International Journal of Innovative Research in Engineering & Management (IJIREM)

ISSN: 2350-0557, Volume-3, Issue-2, March-2016

Dynamic Multi-Key Choice Symmetric Key Exchange Algorithm for Secured Transaction

Mr. Anil Hingmire
Department of Computer Engineering, Mumbai University, Mumbai, India

Mr. Sundal Jain
Department of Computer Engineering, Mumbai University, Mumbai, India

Ms. Aakanksha Choudhary
Department of Computer Engineering, Mumbai University, Mumbai, India

Mr. Pritam Hazra
Department of Computer Engineering, Mumbai University, Mumbai, India

ABSTRACT

With the ease that the Internet provides, now, it also, demands a higher security and a need of assurance that the confidential data remains intact till it reaches the other end. To fulfill this necessity, many algorithms and systems showed up-each with its own promises and drawbacks but they couldn't withstand attacks like Brute Force and many others which were specially synthesized to crack these algorithms and fail such systems. In this paper, a new system, which ensures a secure transaction for all the scenarios, is discussed. The algorithm deals with keys which can be used for the future transactions and will be ensuring of secure transactions that the cryptanalyst won't crack.

Keywords

Cryptography, Cryptographic algorithms, Symmetric Key, Cryptanalyst, Encryption, Decryption, Plain text, Cipher text, Keyless Encryption, Keyed Encryption, Public key, Private key

1. INTRODUCTION

Cryptography is the way to transform a meaningful message into a form which seems to have no meaning but can be converted back to the meaningful message only by following a specific procedure. Thus the message can be safely send to the destined person without letting others know about the information contained in the message. The procedure i.e. the algorithm is called as the cipher and the plain message is called as the Plain Text, whereas the converted, non-understandable message is known as Cipher Text.

Presenting messages in a secret way isn't a new concept. A famous example of cryptography is the Scytale transposition cipher, used by the Spartan military, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The message was first written on the wound parchment and the unwounded one was sent. The recipient used a rod of the same diameter on which the parchment is wrapped to read the message. This ensured that the process was fast and not prone to mistakes. However the parchment could be burnt or broken. Also, a same diameter rod was mandatory [1].

Plaintext 'ATTACKTHECASTLEBEFOREDAWN' will be written as

A	T	T	A	C	
K	T	H	E	C	
	A	S	T	L	E
	B	E	F	O	R
	E	D	A	W	N

and the non-understandable message will be represented as 'AKABETTSEDTHTFAAELOWCCERN', known as the cipher text.

Thus, cryptography is an art of converting and understandable piece of data into a non-understandable one, which will be carried to the receiver and the receiver will convert it back to the understandable format. The process of converting from understandable to non-understandable form is called as 'Encryption', whereas the reverse process is called as 'Decryption'.

In the above mentioned case, encryption took place without the help of a key, hence 'keyless encryption'. If a key is used while encrypting then it is known as 'keyed encryption'. Keyed encryption is further divided into Symmetric and Asymmetric key cryptography [2].

2. SYMMETRIC AND ASYMMETRIC KEY CRYPTOSYSTEMS

Asymmetric key cryptography, also known as public key cryptography, consists of a pair of public and private keys which are used to encrypt and decrypt message. The user initially receives a public and private key pair from a central authority. Any other user who wants to send the person a message will have to ask for a public key from the public directory. Sender, then, encrypts the message using the public key whereas the receiver will decrypt the message using the private key. And thus, no one will have access to the receiver's private key except for the receiver himself.

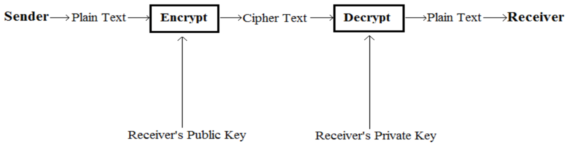

Figure 1: Symmetric key cryptosystem

Copyright © 2016. Innovative Research Publications. All Rights Reserved

Symmetric key cryptography, also known as Secret key cryptography, consists of a single key (Secret key) is used for encryption and decryption. There are various different algorithms present in symmetric key cryptography like DES, Triple DES, Blowfish, IDEA, TEA, CAST-128 and AES (Rijndael).

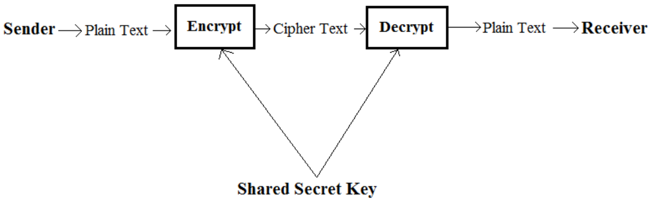

Figure 2: Asymmetric key cryptosystem

3. SECURE TRANSACTION

Today, many credit transactions take place online. Thus one needs to be ensured that his/her money has reached safely at the intended end. This requires a secured transactions system. Thus a secure transaction system makes sure that the data or money has been transferred from one end to another safely without being manipulated in the middle. This implies that a secure transaction system must, widely, use proper encryption decryption algorithms with no loopholes in them. Thus, a secure transaction system must follow all the security goes like confidentiality, integrity and availability i.e. the CIA triad. Data confidentiality is the ability of the system to protect its information against unintended for unauthorized access. Integrity implies the purity of data which means that the data is exactly is what it was before it was to be sent and that no data manipulations have taken place. Availability implies that the resources are available for authorized use even during emergencies and disasters.

4. PROPOSED SYSTEM

When a person wants to send a critical data across the network, the data needs to be encrypted and then sent. But the key that encrypts the data also needs to be shared across the same unsecured network. Thus, it becomes very easy for the hacker monitoring to get his hands over both the keys and the data. And with the help of various softwares available on the Internet, the hacker can easily crack the encryption and fetch the data. What if the key isn't shared when the data is? The hacker will get an encrypted data with no idea how to interpret the haphazard piece of text. This system deals with sharing of keys long before the actual data is exchanged. Following is the procedure followed by the system:

4.1 Algorithm

1. Start.
2. Generate Ki.
3. Connect to the other person.
4. Out of the two ends, at end A, generate Ka.
5. Encrypt Ka by Ki.
6. Send encrypted Ka to B.
7. At end B, generate Kb.
8. Encrypt Kb by Ka.
9. Send encrypted Kb to A.
10. Generate Kx and exchange it using RSA algorithm.

    This will be done previously i.e. long before the actual communication will take place.
11. Sender A will send the encrypted message using either of Ki, Ka, Kb or Kx.
12. Dummy packets will be used to determine the Actual key used by the sender.
13. Decryption by the receiver.
14. Stop.

4.2 Explanation

When the software is installed a key is generated by the software which is Ki. This Key Ki will be same at all the ends where the software is installed. When a person wants to send a message to another person He would request the other person to connect to him. Once the other person has got connected the former person will generate a key Ka. The key Ka will then be encrypted with key ki and send to the receiver. Since the other person also had Key Ki he will decrypt the message and receive the key Ka. Another key Kb will be generated randomly at the receiver's end. This ki Kb will then be encrypted with the help of key Ka and sent to the sender. The sender will decrypt this message and receive key Kb. At this point of time, both the ends will have three keys Ka, Kb and Ki. When the actual message will need to be sent, a key Kx will be generated at both the ends with the help of Diffie Hellman key exchange algorithm. Now while sending the actual message the sender would Encrypt the message using either of these four keys. The receiver after receiving the encrypted message would send two Dummy messages to the sender. If the sender sends back the same to W package The receiver then The receiver will identify the encryption key as Ki. If the sender Sends 1st dummy packet as the same dummy message and a different dummy message as the second dummy message then The sender Would Identify the encrypting key as Ka. If the dummy message sent is not the same but the second one is then the receiver would identify the key as Kb. If either of the messages received by the receiver are not same as what the receiver had sent then the receiver would identify the encrypting key as Kx. Once The receiver identifies the encryption key He would send an acknowledgement to the sender After which the software will change the keys Ka to Ka' and Kb to Kb'.

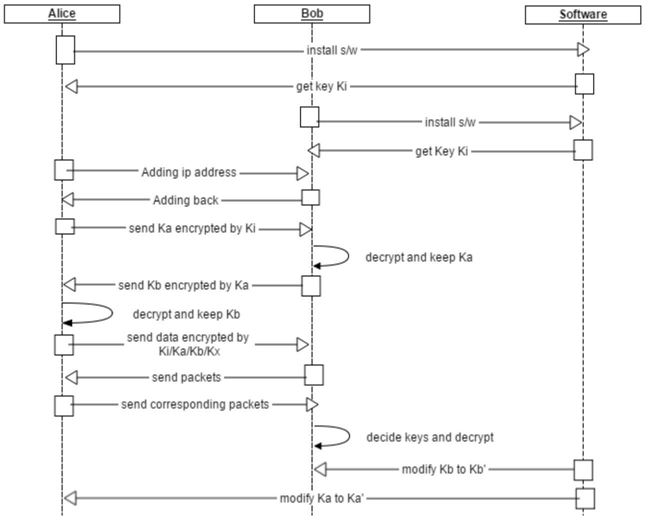

Figure 3: Sequence diagram of the above system

Copyright © 2016. Innovative Research Publications. All Rights Reserved

We have selected RSA algorithm which facilitates Key Generation, Key Distribution, Encryption and Decryption.

4.3 RSA

RSA, an algorithm used for public key encryption, was invented by Rivest, Shamir and Adleman. RSA is widely used for securing confidential and sensitive data which is being sent over any unsecure network. In RSA, either of the public or the private key can encrypt the message and on the receiver side, the other key will decrypt it. Thus, it provides integrity, confidentiality, authenticity and non-reputability of data. Various protocols such as SSH, OpenPGP, S/MIME and SSL/TLS uses RSA for encryption and for digital signature functions. RSA uses 1024 or 2048 bit keys and relies on factoring of large integers but as the technology advances, the computation power increases and more efficient factoring algorithms can be discovered. Thus RSA can become vulnerable in near future [3].

4.4 Key Generation

The key generation in RSA is as follows:

a. Choose two distinct, large prime numbers p and q.
b. Calculate n=p*q
c. Calculate $\varphi(n)=(p-1)*(q-1)$, where φ is the Euler's totient function.
d. Choose an integer e such that $1<e< \varphi(n)$ and $GCD(e, \varphi(n))=1$ i.e. e and $\varphi(n)$ should be coprime. e is the public key exponent.
e. Solve the following for d: $(d*e) \bmod \varphi(n)=1$. d will be the private key exponent.

4.5 Key Distribution

For Bob to send a message to Alice, Alice will transmit her public key (n,e). Private key is never distributed.

4.6 Encryption

If Bob is to send any message M to Alice then, M will be needed to converted into an integer, say m., such that $0 \leq m<n$ and $GCD(m,n)=1$.

The cipher text c will be calculated as

$$c=m^e \bmod n$$

The cipher text c will be sent to Alice.

4.7 Decryption

To recover original message m, Alice will use the private key exponent d using the following:

$$m=c^d \bmod n$$

4.8 Limitations

It is compulsory that the two prime numbers selected at the first place are large enough otherwise it would be easy to factorize n. Also, the two prime numbers should not be close. Otherwise they can be figured out as neighbors of root n. Since the cipher text is the e^{th} power of the integer, the message can be easily recovered by taking e^{th} of the corresponding integer equation. If Alice and Bob have their public keys in the form (e_1,n) and (e_2,n) and if e_1 and e_2 are co-prime then by number theory, there would exist integers a and b such that $ae_1+be_2=1$ so any other person who knows e_1,e_2 will be able to find out a and b. The message could be calculated as $(c_1^a c_2^b) \bmod n$. Lastly, say, e=3 and say, three people have their public keys as (e,n_1), (e,n_2) and (e,n_3) and say same plain is sent to them then if any other person, Jane, intercepts these, she can find out $GCD(n_1,n_2)$, $GCD(n_1,n_3)$ and $GCD(n_2,n_3)$. Any of these results which is greater than 1, will be one of the prime factors and then the other can be found out easily. This is known as Hastad's attack [4].

But these were rare cases that might occur and hence, we use RSA for key generation, key distribution, encryption and decryption, though other algorithms can be used for the same in this system.

5. ADVANTAGES OF THIS SYSTEM

1. The biggest advantage of the system is that generates keys dynamically which means no one can predict the key and this fact makes it more secure.
2. Another advantage is that after every transaction the key is changed so that the cryptanalyst will need to figure it out again before which the current transaction would actually get over.
3. This system makes use of four different keys out of which only one key is used at a time, for one transaction. Also the keys change after the transaction is done which means that even if the cryptanalyst finds out one right key, he has a possibility of 0.25 that he figured out the right key.

6. CONCLUSION

This algorithm is more secured than any other key distribution algorithm as the keys are dynamically generated and it keeps on changing in every transaction. So it is difficult for cryptanalyst to figure out the keys and hence security of the system increases.

REFERENCES

[1] https://en.wikipedia.org/wiki/History_of_cryptography

[2] International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March 2015: A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms, Nivedita Bisht, Sapna Singh.

[3] R. Rivest,A Shamir, L. Aldeman, "A Methoed for Obtaining DigitalSignatures and Public-key Cryptosystems," J. Communications of the ACM, 1978, 21(2): 120-126.

[4] https://dedekindsparadise.wordpress.com/2011/07/24/limitations-of-rsa/