Some Study on Public Key Cryptography Algorithms

Chithra Devi R[1] Ananda Devi R[2] Bharathy J[3]
[1,2,3]Assistant Professor
[1]Department of Information Technology [2,3]Department of Computer Science Engineering
[1]Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, Tamil Nadu, India [2,3]Govindammal Aditanar College for Women, Tiruchendur, Tamil Nadu, India

Abstract— In recent years, the need for security in web based applications has increased many folds. The desire of secrecy has led nations to turn to cryptography for effective and safe communication by implementing various encryption methods. In this paper, we made a detailed study on different cryptography algorithms such as RSA, Diffie-Hellman and ElGamal and its performance was assessed.

Key words: Data Encryption, Decryption, Ciphers, Security, Algorithm, RSA, Diffie-Helman and ElGamal

I. INTRODUCTION

Cryptography makes websites to perform electronic transmissions safe and secure. For a website, to secure all the transmitted data between the two parties, it must be properly encrypted. Due to the large number of commercial transactions on the internet, cryptography is the key in ensuring the security of the transactions. In the digital world, cryptography offers three core areas where protection is at most important and then authentication, integrity, and confidentiality [1]. In a web based application, when the user connects to the secure (HTTPS) websites such as Internet Banking application, the browser must establish a secure TLS session. The web page should be rendered in the browser in encrypted form. The client request and response between the client and the server is encrypted using public key encryption [2]. A web application uses public key cryptography to create a shared session key. It then communicates through.

Symmetric key cryptography using this shared session key. Public key cryptography remains the most popular online protocol (over private key cryptography) because users never need to transmit or reveal their private keys to anyone, which is used for the criminals discovering an individual's secret key during the transmission [3].

II. BASIC CONCEPTS

A. Public Key Cryptography

Public Key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication. Public-key algorithms are based on mathematical functions rather than substitution and permutation. Fig.1 shows the diagrammatic representation of cryptography. Fig. 2 shows how public key cryptography can be used when confidentiality, authentication and both are required.

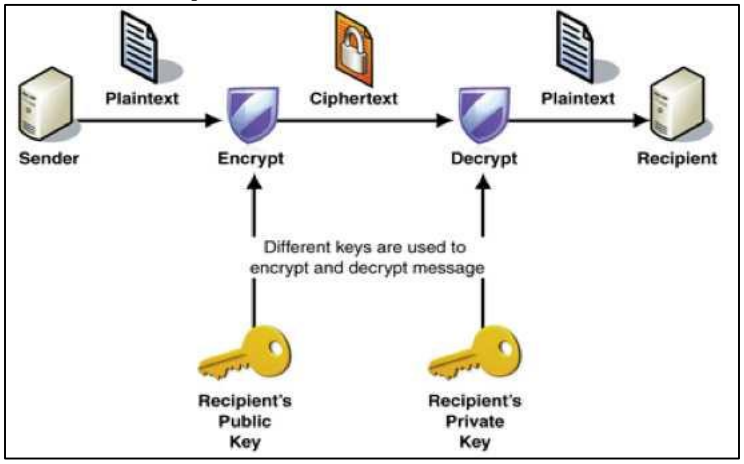

Fig. 1: Public Key Cryptography

B. Asymmetric Keys

Two keys, a public key and a private key, that are used to perform encryption and decryption or signature generation and signature verification.

C. Public Key Certificate

A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key [4].

D. Public Key Infrastructure (PKI)

set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

E. Public and private key

This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

F. Ciphertext

This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts [5].

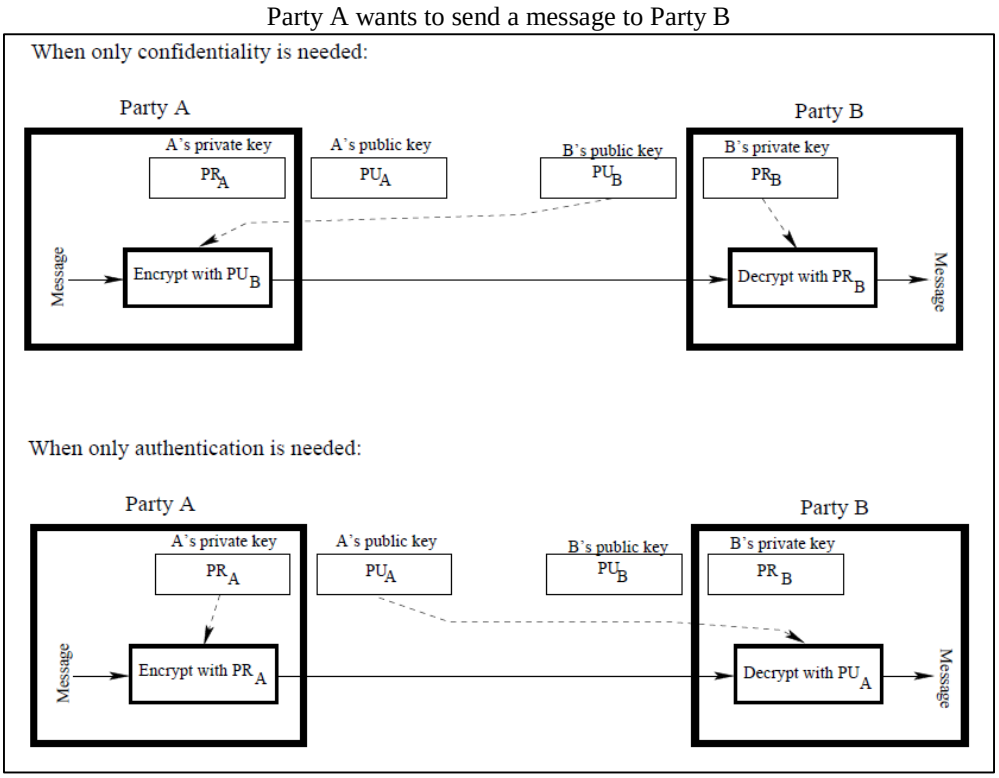

Fig. 2: Public key cryptography used when confidentiality, authentication and both are required respectively

Decryption algorithm- This algorithm accepts the ciphertext and the matching key, in turn produces the original plaintext.

III. CRYPTOGRAPHIC ALGORITHMS – A STUDY

A. Rivest-Shamir-Adleman (RSA)

This scheme is the most widely accepted and implemented general-purpose approach for public-key encryption. The public-key cryptography that was made possible by this algorithm was foundational to the e-commerce revolution that followed. It can be used to encrypt a message without the need to exchange a secret key separately. Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key. The minimum recommended key length for a secure RSA transmission is currently at least 1024 bits. A key length of 512 bits is no longer considered secure, although cracking it is still a tough task.

1) RSA – Algorithm:

Select two prime numbers, p and q.
Calculate n = pq.
Calculate f(n) = (p - 1) (q - 1).
Select e such that e is relatively prime to f(n) and less than f(n).
Determine d such that $d \equiv e^{-1} \pmod{f(n)}$
Public key PU = {e, n}
Private key PR = {d, n}

Ciphertext: $C = M^e \bmod n$ where, Plaintext: $M < n$
Plaintext: $M = C^d \bmod n$ where, Ciphertext: C

RSA provides security from the attacks such as Brute force, Mathematical attack, Timing attacks, Hardware fault-based attack and chosen cipher text attacks. The biggest advantage of RSA is that it is a public-key cipher, and this makes it a lot easier to solve the fundamental problem of cryptography, which is to safely distribute keys. Some of their weaknesses are:

- If a small exponent like e=3 is used and send the same message to different recipients and just use the RSA algorithm without adding random padding to the message, then an eavesdropper could recover the plaintext.
- If an attacker can convince a key holder to sign an unformatted encrypted message using the same key then she gets the original.

B. Diffie – Hellman Algorithm

The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages. Diffie-Hellman is a way of generating a shared secret between two people in such a way that the secret can't be seen by observing the communication [6]. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. At the end of the communication both sender and receiver have the same key. This is particularly useful because you can use this technique to create an encryption key with someone, and then start encrypting your traffic with that key. And even if the traffic is recorded and later analyzed, there's absolutely no way to figure out what the key was, even though the exchanges that created it may have been visible. This is where perfect forward secrecy comes from. Analyzing the traffic at a later date can break in because the key was never saved, never transmitted, and never made visible anywhere.

1) How it works?

For example, X and Y decide publicly on two prime numbers through Z, g and n. Generally g is a small prime number and n is quite large, usually 2000 or more commonly 4000 bits long. So now X, Y and Z all know these numbers. Now X decides secretly on another number, a. and Y decides secretly on a number, b. Neither X nor Y send these numbers, they are kept to themselves. X performs a calculation, g^a mod n, which is said to be A, since it comes from a. Y then performs g^b mod n which is said to B.

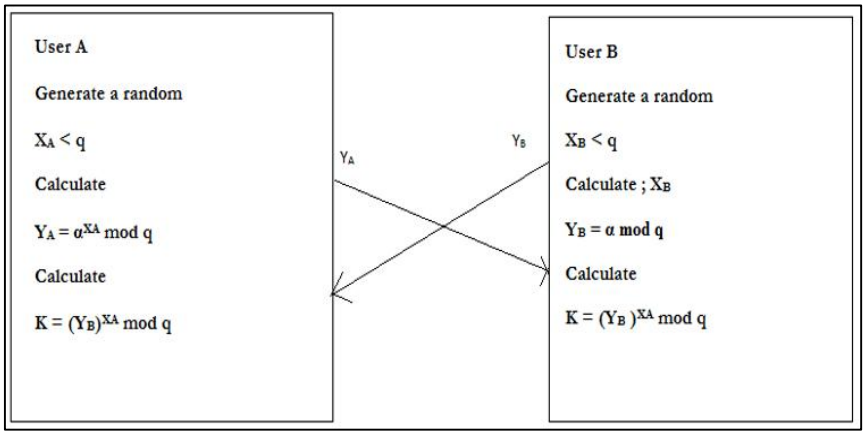

Fig. 3: Diffie – Hellman Algorithm

X sends Y, A, and Y sends X, B. Note Z now has 4 numbers, A, B, g and n but not a or b. Finally, X takes Y's B and performs B^a mod n. Similarly, Y takes X's A and performs A^b mod n. This results in the same number i.e. B^a mod n = A^b mod n. They now have a shared number. Fig. 3 shows the working principle of Diffie – Hellman Algorithm

The advantage of Diffie-Hellman algorithm are the sender and receiver have no prior knowledge of each other, communication can take place through an insecure channel and sharing of secret key is safe. Some of its disadvantages are it cannot be used for asymmetric key exchange, cannot be used for signing digital signatures and the nature of the Diffie-Hellman key exchange does make it susceptible to man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange.

C. Elgamal Cryptographic System

ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. ElGamal cryptographic system, called Elliptic Curve Variant, is based on the Discrete Logarithm Problem [7]. It derives the strength from the assumption that the discrete logarithms cannot be found in practical time frame for a given number, while the inverse operation of the power can be computed efficiently. The ElGamal Algorithm provides an alternative to the RSA for public key encryption.

1) Generating the ElGamal public key:

Here, two parties X and Y have a (publicly known) prime number p and a generator g. X chooses a random number a and computes $A = g^a$. Y does the same and computes $B = g^b$. X's public key is A and her private key is a. Similarly, Y's public key is B and his private key is b.

2) Encrypting and decrypting messages:

If X now wants to send a message m to Y, he randomly picks a number k which is smaller than p. He then computes:

$$c_1 = g^k \bmod p$$
$$c_2 = A^k * m \bmod p$$

and sends c_1 and c_2 to X. X can use this to reconstruct the message m by computing

$$c_1^{-a} * c_2 \bmod p = m$$

Because

c1-a * c2 mod p = (gk)-a * Ak * m
= g-a * k * Ak * m
= (ga)-k * Ak * m
= A-k * Ak * m
= 1 * m
= m

Security of the RSA depends on the difficulty of factoring large integers. Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

3) ElGamal Encryption:

Domain parameters (p, q, g); recipient's public key B; encoded message m in range $0 < m < p - 1$.

1) Choose a random k in the range $1 < k < p - 1$.
2) Compute $c_1 = g^k \bmod p$
3) Compute $c_2 = mB^k \bmod p$
4) Return ciphertext (c_1, c_2).

4) ElGamal Decryption:

Domain parameters (p, q, g); recipient's private key b; ciphertext (c_1, c_2)

1) Compute $m = c_1^{p-b-1} c_2 \bmod p$
2) Return m.

5) Some of its advantages are,

1) One of the strength of ElGamal is its non-determinism-encrypting the same plaintext multiple times will result in different ciphertexts, since a random k is chosen each time.
2) ElGamal encryption is used in the free GNU privacy Guard Software, recent versions of PGP, and other cryptosystems. Its main disadvantages are it needs for randomness, and its slower speed. Its ciphertext is twice as long as the plaintext.

Another disadvantage of the ElGamal system is that the encrypted message becomes very big, about twice the size of the original message m. For this reason it is only used for small messages such as secret keys [8].

IV. PERFORMANCE STUDY

As a part of this study, we implement all the three cryptographic algorithms by means of our web based transactions. The implementation screenshot of RSA, Diffie – Hellman and Elgamal cryptographic algorithms are given in figure 4, 5 and 6 respectively.

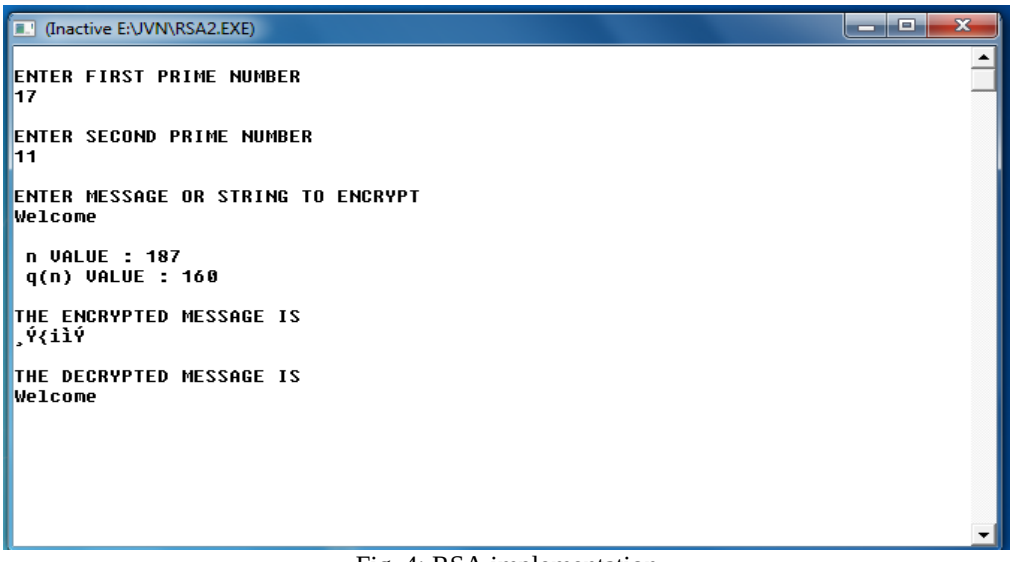

Fig. 4: RSA implementation

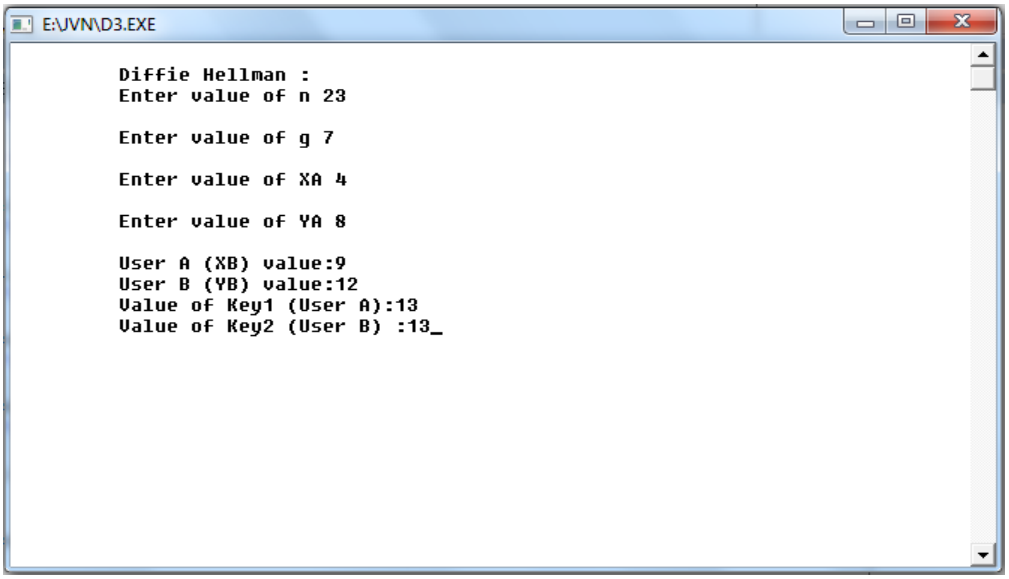

Fig. 5: Diffie – Hellman implementation

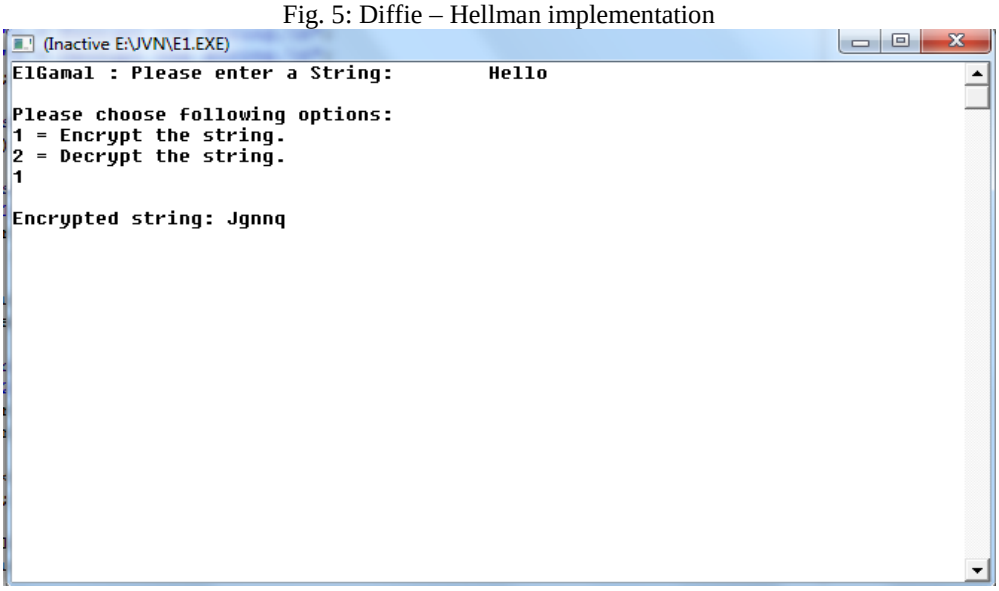

Fig. 6a: Elgamal Encryption

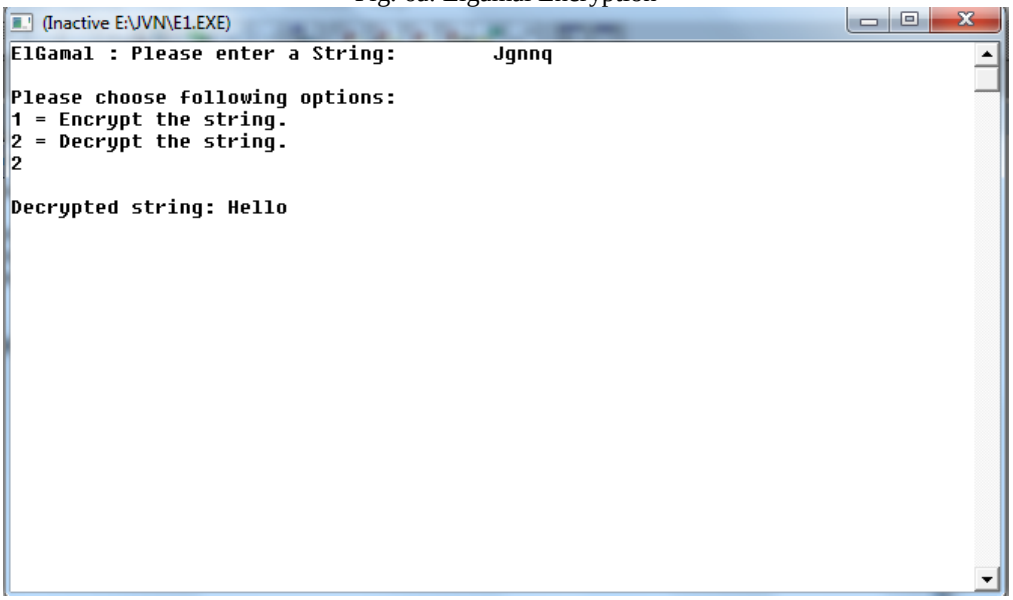

Fig. 6b: Elgamal Decryption

A. Some of the observations from the assessment are

1) The encryption and decryption time of the RSA algorithm is better than the Diffie – Hellman and ElGamal algorithm.

2) Ciphertext RSA has fewer numbers than ElGamal and Diffie – Hellman algorithm.
3) RSA algorithm is faster than other two algorithms.
4) Regarding security, the ElGamal algorithm will be more challenging to solve than the RSA algorithm because ElGamal has a complicated calculation to solve discrete logarithms.
5) Elgamal is better than other two algorithms when the rate of data decryption is considered

B. Applications for Public-Key Cryptosystems

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

V. CONCLUSION & DISCUSSION

Data security is an essential component of an organization in order to keep the information safe from various competitors. Cryptography ensures that the transferred messages are confidentially transmitted. Three cryptographic algorithms are studied and analyzed. Every algorithm has its own strength and weakness and therefore based on the nature of the application, the algorithm can be selected.

REFERENCES

[1] Omar G. Abood, Shawkat K. Guirgui, "A Survey on Cryptography Algorithms", International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018.
[2] Adam J. Elbirt, "Understanding and Applying Cryptography and Data Security", Auerbach Publications, Taylor and Francis Group, 2008.
[3] https://www.cryptomathic.com/news-events/ blog/securing-web-applications-with-cryptographic -zones
[4] Joseph Selvanayagam, Akash Singh, Joans Michael, Jaya Jeswani, "Secure File Storage on Cloud Using Cryptography", International Research Journal of Engineering and Technology (IRJET), 2018.
[5] D. Maheswari, A. Kaushika, A. Jenifer, "A Study on Data Encryption and Decryption Using Hill Cipher Algorithm", International Journal Of Technical Innovation in Modern Engineering & Science (IJTIMES), March - 2018.
[6] Cryptography and Network Security: Principles and Practice, Pearson Publishers, Sixth Edition.
[7] Vikasagarwal, Shruti Agarwal, Rajesh Deshmukh, "Analysis and review of encryption and decryption for secure communication", IJSER, February 2014.
[8] Apoorva, Y. K, "Comparative Study of Different Symmetric Key Cryptography Algorithms", International Journal of Application or Innovation in Engineering and Management, 2013
[9] S. Garg and M. K. Rana, "A Review on RSA Encryption Algorithm," Int. J. Eng. Comput. Sci., vol. 5, no. 7, pp. 17148–17151, 2016.
[10] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. J. Hinek, "Dual RSA and Its Security Analysis," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2922–2933, Aug. 2007.