www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21222-21224
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.06

Asymmetric key algorithms-A Proposed Method

MS Tanusree ghorui, Prof. Samir Kumar Bandyopadhyay
Dept. of Computer Sc. & Engineering, University of Calcutta, Kolkata, India

Abstract

Asymmetric key algorithms use different keys for encryption and decryption. The encryption key is public, decryption key is secret. Anyone can encrypt a message but only the one who knows the corresponding private key can decrypt it. This paper discuss asymmetric key algorithms with its advantages and disadvantages.

Keywords : Public, Asymmetric Key, Encryption and Security.

Introduction

There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption). Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

The object of secure communications has been to provide privacy or secrecy, i.e., to hide the contents of a publicly exposed message from unauthorized recipients. In contemporary commercial and diplomatic applications, however, it is frequently of equal or even greater concern that the receiver be able to verify that the message has not been modified during transmission or that it is not a counterfeit from an unauthorized transmitter. In at least one important class of problems message authentication is needed at the same time that the message itself is revealed.

Cryptography is practice and study of techniques for secure communication in the presence of third parties. Cryptography is the practice and study of hiding information. it is the art and science of converting the plain text into cipher text. In cryptographic terminology, the message is called plaintext. Encoding the contents of the message in such a way that its contents cannot be unveiled by outsiders is called encryption. The encrypted message is called the cipher text. The process of retrieving the plaintext from the cipher text is called decryption. There are four main objectives of cryptography:-

1. Confidentiality: It guarantees that the sensitive information can only be accessed by those users/entities authorized to unveil it.
2. Data integrity: It is a service which addresses the unauthorized alteration of data. This property refers to data that has not been changed, destroyed, or lost in a malicious or accidental manner.
3. Authentication: It is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other.
4. Non-repudiation: It is a service which prevents an entity from denying previous commitments or actions.

It is also known as the public key cryptography. There are two types of key first one is public key which is used for encryption and second is private key which is used for decryption. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. The major drawbacks of asymmetric ciphers are their speed and security strength; they are much slower than the symmetric algorithms and more vulnerable to intruder attacks but they make key exchange easier.

Review Works

Diffie-Hellman is the first asymmetric encryption algorithm, It is a widely used key exchange algorithm [1]. Rivest Shamir Adleman (RSA) is the most commonly used asymmetric algorithm. It can be used both for encryption and for digital signatures. RSA can be used for key exchange as well as digital signatures and the encryption of small blocks of data. Today, RSA is primary used to encrypt the session key used for secret key encryption or the message's hash value. ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie-Hellman key exchange [2]. ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie-Hellman key exchange. The Digital Signature Algorithm (DSA) [5]is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Every signatory has a public and private key. In the signature generation process the private key is used and the public key is used in the signature verification process. Elliptic Curve Cryptography (ECC) was introduced by Victor Miller [3] and Neal Kolbitz as an alternative to established public key systems such as RSA [4].

Proposed Method

Generally symmetric cryptography algorithm is divided into two parts ♣ first one is stream cipher where bit by bit encryption performed and ♣ Second is block cipher where encryption performed on block of bits. In our method we do the following:

Here we use three methods in our algorithm. Such as, shifting, xor and transfer.

- Shifting:- The bits or letters of plain text or message are shifted. This shifting depends on the key which is entered by the user. For example, if the entered message is “I am a girl” and the key is “3” then the result is “l dp d jluo”. I is shifted l, a is shifted d and so on.
- XOR:- “ABCDEFGHI123456” is the predefined key. It is xored with the shifted key. For example, “l dp d jluo” is xored with that key and the result is “b’4a”g”%?^”.
- Trasnfer:- The xored message is written downwards and diagonally. Then moving up after reach the bottom. After reach the top, the message is written downwards again until the whole text is written out. The message is then read off in rows. For example, after the transfer operation the encrypted message is “-‘eg%^b4’”””?”.

Algorithm

- Shifting:

```
printf("\n Enter key: ");
  scanf("%d", &key);

  for(i = 0; str[i] != '\0'; ++i){
     ch = str[i];

     if(ch >= 'a' && ch <= 'z'){
        ch = ch + key;

        if(ch > 'z'){
           ch = ch - 'z' + 'a' - 1;
        }

        str[i] = ch;
     }
     else if(ch >= 'A' && ch <= 'Z'){
        ch = ch + key;

        if(ch > 'Z'){
           ch = ch - 'Z' + 'A' - 1;
        }

        str[i] = ch;
     }
  }

  printf("\n Encrypted message: %s", str);
```

- XOR:

```
length = strlen(str);
            for(count=0;count<length;count++)
            {

str[count]=str[count]^my_key[count];
                    printf("\nthe encrypted string is
%s",str);
                    }
```

- Transfer:

```
for(i=0,j=0;i<length;i++)
{
if(i%2==0)
cc[j++]=str[i];
}
for(i=0;i<length;i++)
{
if(i%2==1)
cc[j++]=str[i];
}
cc[j]='\0';
printf("\nCipher text after TRANSFER :");
printf("\n%s",cc);
```

Comparison

The proposed algorithm is compared with RSA algorithm and the following is found as an indication of better in respect of RSA algorithm.

- RSA is considered as a one-way function of converting plaintext into ciphertext where in our algorithm plaintext is converted into ciphertext through 3 procedures. The procedures are (a) Shifting, (b) XOR and (c) Transfer.
- In RSA algorithm, we need two prime numbers and a text but in our algorithm we need a plain text , shared key (public key) which is known to all and a secret key (private key) which is only sender and receiver (whom sender wants to sends the message) knows, not all. If secret key is matched then the receiver (the genuine one) can get the message.
- If either of two functions(encryption function, key generation) are proved non one-way, then RSA will be broken but in our algorithm , this type of problem can not be happened.
- In fact, if a technique for factoring efficiently is developed then RSA will no longer be safe. But our algorithm is not based on factoring.
- Our algorithm is more secure than RSA algorithm**.**

Conclusions

Information is an asset, which like other important business asset values to an organization. And consequently needs to be suitably protected. Information can be created, lost, processed, stored and corrupted. Cryptography plays a very important role in securing data over the network. A new approach for data security using block cipher symmetric key cryptography was proposed. This new approach uses the concept of encryption number and random number from paper to enhance the complexity of key.

References

1.Alese, B. K.Philemon E.D., Falaki, S. O., September 2012 , Comparative Analysis of Public-Key Encryption Schemes, International Journal of Engineering and Technology, Volume 2, No. 9.

2. S. Vijaykumar and S. Saravanakumar, 2011, Future Robotics Memory Management, Advances in Digital Image Processing and Information Technology, pp. 315–325.

3. S. Vijaykumar and S. Saravanakumar, 2011, Future Robotics Database Management System along with Cloud TPS, Intl. Journal on CloudComputing: Services and Architecture (IJCCSA), pp. 103–114.

4. Rashmi Singh, Shiv Kumar, December 2012, ElGamal Algorithm in Cryptography, International Journal of Scientific & Engineering Research, Volume 3, Issue 12.

5. Williams Stallings, 2006, Cryptography and Network Security, Prentice Hall, 4th Edition.