Hybrid Encryption Algorithm

Gaurav R. Patel, Prof. Krunal Panchal
PG Scholar, Assistant professor
LJIET, Ahmedabad
gauravpatel9092@gmail.com

Abstract - Cryptography is derived from a Greek word which means, the art of protecting information by transforming it into an unreadable format. In order to prevent some unwanted users or people to get access to the data cryptography is needed. This paper introduces hybrid approaches by combining two most important algorithms RSA algorithm and Diffie Hellman algorithm. This hybrid encryption algorithm provides more security as compare to RSA algorithm. The implementation and result is also derived in the paper.

Key Terms - RSA, Diffie-Hellman, Cryptography, Cryptosystem, private-key, public-key

I. INTRODUCTION

Cryptography is a technique to hide the data over communication channel. It is an art to hide the data to strangers. As the technology grows day by day the need of data security over communication channel is increased to high extent. For securing the knowledge cryptography is use.

Symmetric key (also known as secret-key cryptography) uses the only one key for both encryption and decryption. Any message which is encrypted by using the public key can only be decrypted by applying the same public key.
- Use a same key for to encrypt and to decrypt a message.
- Encryption and decryption algorithm is Different

Asymmetric key (also known as public key encryption) uses two different keys to encryption and decryption of the message. The public key is made publicly available and can be used to encrypt messages. The private key is kept secret and can be used to decrypt received messages. RSA is asymmetric key encryption algorithm.
- Use a (public key) to encrypt a message.
- Another (private key) to decrypt a message.

II. RSA ALGORITHM

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs. RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It involves three steps: [2]

1. Key Generation,
2. Encryption And,
3. Decryption.

Phase 1: Key Generation

RSA involves two keys public key and private key. For encryption we use Public key and for decryption we use private key of message. The key generation takes places as follows [2];
(a) Choose two distinct prime numbers P and Q
(b) Find N such that N= P*Q.
(c) Find the Phi of N, \( \phi(N) = (P-1)*(Q-1) \).
(d) Choose an E such that 1 < E < \( \phi(N) \) and such that E and \( \phi(N) \) share no Divisors other than 1 [E and \( \phi(N) \) are relatively prime]. E is kept as the public key exponent.
(e) Determine D which satisfies the congruence relation.
\[ E*D = 1 \pmod{\phi(N)} \]
Now, the public key consists of public key exponent E and N. And private key consists of private key exponent D & N.

Public Key: (E, N)
Private Key: (D, N)

Phase 2: Encryption

A process of converting Plain Text into Cipher Text is known as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure environment. The process of encryption requires two things - a key and an encryption algorithm. Encryption takes place at the sender side.

\[ C = M^E \pmod{N} \]

Phase 3: Decryption

The process of converting Cipher Text into Plain Text is known as Decryption. Cryptography uses the decryption technique at the receiver side to convert the Cipher Text into original message. The process of decryption requires two things - a key and a decryption algorithm and a key.

\[ M = C^D \pmod{N} \]

III. DIFFIE HELLMAN ALGORITHM

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. [7] Diffie–Hellman key exchange (D–H) is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. 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 communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. [13]

Diffie–Hellman is used by several protocols, including Secure Sockets Layer, Secure Shell, and Internet Protocol Security. Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network. Steps of this algorithm are as:

[1] Select two numbers ‘R’ and ‘G’. ‘R’ is a prime number and ‘G’ is called as base.
[2] Select a secret number ‘A’ and another secret number ‘B’
[3] Calculate public number X = G^A mod R,
   And Y = G^B mod R.
[5] Computes First session key as KA,
   \[ KA = Y^A \pmod{R} \]
[6] Computes second session key as KB,
   \[ KB = X^B \pmod{R} \]
[7] Here KA = KB = K.

IV. PROPOSED HYBRID ALGORITHM

RSA and Diffie Hellman key exchange algorithm is widely used in now days. RSA algorithm is used for providing security of message using encryption and decryption process. The Diffie Hellman algorithm is used to generate the Secret key for the sender and receiver for communication. RSA algorithm provides more security as compared to other algorithm.

In this proposed model we add one more operation which is bitwise XOR operation. Because of this operation we can increase the complexity of the message. This operation is performed after the message is converted in to cipher text. In this proposed approach first we choose two prime numbers and find out the Encryption and decryption key exponents which will be used for encryption and decryption process. For Diffie Hellman algorithm we select A and B. R is a random prime number generated by the system automatically. The public number is generated by the Diffie Hellman algorithm. By using this public number we can generate secret key KA and KB. This will be used to perform XOR operation.

At the sender side the encryption is done using encryption algorithm. When the encryption process completes XOR operation perform between cipher text and the first secret key. After that operation the secret message is sent over the medium.

At the receiver side the XOR operation is again performed between the second secret key and the secret message which is sent by the sender. Using this operation we get the original cipher text. We can decrypt the cipher text using decryption algorithm and get the original message sent by the sender.
In proposed model we take A and B as a random numbers. P, Q and R are prime numbers. G is integer number which is primitive root of R. C1 is cipher text and S1 is secret message. K1 and K2 is key generated by Diffie Hellman algorithm. E and D are encryption exponents and decryption exponents.

Following steps are performed by new proposed algorithm:

Step1: Choose two large prime numbers P and Q and random number A, B and G, R.
Step2: Set A and B for Diffie Hellman key generation
Step3: R and G are automatic generated constants.
Step4: Calculate N= P * Q.
Step5: Find \( \Phi(N) = (P-1)*(Q-1) \)
Step6: Choose integer \( E \), which can satisfy \( \text{GCD}[E, \Phi(N)] = 1 \).
Step7: Calculate \( D \), where \( E*D = 1 \mod \Phi(N) \).
Step8: Now calculate following as public number
\( X= G^A \mod R \), \( Y= G^B \mod R \)
Step9: Secret key \( K_1 = Y^A \mod R \), \( K_2 = X^B \mod R \).
Step10: Encrypt message using RSA algorithm,
\( C_1 = (M^E) \mod N \).
Step11: X-OR between C1 and key K1,
\( S = C_1 \oplus K_1 \)
Step12: At receiver side X-OR is between S and
Key K2, \( C_1 = S \oplus K_2 \).
Step13: Decrypt message using RSA algorithm
\( M= (C_1^D) \mod N \).

Example:

Let us consider that, we have to send a message whose value is 88 i.e. \( m=88 \).

Step1: Choose P=11 and Q=17 and
Random number A=5, B=6 and
G=2, R=997.
Step2: \( N = 11 \times 17 = 187 \)
Step3: \( \Phi(N) = (11-1) (17-1) = 160 \)
Step4: Now calculate following as public number
\( X= 2^5 \mod 997 \), \( Y= 2^6 \mod 997 \)
Step5: \( K_1 = 64^5 \mod 997 = 740 \)
\( K_2 = 32^6 \mod 997 = 740 \)
Step6: Choose integer \( E, E=7 \)
Step7: \( 7^D = 1 \mod \Phi(N) \). \( D = 23 \)
Step 8: Encryption
\[ C_1 = (88^7) \mod 187 = 11 \]
Step 9: XOR between \( C_1 \) and key \( k_1 \)
\[ S = C_1 \oplus K_1 = 11 \oplus 740 = 751 \]
Step 10: At receiver side \( C_1 = S \oplus K_2 \)
\[ C_1 = 740 \oplus 751 = 11 \]
Step 11: Decryption
\[ M = (11^{23}) \mod 187 = 88 \]

V. IMPLEMENTATION

NET Framework (Known as dot net), a software framework which is developed by Microsoft that runs primarily on Microsoft Windows. It provides language interoperability across several programming languages. .NET Framework includes a large library.

.NET Framework's Framework Class Library provides user interface, data-access, database connectivity, cryptography, web-application development, numeric algorithms, and network communications. Programmers produce software by combining their own source with .NET Framework and other libraries. .NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces an integrated development environment largely for .NET software called Visual Studio. [12]

The GUI was developed using Microsoft asp.net framework. The programming language is c#. It provide option to choose user define prime number and the also user can input the message which is sent from sender to receiver.

![GUI View of proposed model](image-url)
VI. RESULT

Table 1 and table 2 shows the encryption time and decryption time for the standard RSA algorithm and proposed model.

<table>
<thead>
<tr>
<th>Standard RSA model</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Q</td>
<td>E</td>
<td>D</td>
<td>E [MS]</td>
</tr>
<tr>
<td>11</td>
<td>17</td>
<td>7</td>
<td>23</td>
<td>0.0036</td>
</tr>
<tr>
<td>401</td>
<td>277</td>
<td>7</td>
<td>31543</td>
<td>0.0040</td>
</tr>
<tr>
<td>1447</td>
<td>941</td>
<td>7</td>
<td>1165063</td>
<td>0.0044</td>
</tr>
<tr>
<td>5693</td>
<td>5791</td>
<td>7</td>
<td>28248583</td>
<td>0.0044</td>
</tr>
<tr>
<td>6917</td>
<td>6997</td>
<td>5</td>
<td>38707469</td>
<td>0.0052</td>
</tr>
<tr>
<td>23899</td>
<td>23909</td>
<td>5</td>
<td>114270677</td>
<td>0.0044</td>
</tr>
<tr>
<td>36037</td>
<td>36017</td>
<td>5</td>
<td>103829806</td>
<td>0.0056</td>
</tr>
<tr>
<td>215981</td>
<td>215983</td>
<td>7</td>
<td>39983822023</td>
<td>0.0093</td>
</tr>
<tr>
<td>317263</td>
<td>317267</td>
<td>5</td>
<td>40262578277</td>
<td>0.0105</td>
</tr>
<tr>
<td>532093</td>
<td>532099</td>
<td>5</td>
<td>226500071213</td>
<td>0.0105</td>
</tr>
</tbody>
</table>

Table 1: encryption and decryption time for RSA

<table>
<thead>
<tr>
<th>Proposed model</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Q</td>
<td>E</td>
<td>D</td>
<td>E [MS]</td>
</tr>
<tr>
<td>11</td>
<td>17</td>
<td>7</td>
<td>23</td>
<td>0.0060</td>
</tr>
<tr>
<td>401</td>
<td>277</td>
<td>7</td>
<td>31543</td>
<td>0.0068</td>
</tr>
<tr>
<td>1447</td>
<td>941</td>
<td>7</td>
<td>1165063</td>
<td>0.0068</td>
</tr>
<tr>
<td>5693</td>
<td>5791</td>
<td>7</td>
<td>28248583</td>
<td>0.0064</td>
</tr>
<tr>
<td>6917</td>
<td>6997</td>
<td>5</td>
<td>38707469</td>
<td>0.0068</td>
</tr>
<tr>
<td>23899</td>
<td>23909</td>
<td>5</td>
<td>114270677</td>
<td>0.0081</td>
</tr>
<tr>
<td>36037</td>
<td>36017</td>
<td>5</td>
<td>103829806</td>
<td>0.0085</td>
</tr>
<tr>
<td>215981</td>
<td>215983</td>
<td>7</td>
<td>39983822023</td>
<td>0.0101</td>
</tr>
<tr>
<td>317263</td>
<td>317267</td>
<td>5</td>
<td>40262578277</td>
<td>0.0105</td>
</tr>
<tr>
<td>532093</td>
<td>532099</td>
<td>5</td>
<td>226500071213</td>
<td>0.0117</td>
</tr>
</tbody>
</table>

Table 2: encryption and decryption time for proposed model
The graph shows the encryption time and decryption time comparison for the standard RSA model and proposed model.

<table>
<thead>
<tr>
<th>Average time</th>
<th>Standard Model</th>
<th>Proposed model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption time</td>
<td>0.0062</td>
<td>0.0081</td>
</tr>
<tr>
<td>Decryption time</td>
<td>0.0172</td>
<td>0.0186</td>
</tr>
<tr>
<td>Total time</td>
<td>0.0234</td>
<td>0.0267</td>
</tr>
</tbody>
</table>

Table 3: Time comparison

Table 3 shows the average time of encryption and decryption process for reading which is shown in table 1 and table 2. It also calculated the total execution time for the standard RSA algorithm and proposed model.

The graph shows comparison of total time between standard RSA model and new proposed model. When comparing with RSA, proposed model requires more time for encryption and decryption. Whereas proposed model is more secured cryptography algorithm than RSA, because proposed model includes X-or concept, which is more difficult for the intruder to find the plain text from the secret message.
VII. CONCLUSION

In the proposed hybrid encryption algorithm, we can improve the security of the message by combining encryption and bitwise XOR operation because of this operation, the complexity of the message is also increased. The new proposed model provides more security compared to the normal RSA algorithm.

REFERENCES