Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography.

Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography.

Chiradeep Gupta[1,3], **N V Subba Reddy**[2]
[1] MTech, Computer Science and Information Security.
[1,2] Department of Computer Science, Manipal Institute of Technology, MAHE, Manipal.
[3] chiradeep.gupta@learner.manipal.edu , [2] nvs.reddy@manipal.edu

Abstract. Cryptography is related and referred to as the secured transmission of messages amongst the sender and the intended receiver by ensuring confidentiality, integrity, and authentication. Diffie – Hellman (DH) key exchange protocol is a well-known algorithm that would generate a shared secret key among the sender and the intended receiver, and the basis of cryptosystems for using public and private key for encryption and decryption process. But it is severely affected by the Man in the Middle (MITM) attack that would intercept and manipulate thus eavesdropping the shared secret key. This paper proposes a model of integrating the public-key RSA cryptography system with the DH key exchange to prevent the MITM attack. The performance of the proposed work has been compared to the DH Key Exchange algorithm as well as RSA Cryptosystem to conclude for effectiveness of the proposed model.

1. Introduction

Cryptography is branch of information security that deals with the concealment of messages to ensure and serve the vital needs of maintaining confidentiality, integrity, and authentication. Security of data can be breached easily and thus, needs to be secured utilizing the most efficient systems available. Cryptographers have developed several such systems in order to achieve the same. In fact, it is an ongoing research on the security level of the cryptosystem for secured message transmission from the authentic sender to the intended receiver [2]. Cryptosystems are widely classified into traditional and modern approaches. But the modern approaches are highly recommended as the traditional cryptosystems such as Caesar Cipher, Vigenère Cipher are susceptible to attacks with ease. Modern cryptosystems are then further bifurcated based on the type of keys being shared among the users in the systems. If it is a shared secret (single) key, then it is symmetric cryptosystem – stream or block ciphers. Otherwise, the other classification is asymmetric cryptosystem. Figure 1 enlists the various types of asymmetric cryptosystem as well [3].

Diffie – Hellman (DH) Key-Exchange Algorithm is based on the idea of asymmetric cryptosystem [1]. For two hypothetic users – Alice and Bob, this algorithm generates a shared secret key among them with the help of public and private keys of Alice as well as Bob [Table 2]. But every algorithm is having a susceptibility towards attack, in the similar fashion it is prone to MITM attack. Such an attack involves intercepting the public keys of Alice and generating a shared secret key known to all the three including the adversary. Table 3 details the attack on the DH Key exchange protocol [6].

The proposed work focuses on inculcating the RSA cryptosystem to secure the DH Key Exchange Algorithm for minimum or no effect of MITM attack.

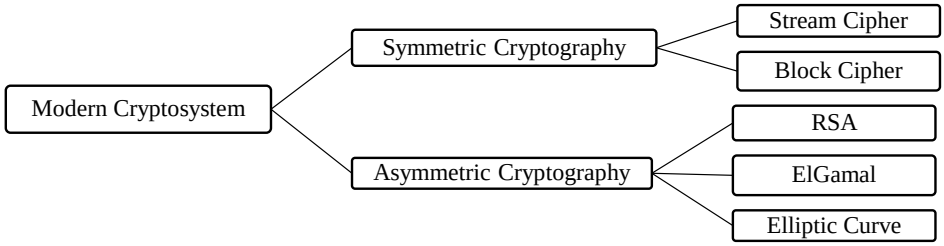

Figure 1. Modern Cryptography – Classification

2. Related Works.

The proposed model is an engender of the literature review of [3], [4], [5], [6], [9] and [15]. Table 1 below elucidates the related works and the proposed models by the authors of the literature reviewed articles in the field of DH Key Exchange and the RSA.

Table 1. Related Works Description in the field of RSA and DH Key Exchange

Author	Description
A.S. Khader, D. Lai.[3]	Proposed an efficient approach of preventing DH Key Exchange against the MITM attack. In their proposed model, they have used Geffe generator to yield a sequence of binary characters with high randomness to ensure non-transmission of the secret keys through channel rather hashed and stored in the server.
J.E. Avestro, A.M. Sison, R.P. Medina.[4]	Proposed model is based on hybrid cryptography of modified Diffie – Hellman key exchange algorithm and RSA in order to prevent MITM attack, thus resulting in a secure algorithm. They have implemented it in such a manner that two-tier security is ensured.
In-A Song, Young-Seok Lee.[5]	The authors have given a suggestion of a protocol to prevent the MITM attack. They have achieved it by using timestamp along with compare to the already existing approaches. Proper examination and analysis aid them in concluding with the results.
A. Taparia, S.K. Panigrahy, S.K. Jena.[6]	Research work was entitled on presenting a three-round key-exchange protocol but with minimum user interference along with the cover of security by combining commitment scheme with the authentication strings to seize the MITM effects. They also concluded that their results can be used for wireless networks.
Tianjie Cao, Dongdai Lin. [9]	It was the joint venture of the entitled authors to figure out and conclude the susceptible nature of the Authenticity of Password in the Key-Exchange based on RSA to dictionary attacks. Their major focus throughout the paper lies in the cryptanalysis of the password validation.
P. Yellamma, C. Narasimham, V. Sreenivas.[15]	Discussion and implementation RSA in data storage as well as security in the cloud has been the focus and the novelty of their work, thus inferring that this public-key cryptosystem has the ability to provide high level of required security when it comes to concealment approach for data of high potential.

Thus, as cited in the list above, the related works are concentric about the security attack to which the DH key exchange protocol is susceptible to as well as the security level provided by the RSA cryptographic system using its encryption-and-decryption techniques. The subsequent sections of the paper discussed about those protocols and methodologies, followed by the proposed model.

3. Algorithms

Prior to discussion of the proposed model and illustrating it with required citations as well as snapshots of executed code, pre-requisite is knowledge about the cryptography system and the protocol used to arrive at the intended result of the work.

3.1 Diffie – Hellman Key – Exchange Algorithm

It a protocol that involves sharing of the public keys amongst the sender and receiver to yield a shared secret key for further message transfer through encryption methodology [3]. This protocol is used for generating keys in the ElGamal and ECC cryptosystems [2]. It is demonstrated in table 2 and figure 2.

Assume, Alice and Bob are two users where both would like to establish such a communication among themselves that it remains concealed and secured. The finally obtained shared secret key 'k' is the common key to be used by Alice and Bob for encryption and decryption. It would follow in such a manner that Bob deciphers the encrypted text received from Alice using 'k' [1]. Thus, both the sides computed values of 'k' must be the same values for encryption and decryption purposes [7].

Table 2. Diffie-Hellman Key Exchange Protocol

	Algorithm Steps
1	Agreement on large prime number 'p' and base generator 'g' **Alice** • 'a' as secret key • $\alpha = g^a \pmod p$ … (1)
2	**Bob** • 'b' as secret key • $\beta = g^b \pmod p$ … (2) Here, α and β are the public keys.
3	**Exchange of public keys :** α is shared with Bob and β is shared with Alice **Alice** • Receives β from Bob • $k = \beta^a \pmod p$
4	**Bob** • Receives α from Alice • $k = \alpha^b \pmod p$ Measuring 'k' values
5	Alice : $k = \beta^a \pmod p = g^{ab} \pmod p$ [from (1)] Bob : $k = \alpha^b \pmod p = g^{ba} \pmod p$ [from (2)] Thus , k(Alice) = k(Bob) where k is the shared secret key.

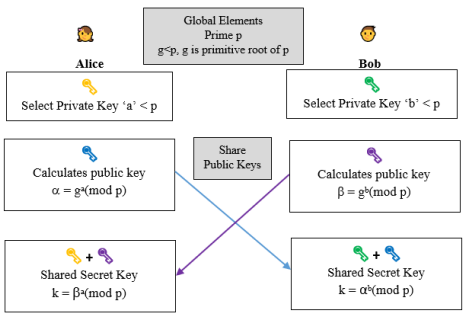

Figure 2. DH Key Exchange – diagrammatic view

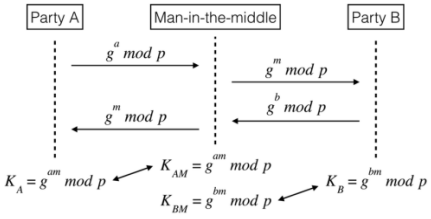

Figure 3. Man-in-the-Middle Attack [16]

3.2. Man-in-the-Middle (MITM) attack on DH Key Exchange Protocol

Illustration in the figure 2 states the fact that an eavesdropper in the middle would serve as the man in middle. DH Key Exchange is highly susceptible to the MITM attack that involves interference of a third person who intercepts the public keys while they get exchanged [2].

Assume that Eve is the third person and is willing to figure out the communication happening amidst Alice and Bob.[2] He tries and does successfully interception of the public key shared by Alice to Bob. So, the possible attack occurs in the 3rd step, which is illustrated in figure 3. Once Eve, having his own private keys, gets the knowledge of Alice public key, would now compute his own public key using his own private key and shares it with Bob. Unfortunately, Bob comprehends the received public key as the public key shared by Alice and thus uses it for further computation of the secret key value of 'k' (as in step 4 of table 3). Eve shares his public key with Alice as well, making her feel that it is the public key shared by Bob and thus she also uses it to calculate 'k'.[2]

Table 3. MITM Attack on DH Key Exchange Protocol

	Steps
	Initiation :
1	Agreement on large prime number and base generator, 'p' and 'g' respectively, such that : (p,g > 0) and (p>g) **Alice** • 'a' as secret key and calculates $\alpha = g^a \pmod p$ (1) **Bob**
2	• 'b' as secret key and calculates $\beta = g^b \pmod p$ (2) Thus this step involves computing the public keys(α and β) by their own private keys . The classical Diffie-Hellman key exchange protocol remains the same till the current step. **Exchange of public keys** : α is shared with Bob and β is shared with Alice ***Eve*** has the knowledge of 'g' and 'p'
3	• Intercepts α • Private key : 'z' • Computes $\boldsymbol{\lambda} = g^z \pmod p$ (3) • Shared with Alice and Bob
4	**Alice** • Intercepts $\boldsymbol{\lambda}$ as public key of Bob • Computes $k1 = \boldsymbol{\lambda}^a$. (mod p) **Bob** • Intercepts $\boldsymbol{\lambda}$ as public key of Alice • Computes $k2 = \boldsymbol{\lambda}^b$. (mod p) ***Eve*** • Computes $k1 = \alpha^z$. (mod p) • Computes $k2 = \beta^z$. (mod p)
5	Measuring k1 and k2 values : **Alice:** $k1 = \boldsymbol{\lambda}^a$. (mod p) = g^{za} . (mod p) : Alice-Eve key [using equation 3] **Bob :** $k2 = \boldsymbol{\lambda}^b$. (mod p) = g^{zb} . (mod p) : Bob-Eve key [using equation 3] **Eve :** $k1 = \alpha^z$. (mod p) = g^{az} . (mod p) [using equation 1] $k2 = \beta^z$. (mod p) = g^{bz} . (mod p) [using equation 2] Hence, Eve possesses the keys that Alice and Bob have, and which they might use for message transfer. Thus, the system is attacked.

3.3 RSA Cryptography

RSA Cryptography is a public – key asymmetric cryptosystem, developed and proposed by Rivest-Shamir-Adleman [13]. As the name entails, asymmetric (or non-symmetric) cryptosystem involves two keys: public and private key. Message hiding or encryption, done using public key while decrypting the encrypted message on the receiver side requires the use of the private or the secret key [8].

RSA is a public key cryptosystem; thus, it involves both public keys and private keys. It is generally based on the basic idea of one-way trapdoor function; its properties make it easy to share the public keys without security threat to the private key [14]. It involves three distinct phases [Table 4] of key generation, encryption followed by decryption [11]. The key generation would involve random generation of two distinct prime numbers, which are known only to Alice and Bob [10]. Further steps and phases involved in RSA is enlisted below. The mathematics involved in this process is calculation of inverse and modulus(remainder).

Table 4. RSA(Rivest-Shamir-Adleman) Cryptography methodology description

Number of steps	Key Generation Phase : done by Alice, the intended receiver
1	Random generation of two large and distinct prime numbers : P and Q
2	Compute • $n = PQ$ • $\Phi(n) = (P - 1)(Q - 1)$
3	Choose random prime number as e, such that : (i) $1 < e < \Phi(n)$ (ii) (e, $\Phi(n)$) are co-primes.
4	Secret key 'd' is calculated as : $d \equiv e^{-1} \pmod{\Phi(n)}$
5	Public key = { e, n } → shared with Bob Secret key = {d , n} → Kept with herself
Encryption Phase : done by Bob , intended sender.	
6	'm' is the message Bob will transfer to Alice. For that, he hides it as 'C' using the following RSA encryption strategy : Ciphertext, $C \equiv M^e \pmod{n}$ Bob encrypts his message and thus C , the encrypted version of the message is sent to Alice.
Decryption Phase : done by Alice, intended receiver.	
7	Alice receives message C from Bob through an insecure channel. He understands it is an encrypted message and thus decrypts it using her own secret key 'd'. $m \equiv C^d \pmod{n}$ Alice achieves to receive the correct and intended message m , sent by Bob.

Notable remark over here is only when the prime numbers P, Q are known to any person only then RSA would be susceptible to attack of an adversary otherwise which breaking the system to discover the encrypted message being transferred is nearly impossible [12].

4. Limitations and Scope

The scope of the discussed paper lies within easy-to-understand integer values with the limitations of extensive work for higher number of key-size bits.

5. Proposed Work (Research Methodology).

The proposed methodology involves the integration of RSA encryption/decryption technique in the DH Key Exchange. The algorithm is described in the table 5 with illustration-aided validation in the subsequent table 6 validating the proposed model.

Table 5. RSA-Integrated Diffie-Hellman Key-Exchange Protocol

Number of Steps	Description
1	Random generation of large prime numbers : p, q, X and g such that : • $0 < g < p$, $0 < g < q$, $p \neq q$ and $g < X$ So, 'p' and 'q' : large and distinct prime numbers and at the same time greater than the value of the base generator 'g'. Note – • 'p' and 'q' : secret and known only to Alice and Bob. • X and g are global elements.
2	Compute : $n = p \times q$ and $\Phi(n) = (p - 1) \times (q - 1)$
3	Alice and Bob agree on random generated 'e' such that : $(\Phi(n) > e)$, $(\Phi(n), e > 1)$ and they are co-primes.
4	**Alice** • Selects $a < X$ • Computes $d_1 \equiv e^{-1}(\bmod \Phi(n))$ • Public key $\alpha = g^a(\bmod X)$ • Public key encryption of α $C_1 \equiv \alpha^e(\bmod n)$ • Decrypting received message $\beta = R_1 \equiv C_2{}^{d}{}_1(\bmod n)$ • Secret key calculation $k_1 = \beta^a(\bmod X) = g^{ba}(\bmod X)$ **Bob** • Selects $b < X$ • Computes $d_2 \equiv e^{-1}(\bmod \Phi(n))$ • Public key $\beta = g^b(\bmod X)$ • Public key encryption of β $C_2 \equiv \beta^e(\bmod n)$ • Decrypting received message $\alpha = R_2 \equiv C_1{}^{d}{}_2(\bmod n)$ • Secret key calculation $k_2 = \alpha^b(\bmod X) = g^{ab}(\bmod X)$
5	$k_1 = g^{ba}(\bmod X) = g^{ab}(\bmod X) = k_2 = k$, which is the **secret key, shared amongst both.**

Table 6. Validation of RSA-Integrated Diffie-Hellman Key-Exchange Protocol

	Steps
1	Let **$p = 13, q = 11, X = 23$ and $g = 9$** Condition check : $(p = 11) \neq (q = 3)$, $(p > g)$, $(q > g)$, $(p, q, g > 0)$ and $(g < X)$. **Global elements : { X=23 , g=9 }**
2	Computing n and $\Phi(n)$ • $n = 13*11 = 143$ and $\Phi(n) = (11 - 1)*(13 - 1) = 120$
3	Alice and Bob agree on random generated 'e' such that : $(\Phi(n) > e)$, $(\Phi(n), e > 1)$ and they are co-primes. So, they choose $e = 13$: $(1 < 13 < 120, \gcd(13,120) = 1)$.
4	**Alice** • Selects $a = 4$. $(4 < 23)$ • Computes $d1 \equiv 13^{-1}(\bmod 120) = 37$. • Public key $\alpha = 9^4(\bmod 23) = 6$ • **Public key encryption of α** **$C_1 \equiv 6^{13}(\bmod 143) = 84$** • **Decrypting received message** **$\beta = R_1 \equiv 81^{37}(\bmod 143) = 16$** Thus, the public key of Bob is shared with Alice with confidentiality ensured. • Secret key $k_1 = 16^4(\bmod 23) = 9$ **Bob** • Selects $b = 3$ $(3 < 23)$ • Computes $d2 \equiv 7^{-1}(\bmod 120) = 37$. • Public key $\beta = 9^3(\bmod 23) = 16$ • **Public key encryption of β** **$C_2 \equiv 16^{13}(\bmod 143) = 81$** • **Decrypting received message** **$\alpha = R_2 \equiv 84^{37}(\bmod 143) = 6$** Thus, the public key of Alice is shared with Bob with confidentiality ensured. • Secret key $k_2 = 6^3(\bmod 23) = 9$
5	$k_1 = k_2 = 9 = k$. Thus , 9 is the secret key, possessed by both Alice , Bob.

6. Implementation and working of RSA-Integrated DH Key-Exchange Protocol.
Table 5 clearly elucidates the algorithm of the proposed work.

Alice and Bob are two users who wish to communicate among themselves in a secured manner. They make a proposal that their public keys should be encrypted such that when shared and exchanged are known only to them and no one else can intercept it. The proposed model integrates the RSA system into the Diffie-Hellman Key Exchange algorithm to meet the same. Initially it generates 4 large non-negative , non-zero random numbers – p, q, X and g such that they meet certain necessary conditions:

- p and q are distinct
- p, q are larger than the base generator 'g' value
- global element X is greater than 'g'
- p and q are kept private while X, g are global elements.

This is followed by RSA protocol of determining 'n' and 'Φ(n)' values required to compute the public and private keys of each of the users. As mentioned in step 2 of table 4 as well as table 5,

- n = product(p,q)
- Φ(n) = product((p-1), (q-1)). Φ(n) is regarded as the Euler's totient function.

Now, Alice and Bob agrees on a randomly generated value 'e' such that Φ(n) and 'e' are co-primes (mathematically, it refers to their greatest common divisor as 1) as well as Φ(n) is larger to the value of 'e'. Alice and Bob select their own secret keys 'a' and 'b' respectively such that (a, b) < X. Modulo inverse of 'e' with respect to Φ(n) results in the another set of private keys 'd1' and 'd2' computations by Alice and Bob respectively while 'α' and 'β' are determined by Alice and Bob as exponential functions of g with their respective secret keys, modulus X.

Since the proposed system majorly involves DH key exchange algorithm, following steps would involve exchange of the computed public keys of Alice and Bob amongst themselves over an insecure channel. Prior to this, the initially computed 'e' and 'n' would be used to encrypt the public keys 'α' and 'β'. Any third-party attacker requires to have the prior knowledge of 'p' and 'q' in order to break those ciphertexts since 'n' is a product of those secret large prime numbers. Encryption of the public keys would be followed by exchanging those ciphers amongst the users – Alice and Bob. The computed set of private keys 'd1' and 'd2' would suffice in helping the users to decrypt the received ciphers to gain the originally shared public keys. Once Alice has decrypted the public key of Bob using 'd1' and Bob of Alice using 'd2', DH exchange algorithm follows in determining the shared secret keys 'k1' and 'k2' using respective secret keys and the decrypted public keys.

As explained above, an adversary may aim to determine the ciphers exchanged but it would be nearly impossible to break the value of the product of the secretly kept large prime numbers.

7. Results and Discussions.
RSA-Integrated DH-Key exchange algorithm involves both the Diffie-Hellman key-sharing protocol as well as the RSA cryptosystem. It becomes immensely important to compare the performance of the newly proposed system with respect to the used systems in the model. Also important to note is the fact that the proposal made would be less prone to the MITM attack unlike the classical DH key exchange algorithm.

The implementation of the proposed model is displayed in Figure 4, along with the time taken to execute the proposed algorithm. This is an approach that details the merge of RSA cryptosystem in the DH Key Exchange for concealment of the public keys exchanged amongst Alice and Bob. Performance Analysis of this model [Table 7] can be performed in contrast to the already established and existing models.

It is definite to mark that complexity of the algorithm, proposed in Section 5, would be higher than the existing methodologies of RSA cryptosystem and the DH Key Exchange Algorithm. But it would be definitely less or not prone to the MITM attack where the eavesdropper would not be able to decipher the encrypted public keys without the knowledge of the secret key computed based on the RSA scheme, and thus can be defined as a better approach for preventing the MITM attack of the Key Exchange Protocol.

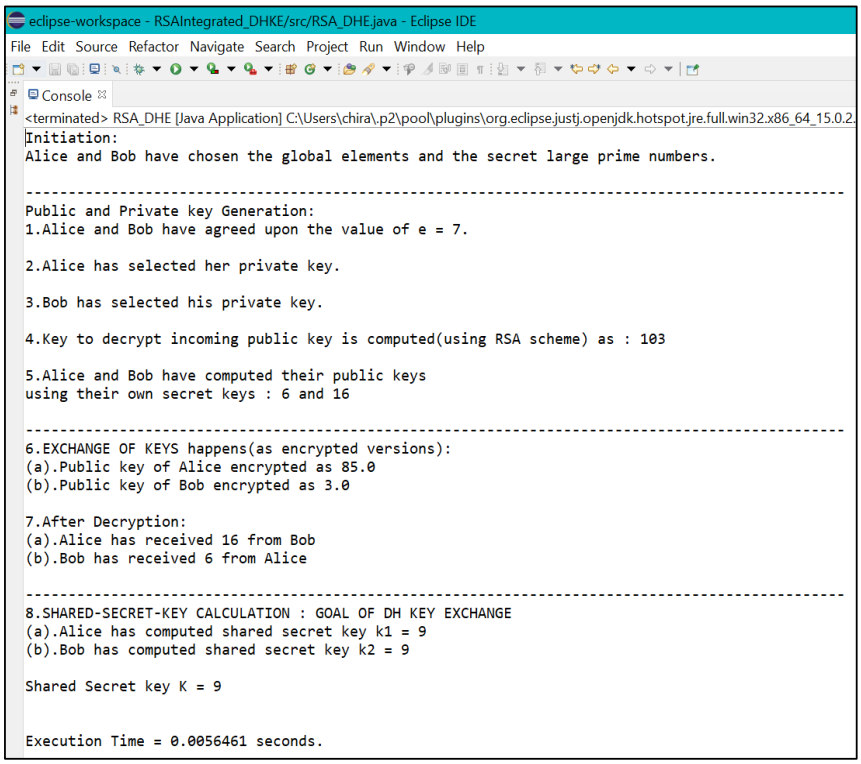

Figure 4. Proposed Model Implementation.

Table 7. Performance Analysis and Comparison of proposed work with existing models

Algorithm	Performance with respect to time
Proposed Model : RSA-Integrated Diffie-Hellman Key Exchange Protocol	0.0056461 seconds.
Cryptosystem : RSA Cryptography System	0.0060817 seconds.
Algorithm : Diffie-Hellman Key-Exchange Protocol	0.0088370 seconds.

8. Conclusion and Future Work

The paper has introduced a model that would amalgamate the RSA cryptosystem phases of key generation, encryption and decryption into the well-known DH Key Exchange for preventing the latter to be prone to the MITM attack.

In future, extension to the current model would be primary focus for implementation within the cryptosystems that utilizes DH Key Exchange Protocol for key-generation. Also, examining higher values for input to ensure no breach to security throughout public key exchange would even be considered in the long run.

References.

[1]. Nan Li, "Research on Diffie-Hellman key exchange protocol," *2010 2nd International Conference on Computer Engineering and Technology*, 2010, pp. V4-634-V4-637, doi: 10.1109/ICCET.2010.5485276.

[2]. Stallings, W., 2006. *Cryptography and network security, 4/E*. Pearson Education India.

[3]. A. S. Khader and D. Lai, "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol," *2015 22nd International Conference on Telecommunications (ICT)*, 2015, pp. 204-208, doi: 10.1109/ICT.2015.7124683.

[4]. J. E. Avestro, A. M. Sison and R. P. Medina, "Hybrid Algorithm Combining Modified Diffie Hellman and RSA," *2019 IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E)*, 2019, pp. 100-104, doi: 10.1109/TIME-E47986.2019.9353292.

[5]. In-A Song and Young-Seok Lee, "Improvement of Key Exchange protocol to prevent Man-in-the-middle attack in the satellite environment," *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2016, pp. 408-413, doi: 10.1109/ICUFN.2016.7537060.

[6]. A. Taparia, S. K. Panigrahy and S. K. Jena, "Secure key exchange using enhanced Diffie-Hellman protocol based on string comparison," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 722-726, doi: 10.1109/WiSPNET.2017.8299856.

[7]. G. Yang, J. Chen, Y. Lu and D. Ma, "An efficient improved group key agreement protocol based on Diffie-Hellman key exchange," *2010 2nd International Conference on Advanced Computer Control*, 2010, pp. 303-306, doi: 10.1109/ICACC.2010.5486666.

[8]. X. Huang and W. Wang, "A Novel and Efficient Design for an RSA Cryptosystem With a Very Large Key Size," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 10, pp. 972-976, Oct. 2015, doi: 10.1109/TCSII.2015.2458033.

[9]. Tianjie Cao and Dongdai Lin, "Cryptanalysis of two password authenticated key exchange protocols based on RSA," in *IEEE Communications Letters*, vol. 10, no. 8, pp. 623-625, Aug. 2006, doi: 10.1109/LCOMM.2006.1665131.

[10]. K. N. Bangera, N. V. S. Reddy, Y. Paddambail and G. Shivaprasad, "Multilayer security using RSA cryptography and dual audio steganography," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017, pp. 492-495, doi: 10.1109/RTEICT.2017.8256645.

[11]. S. A. Jaju and S. S. Chowhan, "A Modified RSA algorithm to enhance security for digital signature," *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, 2015, pp. 1-5, doi: 10.1109/IEMCON.2015.7344493.

[12]. I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," *2017 World Congress on Computing and Communication Technologies (WCCCT)*, 2017, pp. 172-175, doi: 10.1109/WCCCT.2016.50.

[13]. R. Minni, K. Sultania, S. Mishra and D. R. Vincent, "An algorithm to enhance security in RSA," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013, pp. 1-4, doi: 10.1109/ICCCNT.2013.6726517.

[14]. T. Wenxue, W. Xiping, X. Jinju and P. Meisen, "A mechanism of quantitating the security strength of RSA key," *2010 Third International Symposium on Electronic Commerce and Security*, 2010, pp. 357-361, doi: 10.1109/ISECS.2010.85.

[15]. P. Yellamma, C. Narasimham and V. Sreenivas, "Data security in cloud using RSA," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013, pp. 1-6, doi: 10.1109/ICCCNT.2013.6726471.

[16]. Yang, Xuechao & Yi, Xun & Khalil, Ibrahim & Fengling, Han & Tari, Zahir. (2016). Securing Body Sensor Network with ECG. 298-306. 10.1145/3007120.3007121.