International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 545-548
e-ISSN:2278-621X

STUDY ON SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY ALGORITHM

Ms.Roopa Shenoy[1], Ms.Prathiksha[2] & Ms.Thripthi S Shetty[3]

Abstract- Data is any type of stored digital information. Security is the method of protecting data and information. Data security refers to defensive virtual privateness measures which are implemented to save you unauthorized get right of entry to the computer system, nonpublic database, and websites. Cryptography is one of the important concepts in a computer world. Cryptography basically hides the data and information. Encryption and Decryption are the two terms used in the Cryptography. There are numerous cryptography strategies available and amongst them, AES is one of the most powerful techniques. In this paper, we carried out a study on some of the best algorithm which facilitates to encrypt and decrypt the data.
Keywords – Cryptography, Symmetric, Asymmetric, AES, Blowfish, Diffe-Hellman,RSA

1. INTRODUCTION

In recent years, a lot of applications based on the internet are emerging such as online shopping, stock trading, internet banking and electronic bill payment etc. Such transactions, over a wire or wireless public networks, demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability, and confidentiality, integrity and availability, also known as CIA triad [7].

The NIST Computer Security Handbook [NIST95] defines the term computer security as, "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." Security is the mechanism by which information and services are protected from unintended or unauthorized access, change or destruction. Security in networking is based on Cryptography (a word with Greek origins, means "secret writing"), the science and art of transforming messages to make them secure and immune to attack [8].

Cryptography is an artwork of hiding facts. It hides information in such a way that it can be readable to only intended recipient. It uses two powerful techniques, Encryption and Decryption. Encryption is the approach of converting simple text into the encrypted form. Decryption is the method of transforming encrypted text into plain text.

Symmetric-key algorithms [1] are algorithms for cryptography that use the identical cryptography keys for both encryptions of plain text content and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[2] This requires that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption [3].

Asymmetric cryptography [4], also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys may be used to encrypt a message; the alternative key from the one used to encrypt the message is used for decryption

The rest of the paper is organized as follows. AES, Blow fish, Diffie-Hellman, RSA Algorithms explained in section II. Concluding remarks are given in section III.

2. AES ,BLOWFISH,RSA,DIFFIE-HELLMAN ALGORITHM

2.1 AES Algorithm –

AES is Symmetric key algorithm. It is more secure than the DES algorithm because it uses 3 different keys (128,192,256 bit).Block size of AES is 128 bits.

[1] Master of Computer Application, St. Aloysius Institute of Management and Information Technology (AIMIT), Beeri, Mangalore -575022, Karnataka, India
[2] Master of Computer Application, St. Aloysius Institute of Management and Information Technology (AIMIT), Beeri, Mangalore -575022, Karnataka, India
[3] Master of Computer Application, St. Aloysius Institute of Management and Information Technology (AIMIT), Beeri, Mangalore -575022, Karnataka, India

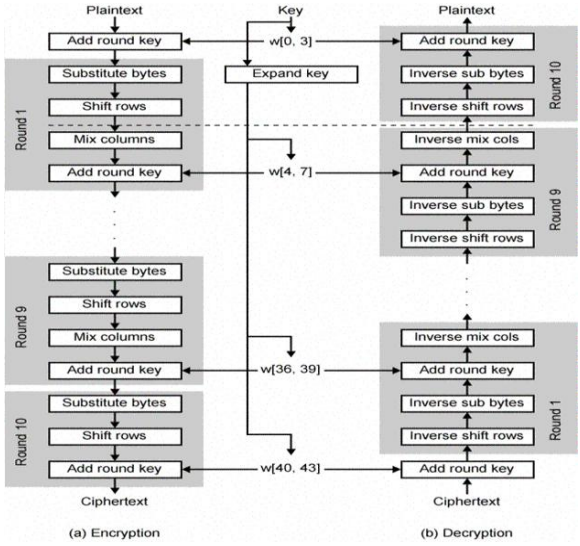

Figure1. AES Encryption and Decryption

AES algorithm starts with an Add round key stage followed by nine rounds of four stages and a tenth round of three stages. Four Stages of AES Algorithm are:

- Substitute bytes : each byte within the state is substituted by another one using S-Box
- Shift rows: each row within the 4x4 array is shifted a certain amount to the left
- Mix Columns: a linear transformation on the columns of the state
- Add Round Key: All the bytes from the state are combined with a round key. Each round contain different and taken from the Rijndael key schedule

The tenth round leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm encompass the following:

- Inverse Shift rows
- Inverse Substitute bytes
- Inverse Add Round Key
- Inverse Mix Columns

2.2 Blowfish Algorithm –

Blowfish algorithm is Symmetric key algorithm which is designed to replace DES algorithm. Blowfish is popular for its tremendous speed and effectiveness. An E-commerce structure uses Blowfish for securing bills to password management equipment, and to protect passwords. Blowfish has a 64-bit block length and a key length of anywhere from 32 bits to 448 bits. It is a 16-round Feistel cipher and it makes use of large key-dependent S-boxes.

It is divided into two parts. 1. Key-expansion 2. Data Encryption

Key-expansion will change a key at most 448 bits into many sub keys arrays totaling 4168 bytes. Blowfish makes use of big variety of sub keys.. Data Encryption is having a function to repeat 16 times of network. Every round consists of key-dependent permutation and a key and data-dependent substitution. All operations are Xor and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for every round.

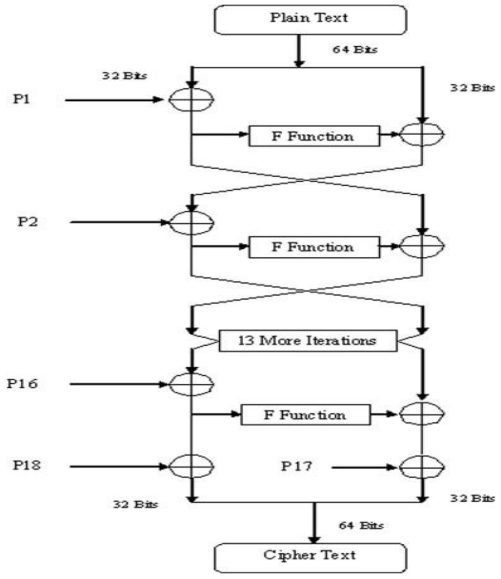

Figure2. Blowfish Key-expansion and data Encryption

2.3 RSA ALGORITHM –

RSA algorithm is used by modern computer to encrypt and decrypt the messages .Because it uses two exclusive key for encryption and decryption it is it is Asymmetric key algorithm. It creates two large product of prime number and uses the arbitrary value as their public key.

RSA Algorithm is divided into three phases:

- Key Generation: Whoever desires to get hold of secret messages creates a public key (that is posted) and a private key (kept secret).The keys are generated such a way that it is 'difficult' to search the private key by solely knowing the public key.
- Encryption: A secret message is encrypted by using public key
- Decryption: Only the intendent receiver will decipher the key secret message using the private key.

RSA Key Generation

- Step 1 : Take two totally different prime numbers: p and q
- Step 2 : Calculate n by using the formula
  n=p.q
- Step 3 : Compute φ (n)
  φ = φ (n)=(p-1).(q-1)
- Step 4 : Choose arbitrary e that is lesser than n and comparatively prime to φ
  1< e < φ (n)
- Step 5 : Compute d
  d=(e.d) mod (φ (n))=1

From these numbers the keys are composed:

- Public key combination is (e, n).
- Private key combination is (d, n).

Most effective the general public key (e, n) is posted; all the different numbers concerned (p,q,φ,d) must be kept private. The main property of this construction is that it is difficult' to work out "d" simply from numbers "e" More precisely:

- It is 'difficult' to calculate d without knowing φ.
- It is 'difficult' to solve n into p.q (which is required for computing φ).

RSA Decryption :

First of all we'd like the private key of the person who got the encrypted message:

Private key is:(d,n)

Next we need the encrypted message: "m' "

Decrypted message m = (m'^{d} mod n)

The message "m" should match with the above chosen letter

2.4 Diffie-Hellman Algorithm –

Diffie-Hellman [5] 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. It is an essential distinction: you're not sharing information at some point of the key exchange; you are growing a key collectively.

This is especially beneficial due to the fact you could use this technique to create an encryption key with a person, after which begin encrypting your traffic with that key. Or even if the traffic is recorded and later analyzed, there may be honestly no way to parent out what the important thing turned into, even though the exchanges that created it could were seen. This is where best ahead secrecy comes from. Nobody analyzing the traffic at a later date can break in because the key become in no way saved, never transmitted, and in no way made seen anywhere.

The manner it really works is reasonably easy. Lots of the mathematics is similar to you see in public key crypto in that a trapdoor feature is used. And at the same time as the discrete logarithm trouble is traditionally used (the xy mod p business), the overall method may be modified to apply elliptic curve cryptography as well.

But even though it makes use of the equal underlying ideas as public key cryptography, this isn't uneven asymmetric cryptography because not anything is ever encrypted or Decrypted during the alternate key exchange. it is, but, an essential building-block, and was in fact the base upon which asymmetric crypto was later constructed. Diffie Algorithm Working:

Step1 : Pick out prime number q
Step 2 : Take primitive root of q
α is primitive root of q
(q and α are public values)
Step 3 : Select private value Xa(Xa should be less than q)
Step 4 : Calculate Ya
$Ya = \alpha^{Xa} \bmod q$
Step 5 : Send the public values(q, α ,Ya) to Receiver
Step 6 : Now Reciever get the pulic values of Sender and repeat te above stes
Step 7 : Select private value Xb(Xa should be less than q)
Step 8 : Calculate Yb
$Yb = \alpha^{Xb} \bmod q$
Step 9 : Send the public value back to(q,α,Yb) to sender
Step 10 : Calculate Ka
$Ka=Yb^{Xa} \bmod q$ (Xa is private value of Sender)
Step 11 : Calculate Kb
$Kb=Ya^{Xa} \bmod q$ (Ya is private value of Receiver)
Sep 12 : If Ka==Kb the connection is establishes else not established

The most serious[6] limitation of Diffie-Hellman in its basic or "pure" form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium. Diffie-Hellman is well suited for use in data communication but is less often used for data stored or archived over long periods of time.

3. CONCLUSION

The usage of internet and network is developing hastily. So there are more requirements to secure the information transmitted over unique services. To provide the security to the network and data specific encryption and decryption method are used. In this paper, we have done the study on the encryption and decryption algorithm such as AES, Blowfish, RSA, and Diffie-Hellman. All the techniques are precise for real time encryption and decryption. Every approach is precise in its own way, which is probably suitable for different application and has its own pro's and con's. According to study, it may be observed that AES algorithm is maximum efficient in terms of speed, time, and throughput and avalanche effect. Security provided by these algorithms may be better in addition, if multiple set of algorithm is applied to data.

In future we will combine the algorithm either sequentially or parallel to provide the more secure environment to protect the data.

4. REFERENCES

[1] https://en.wikipedia.org/wiki/Symmetric-key_algorithm
[2] Delfs, Hans & Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.
[3] Mullen, Gary & Mummert, Carl (2007). Finite fields and applications. American Mathematical Society. p.112.ISBN 9780821844182.
[4] http://searchsecurity.techtarget.com/definition/asymmetric-cryptography
[5] https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english
[6] http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange
[7] Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010.
[8] Behrouz A Forouzan, "Data Communications and Networking", cGraw-Hill, 4th Edition.