International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AN INNOVATIVE APPROACH TO KEY EXCHANGE: DUAL SECURED DIFFIE - HELLMAN WITH RSA AND IMPROVED AFFINE CIPHER INTEGRATIONS

Mrs. R. Ramakrishnaveni[1] and Dr. K. Santhi[2]

[1]Research Scholar, Department of Computer Science,
Dr.N.G.P. Arts and Science College, Bharathiyar University, India
ramakrishnaveni0123@gmail.com

[2] Professor, Department of Information Technology,

Dr. N.G.P. Arts and Science College, Bharathiyar University, India

santhi@drngpasc.ac.in

Abstract

The pace of technological change is sprouting at an incomparable rate, with emerging technologies such as Artificial Intelligence, Internet of Things, Block chain transforming industries and reforming the way we live now-a-days. However, this rapid pace of change presents significant challenges for data security. The role of data security ensure the confidentiality, integrity and authenticity while data in transit and data at rest. Cryptography is the science to refer as the secured transmission of messages amongst the sender and the intended receiver. In cryptography, there are two kind of algorithms employed in which generates key concepts in dealing with security protection between two parties over an internet. On the side of symmetric algorithm, it is possible to generate only one secret or private key to secure the message between two parties where as in the side of asymmetric algorithm, it would generate two keys referred as public key for encryption process as well as private key for decryption process to strengthen the security protection of message transmission. In these aspects, RSA algorithm is integrated with Diffie –Hellman Key Exchange protocol to prevent Man-in the Middle attack. However, the analysis of RSA cryptography, it has a vulnerability in small number prime factorization. Consequently, this paper proposes a model of implementation of Diffie-Hellman Key Exchange protocol is integrated with RSA and improved Affine Cipher to afford greater strength to the key.

Keywords: DH Key Exchange, RSA and Improved Affine Cipher.

I. INTRODUCTION

In the modern era, the data security plays the main role for the people those who intentionally wish to communicate and do transaction in secure manner over a public network now-a-days. In the facet, cryptography is the technique of transforming information into unreadable form in order to safeguard it. It is used to prevent unauthorized data access. It is a kind of symmetric and asymmetric keys as specified in the figure 1. In a symmetric key process, the encryption and decryption procedures are carried out using the private key or single key between sender and receiver but, whereas in asymmetric key process, the encryption and decryption procedures

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

are carried out using public key and private key to secure the message in more safe[1][2]. On the other hand, modern crypto system employs in an integrated keys used for encryption and decryption of data security and make it more efficient. Based on these systems, the symmetric and asymmetric algorithms encountered as an Affine Cipher integrated with Diffie - Hellman and RSA Key Exchange Protocol [3].

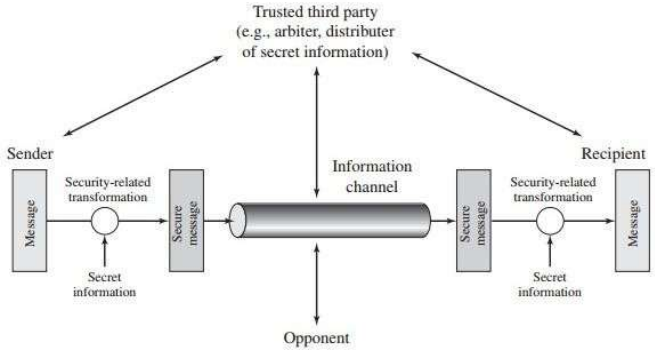

Figure 1: Model of a Crypto System

A. Diffie-Hellman Key Exchange Algorithm

This algorithm is one of the asymmetric algorithm formulated by its namesakes Whitfield Diffie and Martin Hellman in 1976. As given in the figure 2, this algorithm generates a shared secret key among two parities with the help of public and private keys. But the algorithm has a susceptibility towards attack that is prone to Man-in-the-Middle (MITM) attack [4][6]. This algorithm allows two parties to securely agree on a shared key among them. It is used in the SSL / TLS protocols to securely establish a session key for encrypting data between source and destination. It permits a secure method for exchanging keys between remote users and a VPN server [5].

Diffie-Hellman Key Exchange

Step	Alice	Bob
1	Parameters: p, g	
2	A = random() $a = g^A \pmod p$	random() = B $g^B \pmod p = b$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = g^{AB} \pmod p = K$
5	$\longleftarrow E_K(data) \longrightarrow$	

Figure 2: Procedure for Diffie-Hellman Key Exchange

DH Key Exchange - Specification

i) Alice and Bob agree on two large prime numbers, p and g and a public key exchange algorithm.

ii) Alice select a secret integer, a and computes $\alpha = g^a \bmod p$ and send α to Bob.

iii) Bob select a secret integer, b and computes $\beta = g^b \bmod p$ and send β to Alice.

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

iv) Alice computes $s = \beta^a \bmod p$ and Bob computes $s = \alpha^b \bmod p$.
v) Alice and Bob have shared a secret keys, which they can use to establish a secure communication channel.

B. Rivest Shamir Adleman Algorithm

In RSA, this algorithm was developed by the authors Rivest Shamir Adleman in 1978. The significant algorithm of asymmetric aspect, it comes under integer factorization. It depends two prime number factoring technique [6]. The strength of this algorithm depends on complexity of factoring and improving the speed in encryption and decryption of the cipher schemes specified in the beneath figure 3.

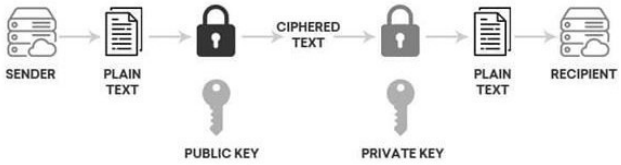

Figure 3: Procedure of Asymmetric Crypto System

RSA Algorithm Specification

RSA is a method of asymmetric algorithm based on public key as well as private key considered for encoding and decoding the messages. It is for multiplying two prime factors together and secreting their integral part for secure communications [7]. Here, the public key is used to encrypt the data while the private key is used to decrypt the data and it's known only to the user. To encrypt, the plaintext can be encrypted by using the public key pair as e and n. To decrypt, the cipher text can be deciphered by using the private key pair as d and n [9].

a. Key Generation

i) Choose two large prime numbers (p and q)
ii) Compute (Prime Factorization) : $n=p*q$
iii) Compute (Euler's Totient Function) : $\Phi(n)=(p-1)(q-1)$
iv) Choose a number e (Public exponent) where $1 < e < \Phi(n)$
v) Compute (Private Exponent) : $d = e^{-1} \pmod{\Phi(n)}$
vi) Bundle the public key pair as (e, n)
vii) Bundle the private key pair as (d, n)

b. Encryption Process

If the plaintext is m, cipher text (c) = $m^e \bmod n$.

c. Decryption Process

If the cipher text is c, plaintext (p) = $c^d \bmod n$.

C. Affine Cipher Algorithm

The simplest mono-alphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher. To be able to apply mathematical operations on the plaintext, affine cipher combines with the additive and multiplicative ciphers with a pair of keys [8]. The first key is used with the multiplicative cipher; the second key is used with the additive cipher. However, we have used a temporary result (T) and have indicated two separate operations to show that whenever we use a combination of ciphers we should be sure that each

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

one has an inverse at the other side of the line and that they are used in reverse order in the encryption and decryption as mentioned in the figure 4. If addition is the last operation in encryption, then subtraction should be the first in decryption [10][11].

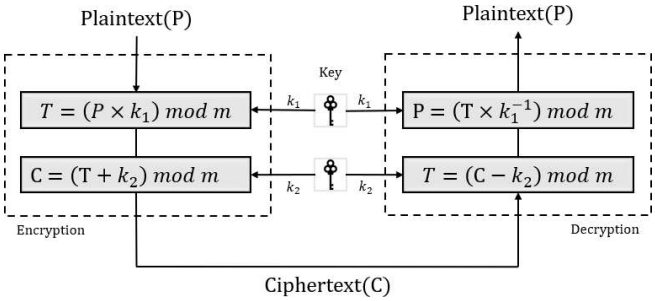

Figure 4: Steps for Affine Cipher Method

Affine Algorithm Specification

Affine is a symmetric algorithm for encryption and decryption process. The keys k_1 and k_2 are considered as prime factors for manipulating cipher text and decipher text.

a. Key Generation

i) K_1 key is a prime factor for multiplicative cipher text.

ii) K_2 key is a prime factor for additive cipher text.

b. Encryption process

i) $T = (C_1 \,.\, k_1) \bmod m$

ii) $C = (T + k_2) \bmod m$

c. Decryption process

i) $T = (C - k_2) \bmod m$

ii) $C = (T \,.\, k_1^{-1}) \bmod m$

II. LITERATURE REVIEW

Chiradeep Gupta and N V Subba Reddy, Shabbir Hassan, Arman Rasool Garidi and Ahmad Raza Shibli considered Diffie-Hellman Key Exchange Protocol introduced the public key algorithm in the cryptosystem. In DH algorithm, two prime numbers were taken initially and public key exchange happened at both sender and receiver then they have shared their secret key to establish the communication channel [10][17]. While exchanging the key, there is no encryption and decryption process implemented here so, Man-in-the-Middle (MIIM) attack may happen in the communication medium. Addulrahman Alhamada, Othman Omran Khalifa examined, that to overcome MIITM issue, an integration algorithm is fused in this part [12][16].

Dua M. Ghadi and Bo Hou observed, RSA algorithm suggested to have two large prime numbers for prime factorization. Then, Euler's Totient function is computed and private exponent is employed with modular multiplicative inverse with public exponent value [13]. With this strong number theory based mathematical background, RSA algorithm offer an encryption and decryption process fused with DH Key Exchange to prevent the attacker while transmission over a public channel [17]. Even though, RSA produces a secure channel, the

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

interceptor may guess its prime numbers and make it failure one. To prevent this attack, key enhancement is required further one to stopover the attempt [14][20].

Septi Yana Wulandari and Donagani Ramakrishna, Mohammed examined, Affine Cipher is a symmetric process, but it uses the mathematical background with distinct prime numbers secreted from both sides separately to compute the encryption and the decryption process. Generally affine cipher is applied for alphabetic characters for crypto process, here, affine cipher process is customized with an integrated DH and RSA Key Exchange encryption and decryption process [15][18]. In the customized affine cipher process, the modular value is based on RSA encrypted key value for further crypto process. As per process given in Table 1, the algorithm is customized approach for further strengthening the encrypted key of an integrated DH and RSA Key Exchange process and it is demonstrated as the proposed work[16][19].

III. PROPOSED METHODOLOGY

Primary steps for proposed algorithm

1. Random generation of large prime numbers : p, q, X and g such that :

$0 < g < p$, $0 < g < q$, $p \neq q$ and $g < X$

2. So, ‘p’ and ‘q’: large and distinct prime numbers and at the same time greater than the value of the base generator ‘g’.

Note:

i) ‘p’ and ‘q’ : secret and known only to Alice and Bob

ii) X and g are global elements.

3. Compute:

i) Prime Factorization : $n = p \times q$ and

ii) Euler’s Totient Function : $\Phi(n) = (p - 1)(q - 1)$

4. Alice and Bob agree on random generated ‘e’ such that ($\Phi(n) > e$), ($\Phi(n), e > 1$) and they are co-primes.

5. Select prime keys for k_1 and k_2 at Alice as well as Bob sides separately.

Table 1: Dual Secured on Diffie-Hellman with RSA and Affine Cipher Integrations

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Alice (Receiver)		Bob (Sender)	
i)	Select $a < X$	i)	Select $b < X$
ii)	Compute $d_1 \equiv e^{-1} (\text{mod } \Phi(n))$	ii)	Compute $d_2 \equiv e^{-1} (\text{mod } \Phi(n))$
iii)	DH : Public Key $\alpha = g^a \text{ (mod X)}$	iii)	DH : Public Key $\beta = g^b \text{ (mod X)}$
iv)	Public Key encryption on α in RSA $C_1 \equiv \alpha^e \text{ (mod n)}$	iv)	Public Key encryption on β in RSA $C_2 \equiv \beta^e \text{ (mod n)}$
v)	Encryption on DH & RSA using Affine $T = (C_1 \cdot k_1) \text{ mod m}$ $C_{11} = (T + k_2) \text{ mod m}$	v)	Encryption on DH & RSA using Affine $T = (C_2 \cdot k_1) \text{ mod m}$ $C_{12} = (T + k_2) \text{ mod m}$
vi)	Decrypting received c_{12} key $T = (C_{12} - k_2) \text{ mod m}$ $C_2 = (T \cdot k_1^{-1}) \text{ mod m}$	vi)	Decrypting received c_{11} key $T = (C_{11} - k_2) \text{ mod m}$ $C_1 = (T \cdot k_1^{-1}) \text{ mod m}$
vii)	Decrypting received Bob β key $\beta = D_1 \equiv C_2^{d_1} \text{ (mod m)}$	vii)	Decrypting received Bob α key $\alpha = D_2 \equiv C_1^{d_2} \text{ (mod m)}$
viii)	Finding secret key $K_{11} = \beta^a \text{ (mod X)}$	viii)	Finding secret keys $K_{12} = \alpha^b \text{ (mod X)}$

Key Exchange

Note: $K_{11} = k_{12} = k$ (k is the secret key for message encryption and decryption process).

IV. PROPOSED PROCEDURE OF MESSAGE ENCRYPTION AND DECRYPTION

Here, an encryption and decryption is employed in two different file formats. Since the secret key value is generated based on large bit size such as 256/512/1024. For speed up the encryption and decryption process in terms of effective performance, the generated secret key value will be reduced by using modulo operation with divider value either 1 byte or 2 byte or 4 byte value. This simplified value is reserved for both text and binary file format. They are demonstrated as given below.

i) Text File Format – Encryption and Decryption

The first one is proceeded with text file as input file along with UTF -8 encoding format employed for encryption and decryption. Here, an encryption is done by each character UTF-8 encoding value along with using secret key generated which is derived from the key enhancement algorithm as given by the table 1.

a. For an Encryption Process:

Cipher-text = File_ Each Char UTF- 8 encoding value + Secret key value

Here, the input file is opened to read an each character's UTF-8 encoding value and added with secret key value together. These value are reserved as encrypted text from sender side and proceed the same manner for all characters in an input file and send that cipher-text to the receiver.

b. For Decryption Process:

Plain-text = Cipher-text – Secret Key value

As received the cipher-text from sender, the receiver decrypts the cipher text that is subtracted from secret key value, afterward the receiver obtained the character value of original file content.

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ii) Binary File Format – Encryption and Decryption

For an encryption process, the raw byte is read from an image file or audio or video as input file. Here, the encryption and decryption are done in this manner as referred as type - I and type -II processes.

a. For an Encryption Process:

- Type – I Process:

R (Remainder) = (Binary File_Each Byte Value + Secret Key Value) mod 256

Here, a binary file is computed by the modulo operation by the value of 256. If the remainder value is under value of 255 then it is directly added with secret key value and computed value is reserved for encryption process.

- Type – II Process:

R (Remainder) = (Type – I Process: Remainder Value) mod 256

If the remainder value is greater of 255, then it goes for further modulo operation by the value 256. The second remainder value is added with secret key remainder value and that calculated value is encoded as encryption process.

b. For Decryption Process:

If received cipher-text value is generated using both Type-I and Type-II processes,

Plain-text = (Type – II Process: Remainder Value + 256) - Secret Key Value

If received cipher-text value is generated using only Type-I process,

Plain-text = (Type – I Process: Remainder Value - Secret Key Value)

V. RESULTS AND DISCUSSION

The proposed model of an integration of DH and RSA Key Exchange protocol is further enriched with affine cipher methods. It becomes immensely important to strengthen the encryption and decryption process while transmission at both sides. Also important to note is that 16 bit affine cipher is taken for prime key factors uniquely between sender and receiver. This model made would be less prone to MITM attack at DH Key Exchange and minimize the chance to attempt to break the RSA prime factorization. Affine cipher bit is customized for prime factors key selection as considered to RSA crypto system. This is an approach that details the fuse of Affine with DH and RSA Key Exchange for concealment of the public keys exchanged amongst Alice and Bob.

It is noticed that time consumption is little bit increasing in utilizing different file size such as text files and image file patterns. Assume time consumption part is feebly increasing, it would be definitely interceptor attempt to become failure. DH public key is fused for RSA key

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encryption then it is further merged with affine encryption to make it strengthen the key factor. This bond among these algorithms are effective to secure the key amongst Alice and Bob.

Also one important note is that would perform another cryptosystem passing the message from sender to receiver. It is strongly built with secret key with logical ethics. This tricky enactment can definitely holdup the message in a secured manner and it is shown in the table 2. Then, the analysis result report is generated based on the file inputs along with bits size and the type of file format as represented in the figure 5.

Table 2: Result of Implemented Proposed Model

Alice (Receiver)	**Bob (Sender)**
local_time start:2025-08-11T18:21:34.770005300 random number e = 44843 alice a (receiver) pns[4] = 44851 bob b (sender) pns[4]-1 = 44850 alpha = 899815313633791531746388183350553630986284230087296755932514066393047012839651360520270068695218982569364158342042896915832217659987369882089643081549310 Public key encryption of alpha (using RSA) C1 = 377961791887219974370435546980668718059096516713229366496029608852700593619709092519634042023982937932987982895836027706262136877571624613519897435122221053732100902214492885974388880046270954391001732779509768757039702559935150577245015681843850465342292714821879294876244705655501792093142822800679786189797	random number e = 44843 bob b(sender) = 44850 rsa_af_a = 44851 rsa_af_b = 44867 rsa_af_n = 377961791887219974370435546980668718059096516713229366496029608852700593619709092519634042023982937932987982895836027706262136877571624613519897435122221053732100902214492885974388880046270954391001732779509768757039702559935150577245015681843850465342292714821879294876244705655501792093142822800679786189797
	rsa_af_c = 16 Decrypting Alice C1 for computing alice RSA C1 using affine cipher decryption method C1 = 377961791887219974370435546980668718059096516713229366496029608852700593619709092519634042023982937932987982895836027706262136877571624613519897435122221053732100902214492885974388880004

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

16 bit affine k1 = 44851

rsa_af_n = 377961791887219974370435546980668718059096516713229366496029608852700593619709092519634042023982937932987982895836027706262136877571624613519897435122221053732100902214492885974388880046270954391001732779509768757039702559935150577245015681843850465342292714821879294873624470565550179209314282280067978618 98,rsa_af_a = 44851,rsa_af_b = 44867

rsa_af_c = 16

c2-rsa_af_a = 33601

c2-rsa_af_b = 33613

c2-rsa_af_n = 306869360943567620218263908422380473441799124052357083492864744867497227387853988780872762173791554975174641926069945490763226578329826315050646608647284852956143147532107495786471976616120372474627469694721880340431643866831182477627314391803611350856621935621671979026328412193553603691194856175923246084 73

c2-rsa_af_c = 12

Decrypting Bob C2 for computing Bob RSA C2 using affine cipher decryption method

C2 = 306869360943567620218263908422380462709543910017327795097687570397025599351505772450156818438504653422927148218792948736244705655501792093142822800679786189847056555017920931428228006797861897

beta = 291471044642822899680811283194721697477324581468044984361673107322889207765759401644702017659819916751552041233635771177983274438594703613469191421297213 5

Public key encryption of beta (using RSA) C2 = 306869360943567620218263908422380473441799124052357083492864744867497227387853988780872762173791554975174641926069945490763226578329826315050646608647284852956143147532107495786471976616120372474627469694721880340431643866831182477627314391803611350856621935621671979026328412193553603691194856175923246084 73

16 bit affine k1 = 33601

rsa_af_n = 306869360943567620218263908422380473441799124052357083492864744867497227387853988780872762173791554975174641926069945490763226578329826315050646608647284852956143147532107495786471976616120372474627469694721880340431643866831182477627314391803611350856621935621671979026328412193553603691194856175923246084 73,rsa_af_a = 33601,rsa_af_b = 33613

rsa_af_c = 12

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

7344179912405235708349286474486749 7227387853988780872762173791554975 1746419260699454907632285783298263 1505064660864728485295614314753210 7495786471976616120372474627469694 7218803404316438668311824776273143 9180361135085662193562167197902632 8412193553603691194856175923246084 72 sender beta = 2914710446428228996808112831947216 9747732458146804498436167310732288 9207765759401644702017659819916751 5520412336357711779832744385947036 134691914212972135 alice k1 = 6860131402852724870130827298391325 6293477878036478002236922766744212 5803334985607541905555004719013966 7481076728186632268805997898904848 271948658020993807 alice k1 mod by 256 = 15 local_time for file decryption end:2025-08-11T18:21:35.226817400 Execution Time is: 0.4568121 seconds	receiver alpha = 8998153136337915317463881833505536309 8628423008729675593251406639304701283 9651360520270068695218982569364158342 0428969158322176599873698820896430815 49310 bob k2 = 6860131402852724870130827298391325629 3477878036478002236922766744212580333 4985607541905555004719013966748107672 8186632268805997898904848271948658020 993807 bob k2 mod by 256 = 15 file size :1065 encryption done

International Journal of Applied Mathematics

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

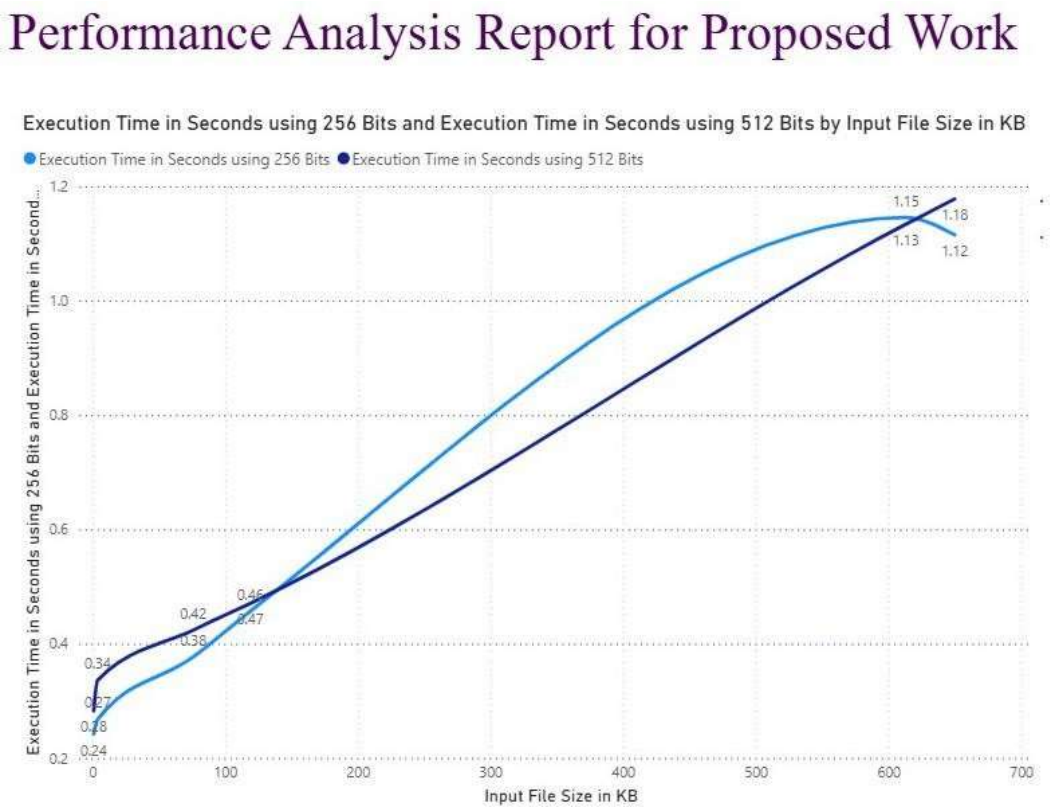

Figure 5: Performance Analysis Report for Proposed Work

VI. CONCLUSION AND FUTURE WORK

The proposed model has implemented an integrated model that would perform an effective Cryptosystem among DH-RSA-Affine Key Exchange encryption and decryption for preventing the MITM attack on top of fewer possible chance to reckon random prime numbers attack in RSA also in Affine and lead their attempt to be padlock while pony-trekking the security key.

In future part, the modified algorithms and various input parameters may be anticipated bestowing to the current scenario working atmosphere and the multi-organizations may require rarer improvement to seizure the attack.

VII. REFERENCES

[1]. Chiradeep Gupta and N V Subba Reddy, “Enhancement of security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography”, Journal of Physics: Conference Series (2022) 012014 doi:10.1088/1742-6596/2161/1/012014.

[2]. Dua M. GHADI, “A Study on Modified RSA Cryptosystem”, Internal Journal of Applied Sciences and Technology, 2023, Research Article, ISSN: 2717-8234.

Received: August 06, 2025

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[3]. Septi Yana Wulandari, "Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message", Proceedings of International Conference in Science and Engineering, ISSN2597-5250 Volume 3, April 2020.

[4]. Cryptography and Network Security Principles and Practice, by William Stallings, 8th Edition – Pearson Paper Back 2023.

[5]. Rashmi (2024). Improved Cyber Security in Healthcare Using an Advanced Encrypted System algorithm and Block Chain Technology. International Journal of Intelligent Systems and Applications, 12 (21s), 2837.

[6]. Bo Hou, "Number theory based modern cryptography: RSA and Diffie-Hellman algorithms" Proceedings of CONF-MPCS 2024, Workshop: Quantum Machine Learning: Bridging Quantum Physics and Computational Simulations, DOI:10.54254/2753-8818/51/2024CH0180.

[7]. Gyanvendra Pratap Singh, "A Brief Review on RSA Algorithm", @ 2024 IJCSPUB | Volume 14, Issue 2 May 2024 | ISSN: 2250-1770.

[8]. Sinambela, R. G., & Fauzi, A. (2023), "Development of Hybrid Encryption Method using Affine Cipher, Vigenere Cipher and Elgammal Algorithm to Secure Test Messages in a Data Communication System". Journal of Artificial Intelligence and Engineering Applications (JAIEA),2(2), 30-40.

[9]. Akash Thakkr and Ravi Gor, "Cryptographic method to enhance the Data Security using Elgamal algorithm and Kamal Transform", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727, Volume 24, Issue 3, Ser.III (May-June.2022), PP 08-14, doi:10.9790/0661-2403030814.

[10]. Shabbir Hassan, Arman Rasool Faridi, Ahmad Raza Shibli, A Novel Approach to Key Exchange : dual Secured Diffie – Helman with RSA Integration", International Journal of Information Securitiy", 2023.

[11]. A Hybrid Cryptographic Algorithm for Secure ECG data transmission and classification using CNN, Dr.S. Rajesh. ISSN 2349 – 5162, Journal of Emerging Technologies and Innovative Research, 2023.

[12]. Abhishek and Dr. Vandana, "A Study on Modified RSA Algorithm in Network Security", (Peer-Reviewd, Open Access, Fully Refereed International Journal), Volume: 04/Issue:04/April-2022.

[13]. M. Shifani Francis, J. Dhalia Sweetlin, "Secure Image Communication: Integrating Diffie-Hellman Key Exchange for Enhanced Confidentiality" 2024, 3rd International Conference on IEEE Society.

[14]. Shivam, Midha, S., and Ramola, B. "Cryptography in Network Security", 2022 International Conference on Cyber Resilience, DOI: 10.1109/ICCR56254.

Received: August 06, 2025

Volume 38 No. 11s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[15]. Ahmed, S, and Ahmed, T.2022, "Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review". International Journal of Scientific and Research Publications. 12(7),, pp.161-173.

[16]. Donagani Ramakrishna; Mohammed Ali Shaik, "A Comprehensive Analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges", Published in IEEE Access (Volume: 13), ISSN:2169-3536, DOI:10.1109/ACCESS.2024.3518533.

[17]. Abdulrahman Alhamada; Othman Omran Khalifa: Farah Diyana Bt. Abdul Rahman; Haidawati Mohamad Nasir, "Secure Key Exchange for Protecting Health Data Diffie-Hellman Based Approach", 2023 IEEE 9th Internatinal Conference on Smart Instrumentatin, Measurement and Applications (ICSIMA), DOI:10.1109/ICSIMA59853.2023.10373446.

[18]. Research Trends Review on RSA Scheme of Asymmetric Cryptography Techniques, Bulletin of Electrical Engineering and Informatics, Vol.10, No. 2021.

[19]. Comparing Symmetric and Asymmetric Cryptography in Message Encryption and Decryption by using AES and RSA Algorithms, Ridwan B.Marqa, ISSN No: 1006-7930.

[20]. A Handbook of Applied Cryptography by Alfred J. Menezes,Paul C. Van Oorschot and Scott A. Vanstone, CRC Press Series on Discrete Mathematics and Its Applications Bruce Schneir, "Applied Cryptography", CRC Press.

Received: August 06, 2025