. Figure (8) show the HiSea's overall design, where keys, plain text, and encrypted text are structured in matrix 4 order in encryption method. HiSea encryption text, that is defined by protection and wide space and also has complex keys to guess or measure or time-consuming for attacker, this is added to enhance the encryption difficulty [14]. Algorithm(2) illustrates the steps of HiSea Algorithm.
4- Proposed Enhanced Multistage RSA Encryption Model (ORSA, DRSA, HRSA)

The traditional methods of encrypted data can only keep data security against malicious purposes by unauthorized person, therefore, effective methods of encryption / decryption are needed to improve data security. The main features for distinguishing and classifying the encryption algorithm from another are its skill in securing critical data against malware activity and their effectiveness. The aim of this proposed multistage model is to enhance the strength of already existing cryptography algorithms. In these encryption algorithms, the encryption is applied to original data many times at each phase with different robust encryption algorithms. This encryption algorithms will increase the complexity of encryption algorithm at large scope. The enhanced multistage model named as (ORSA, DRSA, HRSA), where ORSA is short for (OAEP-RSA), DRSA is short for (DH-RSA), and HRSA is short for (HiSea-RSA) consequently. In this research, performance and complexity of mentioned cryptography algorithms were presenting with different four cases. Using of multistage encryption will rise the popularity of applied cryptography for the improvement of data security. As the applying of multistage encryption can be complex but it enormously enhances the data security. Some changes was made into the structure of enhanced multistage RSA algorithm so that it resist against the cryptanalyst attacks and it will be work fine against the brute force attack.

4.1- Case1: (ORSA) Model

This model according to study [11]. OAEP benefits from combining good safety assurances with good results, this process works as shown in section 3.2 previously. OAEP in particular combined with RSA, which offers greater security against what is considered adaptive cipher-text attacks. ORSA is indeed a public-key encryption system that combines RSA with OAEP system. ORSA ‘s protection is depending on the reliability of the basic RSA encryption or decryption as contrasted with RSA, ORSA seems to be more reliable than RSA's cryptography algorithm since ORSA involves OAEP definition, which is challenging for the intruder to locate the plain-text from the secret text. For more illustration about ORSA model see figures (9), (10), tables (4), (5).
Figure (9): Case1 (ORSA-Encryption((n,e),M,P))

Figure (10): Case1 (ORSA-Decrypt(K,c,P))

Table (4): Symbol meaning of ORSA-Encryption (Case1)

| Symbol | Mean |
|--------|------|
| n, e   | RSA Recipient’s public key |
| M      | The encrypted message |
| m      | Integer message |
| EM     | Encoded Message |
| C      | Ciphertext |
| c      | Integer ciphertext |
| P      | Encoding parameters |
| k-1    | Length of EM |
| OS2IP  | Octet String to Integer Primitive |
| I2OSP  | Integer to Octet String Primitive |
4.2- Case2: (DRSA) Model

In now days exchange algorithm RSA and D-H key is widely used, this model according to study [12]. In this study, the operation of bitwise, XOR additive making the message more compelling. This operation follows that convert message to cipher. This technique, first select two primes then discover which key exponents will be used to decryption and encryption. Selected for the D-H algorithms ‘A’ and ‘B’. ‘R’ is random primes autogenerated by system. The general number will be generated by the D-H algorithm, which was generated using this public number private key ‘K1’ and ‘K2’ is used to execute XOR operation. Encryption is achieved on the sender side, using the encryption algorithms. After the process of encryption terminates XOR between the text of the cipher and the first secret key. The secret data is sent over the medium after this operation. The XOR operation between the private 2nd key k2 and the secret message sent by the sender is again performed on the receiver side. Using this operation, cipher text is obtained, after which the cipher text is decrypted by decryption algorithm. See figure (11), table (6), algorithm (3), it’s clear that figure (11) is the result of concatenation between figure (2) and figure (7) with addition some operations and steps according to study[12].

Table (5): Symbol meaning of ORSA-Decryption(Case1)

| Symbol | Mean |
|--------|------|
| K      | recipient’s RSA private key |
| M      | Recover Message |
| m      | Integer message |
| EM     | Encoded Message |
| C      | ciphertext to be decrypted |
| P      | Encoding parameters |
| OS2IP  | Octet String to Integer Primitive |
| I2OSP  | Integer to Octet String Primitive |
Figure (11): Case2 (DRSA) Model

Table (6): Symbol meaning of (DRSA) Model (Case2)

| Symbol  | Mean                                      |
|---------|-------------------------------------------|
| A, B    | Random Number                             |
| P, Q    | Prime numbers                             |
| G       | Integer primitive root of R number        |
| C1      | Ciphertext                                |
| S1      | Secret message                            |
| K1, K2  | Keys calculated by D-H algorithm         |
| E, D    | Exponents of encryption and decryption    |

Algorithm (3): (DRSA) (Case2)

| Step No. | Step Calculation                                                                 |
|----------|-----------------------------------------------------------------------------------|
| 1        | Select P and Q as two large prime numbers and A, B as a random number and G, R.  |
| 2        | A and B are set for D-H key generation                                             |
| 3        | R and G are automatic generated constants                                          |
| 4        | N= P * Q is calculated                                                             |
| 5        | Find Phi (N) = (P-1)*(Q-1)                                                      |
| 6        | Integer E is chosen, which can satisfy GCD [E, φ(N)] = 1, φ(N), Where 1 < E < φ(N)  |
| 7        | D is calculated, where E^2D = 1 mod φ(N)                                           |
| 8        | Now calculate following as public number, Calculate X= G^A mod R, Y= G^B mod R     |
| 9        | Secret key K1 = Y^A mod R, K2 = X^B mod R                                         |
| 10       | Encrypt message using RSA algorithm, C1= (M^E) mod N                               |
| 11       | XOR between K1 and key K2, S= C1 ⊕ K2                                              |
| 12       | At receiver side XOR is between S and key K2, C1= S ⊕ K2                           |
| 13       | Decrypt message using RSA algorithm M= (C1 ⊕ D) mod N                             |
4.3- Case3: Proposed (ORSA, DRSA) Model
In this case, the proposed multiple encryption model provides greater data security by using a highly effective and secure encryption algorithms. In this model, two high security algorithms with RSA are integrated in a single cryptographic systems and information security is greatly improved. The model has finally been established to be very effective and safe against the security threats. Figure (12), illustrates the proposed model according to case3.

![Diagram of Case3: Concatenation of Cas1 & Case2]

M: Original Message.
C1: Ciphertext output of case1.
C2: Ciphertext output of concatenation case1 & case2 respectively.

4.4- Case4: Proposed Enhanced Multistage RSA Encryption Model (ORSA, DRSA, HRSA)
In the proposed model, many encryptions are performed using various efficient encryption algorithms performed in case3 in addition to new algorithm named HiSea algorithm. The resultant encryption will be stronger by using three different types of encryption algorithms with RSA algorithm, expecting to achieve a better level of security. In this proposed multistage encryption model, the plain text is given as an input. The plaintext encryption is done using ORSA algorithm and the resulted output comes out as cipher C1. Then the encrypted output data is used as an input for the second encryption operation by DRSA encryption algorithm, the resulted output is generated in the form of cipher C2. This C2 is given as the input for third encryption operation by HRSA encryption algorithm, the last resulted output is formed as a final
output of multistage encryption in the form of final cipher C3. As, the plaintext is encrypted three times by different encryption algorithms that is proved as secure encryption algorithms, the resulted output of the multistage encryption model is considered as a highly secured cipher. The process of encryption by the proposed enhanced multistage encryption system (ORSA, DRSA, HRSA) is represented as show in figure (13).

5-Results Analysis:

Improving the robustness of the algorithm by using a set of different cryptography algorithms instead of one algorithm. Experimental results show that using the proposed model together with multi-stage algorithms has resulted in increased performance compared to using the algorithms oneself. In this research the public key enhanced results of RSA increase the complexity of the search space and probability of attackers cracking the RSA algorithm. In cryptanalysis, a brute force attack attack is a form of defeating a cryptographic scheme by trying a large list of alternatives, if there are n possible keys, on typical a brute force attack would be expected to find a key after n-1 trials etc. The proposed enhanced multistage encryption model generates better performance due to following points:

- It supports big data block sizes.
- It offers strict protection against attacks of difference.
- The multi-layer encryption is considered as protected encryption algorithm.
- Large number of possibilities need to be tested to dedicate the right key.
- It is computationally safe against attack by brute force as it takes a lot of time to test all possible keys.

6-Conclusion:

The proposed model can be work as primary model in the field of cryptography. The results of case1 according to [11] included Improve text protection by mixing encryption and XOR bitwise, also increases the complexity of the message, this model provides greater security compared to the normal RSA algorithm. While in case2 according to [12], a minor improvement of the well-known and functional RSA-OAEP has been used, according to this model it has additional advantages, protection remains highly related with the RSA problem's hardness. In this research, a multistage RSA encryption algorithm is proposed for high security using case3 and case4, case3 included concatenation between case1 and case2, while case4 included a combination of RSA, OAEP, D-H, and Hissea algorithms. Also the multistage encryptions advantage is the providing of better security as some component ciphers are broken or some of the secret keys are recognized, the original data confidentiality can be maintained by the multistage encryptions.

References:

[1] Mayes, Strong Triple Data Encryption Standard Algorithm using Nth Degree Truncated Polynomial Ring Unit. Journal of Science. 2017. Vol. 58, No.3C, pp: 1760-1771.
[2] Halah H, Mayes M, Improved Rijndael Algorithm by Encryption S-Box Using NTRU Algorithm, Iraqi Journal of Science, 2015, Vol 56, No.4A, pp: 2982-2993.
[3] Deborah G, Ariel M, Ruji P, Strengthening The Vernam Cipher Algorithm Using Multilevel Encryption Techniques, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 10, OCTOBER 2019 ISSN 2277-8616.
[4] Waleed K, Mohammed M, Norrozila S, An Enhanced Encryption Algorithm for Database Protection Based on Dynamic Key and Reverse String, Journal of Engineering and Applied Sciences 12 (5): 1186-1191, 2017 ISSN: 1816-949X.
[5] Sharad Boni, Jaimik Bhatt, Santosh Bhat, “Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm”, International Journal of Computer Applications (0975 – 8887) Volume 130, No.15, PP 7-11, November-2015.
[6] R. Divya and A. M. M, “The PolyVernam Cipher,” vol. 3, no. Viii, pp. 489–496, 2015.
[7] A. E. Omolara, A. Jantan, O. I. Abiodun, and H. Arshad, “An Enhanced Practical Difficulty of One-Time Pad Algorithm Resolving the Key Management and Distribution Problem,” vol. I, 2018.
[8] A. Rahman Dalimunthe, H. Mawengkang, S. Suwilo, and A. Nazam, “Vernam Cipher with Complement Method and Optimization Key with Genetic Algorithm,” J. Phys. Conf. Ser., vol. 1235, p. 012030, 2019.
[9] Fausto M, Jenny T, Miranda Alba, Danilo N, RSA EncryptionAlgorithm Optimization to Improve Performance and Security Level of NetworkMessages, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, August 2016.
[10] Dripto Chatterjee, Joyshee Nath, Suvadeep Dasgupta, Asoke Nath “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.
[11] Preetha M, Nithya M, A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, June 2013, pg.126 – 139.
[12] Gaurav R, Krunal P, Hybrid Encryption Algorithm, International Journal of Engineering Development and Research, 2014, Volume 2, Issue 2, ISSN: 2321-9939.
[13] Heba H, Mohamed T, Eltawel S, A robust Computational DRM Framework for Protecting Multimedia Contents using AES and ECC, Alexandria Engineering Journal, 2020.
[14] Shaimaa K, Waleed R, Ahmed O, Zainab K, Subject Review: Comparison between 3DES, AES, &HiSea Algorithms, IJSRSET, Volume 6, Issue 6, 2019.