WWJMRD 2017; 3(11): 28-30
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Jyotirmoy Das
Research Scholar, Dept. of Computer Science & Engineering, Assam Down Town University, India

Sangeeta Kakoty
Associate Professor, Dept. of Computer Science & Engineering, Assam Down Town University, India

Majidul Ahmed
Assistant Professor, Dept. of Information Technology, Gauhati Commerce College, India

Correspondence:
Jyotirmoy Das
Research Scholar, Dept. of Computer Science & Engineering, Assam Down Town University, India

A Modified Public Key Encryption Technique using Masked Keys

Jyotirmoy Das, Sangeeta Kakoty, Majidul Ahmed

Abstract
The area of Information Security plays an important role in protecting the confidentiality of electronic data. Cryptography is a field of Information Security where a sender's message gets encrypted and the message gets decrypted at the receiver's end. This paper critically analyses the Diffie Hellman Key Exchange protocol and the RSA algorithm, the two most popular techniques that are part of Public Key Cryptography. In this paper, we also introduce an approach to combine the Diffie Hellman Key Exchange protocol and RSA to build a more efficient cryptographic scheme where the public key will be masked in order to provide an extra layer of security.

Keywords: Information Security, Cryptography, Public key, Diffie Hellman, RSA

Introduction

Network security has become an important issue in recent times and Cryptography has been playing an important role in information security system. Many techniques are needed to protect the electronic data. At first the data which is to be transmitted from a sender to a receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using some decryption technique the receiver can view the original data. Many cryptographic algorithms are widely available and used in the field of information security. These algorithms can be categorized into Symmetric or Private Key algorithm and Asymmetric or Public key algorithm. In this paper we keep our focus on Asymmetric or Public Key Cryptography which is has the ability to provide better security than Symmetric or Private Key Cryptography. This paper mainly focuses on the two most remarkable achievements of modern cryptography namely, the Diffie Hellman Key Exchange Protocol and the RSA Algorithm which are a part of Public Key Cryptography.

Public Key Cryptography

Until the mid-1970s, cryptography was exclusively based on private key algorithms where a single key was used for both encryption and decryption process. Both the parties must agree on the secret key before the actual exchange of data takes place. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. The idea of public key cryptography was first presented by Martin Hellman, Ralph Merkle, and Whitfield Diffie at Stanford University in 1976. Public-key cryptography, also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and other one is public [1]. No other key can decrypt the message, not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else.

Diffie Hellman Key Exchange

Diffie Hellman allows two users to exchange a symmetric secret key through an insecure wired or wireless [7, 8] channel and without any prior secrets [6]. It is an amazing and ubiquitous algorithm found in many secure connectivity protocols on the Internet [2, 5]. The Diffie-Hellman algorithm itself does not encrypt data, but it generates a secret key which is common to both the sender and the recipient. Through mathematically linked processes the two parties can independently generate the same secret key and then use it to build a session key for use in asymmetric algorithm [3]. The first appearance of Diffie Hellman was in 1976 [4]. Steps of this algorithm are as follows:

1. Take two numbers “p” and “g”, “p” is a large prime number and “g” is called the generator.
2. User 1 chooses a secret random number “a” and computes U1 = g^a mod p
3. User 2 chooses a secret random number “b” and computes U2 = g^b mod p
4. User 1 and User2 exchanges their respective public numbers U1 and U2 with each other.
5. User 1 computes the secret key with K1= $U1^a$ mod p and User 2 computes the secret key with K2= $U2^b$ mod p.
8. By the laws of algebra, K1 = K2 = K, thus both users having a shared key K.

The RSA Algorithm

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, ie on the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. It is still widely used in electronic commerce protocols, and is believed security depends on the difficulty of decomposition of large numbers [9].

Following are the steps involved in RSA algorithm:

Step 1. Choose two random prime integers *p* and *q where* p should not be same as q.

Step 2. Calculate the product $n = p*q$ and phi (n)=(p-1)*(q-1)

Step 3. Choose random e; 0 <e< phi (n), with gcd(e, phi(n)) = 1.

Step 4. Compute the inverse, d =e^{-1} mod phi (n)

Step 5. The encryption function is $E(m) = m^e$ mod *n*, or any message *m*.

Step 6. The decryption function is $D(c) = c^d$ mod *n*, for any cipher text *c*.

Step 7. The public key is the pair of integers (*n*, *e*).

Step 8. The private key is the triple of integers (*p*, *q*, *d*).

Limitations of the RSA Algorithm

Some of the limitations in the RSA algorithm are:

(a) The factors of public key “n” can be found out by hit and trial due to which the security quotient of RSA algorithm gets reduced. [4]

(b) Since the public key pair is available to all, using the key pair (n,e) anyone can try to encrypt some plaintext and generate some encrypted texts and try to check if the generated encrypted texts matches to some other encrypted texts, which could lead to problems.

Proposed Model

The RSA algorithm on its own is a very well defined public key algorithm but there are some limitations on which the attackers can get their hands dirty and one of the limitations being the exposure of the public key pair (n,e) which if guessed correctly could lead to serious damage in the implementation of the whole cryptosystem. Hence in this paper, a new model has been proposed for the security of public key cryptosystem which combines the Diffie-Hellman Key Exchange algorithm and RSA algorithm. The shared secret key between two parties generated using Diffie Hellman protocol will be used to mask the public key pair (n,e) that is generated during the key generation phase in RSA. This approach won’t be prone to mathematical factorization attack like RSA. The working process of the proposed scheme is given here:

Step 1: Implement Diffie Hellman Key Exchange protocol and obtain a shared secret key K.

Step 2: Implement RSA algorithm to generate the public key pair (n,e) and private key (p,q,d).

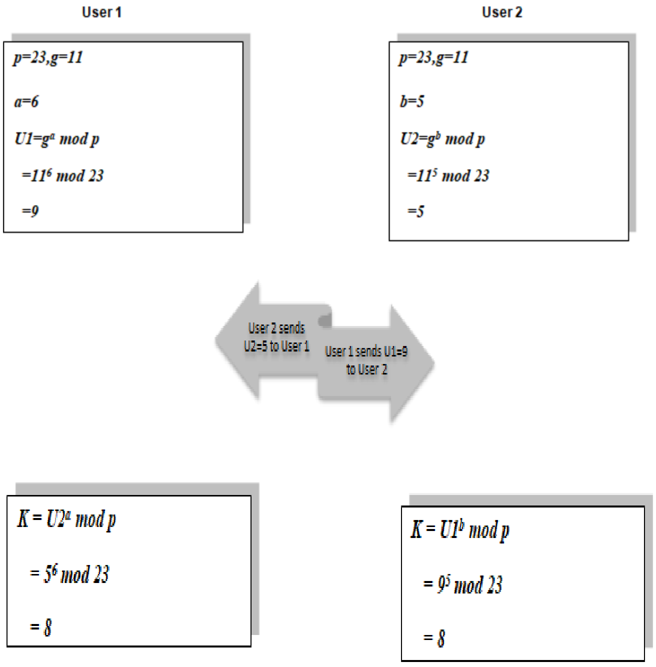
Step 3: Mask the public key pair using the shared secret key K between two users.

Step 4: Unmask the masked public key pair at the other end using the shared secret key K to encrypt the plaintext message.

Step 5: Decrypt the encrypted plaintext message to obtain the plaintext message.

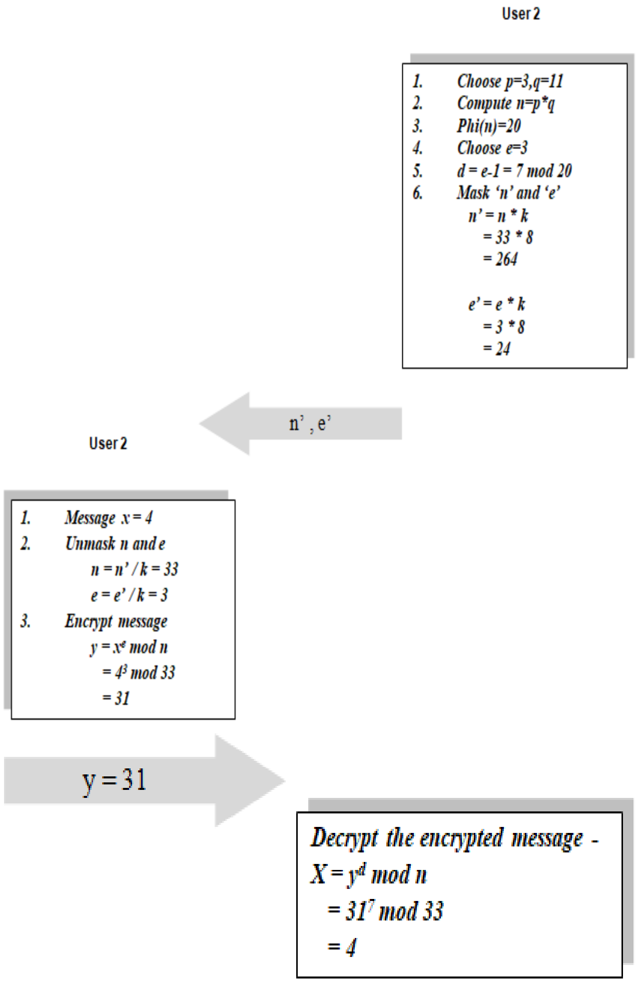
Following is the explanation of the proposed algorithm. We are explaining the above steps with the help of a small example and trying to prove the double security on public key through this.

First implement the Diffie Hellman Key Exchange algorithm to get the shared secret key.



Therefore, the shared secret key K=8

Now let us implement the RSA and mask the public key,



Thus, the encryption and decryption process works successfully using our proposed scheme.

Conclusion

The proposed approach is likely to provide more security than the normal RSA algorithm as the public key pair (n,e) is masked using the shared secret key obtained from Diffie Hellman Key Exchange protocol. Since the public key is masked, hence it becomes more difficult for intruders to get into the system hence providing more security to the overall cryptosystem.

Acknowledgement

The first author acknowledges the academic support given by Assam down Town University (AdtU), Guwahati, Assam.

References

1. Arya, P.K., Aswal, M.S., Kumar, V., “Comparative Study of Asymmetric Key Cryptographic Algorithms”, International Journal of Computer Science & Communication Networks,Vol 5(1),17-21
2. Bhattacharya, P., Debbabi, M. Otrok, H., “Improving the Diffie-Heliman Secure Key Exchange”, 2005 International Conference on Wireless Networks, Communications and Mobile Computing
3. Carts, D., “A Review of the Diffie Hellman Algorithm and its Use in Secure Internet Protocols”, SANS Institute, 2001.
4. Chabra, A., Mathur. S., “Modified RSA Algorithm a secured approach”, International Conference on Computational Intelligence and Communication Systems, 2011
5. Diffie, W., Hellman, M.E., “New Directions in Cryptography”. IEEE Transaction on information theory, IT-22, pp. 472-492, 1978.
6. Garg, V., Rishu, “Improved Diffie-Hellman Algorithm for Network Security Enhancement”, International Journal Computer Technology & Applications, Vol 3 (4), 1327-1331
7. Internet Engineering Task Force (IETF) Working Group. Diffie-Hellman Key Agreement Method, RFC 2631, June 1999.
8. Otrok, H., Mourad, A., Debbabi, M., Assi, C., “Improving the Security of SNMP in Wireless Networks, to appear in the proceedings of Wireless-Com 2005.
9. Song, R., Korba, L., “Security Communication Architecture for Mobile Agents and E-commerce”, National Research Council Canada, 2003.
10. Zhou, X., Tang, X., “Research and Implementation of RSA Algorithm for Encryption and Decryption”, 2011 the 6th International Forum on Strategic Technology. DOI: 10.1109/IFOST.2011.6021216