Message Delivering on the Network Using Ensemble Data Encryption and Key Exchange Algorithm

Phyu Phyu Khaing
Computer University, Monywa
phyukhaing7@gmail.com

Abstract

Nowadays, people widely use computer networks to communicate from one place to another. Security is needed to protect data from hacker. Cryptography is one of the primary ways to do the job. In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for security, and typically for confidential communications. This paper is implemented by combining Data Encryption Standard and Diffie-Hellman Key Exchange Algorithm (D-H) that will solve to protect a secure key. By using two algorithms, at first, if Diffie-Hellman Key Exchange Algorithm uses to compute, it gets the secret key in this system. And then getting secret key is needed to use again by DES algorithm for encryption and decryption techniques.

Keywords: Diffie-Hellman key exchange, DES, data encryption, block cipher, stream cipher

1. Introduction

Networking operates among of computers to communicate with each other, shares objects, and so on. The objective of networking enhances human-to-human communication without regard to the physical location of resource and the user. More and more computer systems are connected to the net of nets to improve electronic communication, business-to-business applications, E-Commence and information retrievals. The manifold possibilities and conveniences of the connection with the Internet lead to an increasing dependency of being online, not only for commercial activities but also for the private way of life.

The only way to enforce protection in communication channel is by the application of cryptography. The cryptography was used mainly to secure the communication of the powerful and influential. So, Cryptography was used as a tool to protect national secret and strategies.

In general, cryptography is used to protect data while it is being communicated between two stations. In the first case, key must be available at the transmitter and receiver simultaneously during communication. In the second case, key must be maintained for the duration of the storage period.

Modern cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secrets called keys. A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without knowledge of the key. Some algorithms are used for Key Management. So, we describe the implementation of D-H Algorithm using key management.

The rest of the paper is organized as follows. In section 2, we describe the related work. In section 3, we present concept of cryptography. In section 4, we explain the proposed Diffie-Hellman key exchange and DES algorithms. In section 5, we represent the proposed system architecture. In section 6, we give conclusion of our system.

2. Related work

W.Diffie and M.E.Hellman published in 1976 the idea of public key cryptography in their paper and this was considered a breakthrough in the field of secret-key distribution. This has always been a major difficulty, and the prominent way of doing this was, before the public key techniques, physical and cumbersome distribution of the keys. Diffie and Hellman's discovery made it possible to securely exchange encryption keys by a communicating party and insecure communication line. There are no requirements of knowing the other part, nor any transmission of the actual key. The algorithm was named "Diffie-Hellman key exchange" DHK, and is the first practical public key algorithm ever published. [8]

In 1998, Menezes and Wu founded how the discrete logarithm problem in *GL (n, q)* could be reduced in probabilistic polynomial time to the logarithm problem in small extensions of the finite field F_q. It has also been shown that the Index-Calculus method for determining the discrete logarithm in a finite field takes sub exponential time. Thus, the group *GL (n,q)* offers no significant advantage over finite fields whose security is based on the difficulty of computing discrete logarithms in a group. [1]

Author Joshua B. Nelson, B.A explored the Diffie-Hellman key exchange in *GL (n, q)* and in M_n(R). They presented a cryptosystem capitalizing on the notion that Jordan Canonical form is not defined for a matrix over a ring, and thus the group of matrices over a ring $M_n(R)$ offers an advantage over the group *GL (n, q)*. [7]

3. Cryptography

Cryptography is a branch of mathematics based on the transformation of data. It can be applied to protect communication channel. It provides the basis for most computer security mechanisms. Cryptography has a long and fascinating history. It is an effective way of protecting sensitive information.

Encryption is the process of encoding a message in such a way as to hide its contents. Modern cryptography includes several secure algorithms for encrypting and decrypting messages.

There are two main class of encryption. The first uses shared secret keys – the sender and the recipient must share the knowledge of the key and it must not be revealed to anyone else. The second class of encryption algorithms uses public/private key pairs – the sender of a message uses a public key – one that has already been published by the recipient – to encrypt the message. The recipient uses a corresponding private key to decrease the message. Although many principles may examine the public key, only the recipient can decrypt the message, because he has the private key.

A message is encrypted by the sender applying some rule to transform the plaintext message (any sequence of bits) to a cipher text (a different sequence of bits). The recipient must know the inverse rule in order to transforms the cipher text into the original plaintext.

In cryptography, cipher consists of block cipher and stream cipher. The modern block cipher is based on the Festal cipher.

3.1. The emergence of cryptography

Cryptography provides the basis for most computer security mechanisms. Cryptography has a long and fascinating history. The military and for secure communication and the corresponding need of an enemy to intercept and decrypt it led to the investment of much intellectual effort by some of the best mathematical brains of their time. History will find observing reading in books on the topic by David Kahn [1967, 1983, and 1991] and Simon Singh [1999]. Whitfield Diffie, one of the inventors of public-key cryptography, has written with first-hand knowledge on the recent history and politics of cryptography [Diffie 1988, Diffie and Landau 1998] and in the preface to Schneier's book [1996].

The publication of Schneier's book Applied Cryptography [1996]. First edition appeared in 1994. Menezes *et al.* [1997] also provides a good practical handbook with a strong theoretical basis.

3.2. Performance of cryptographic algorithm

The performances of cryptography are the following:

(1) Communicate with a shared secret – key.
(2) Communicate with one another via server by using ticket.
(3) Communicate with public-key that distribute a shared secret key.
(4) Communicate with a secure digest function that have not secret.
(5) Communicate by using certificate.

The final method is the best one that is it has a highest security for transmission messages.

3.3. Secret key cryptography

With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

3.4. Modern block ciphers and the data encryption standard

3.4.1. Block Ciphers. Most encryption algorithms operate on fixed-size blocks of data; 64bits is a popular size of blocks. A message is subdivided into blocks, the last block is padded to the standard length if necessary and each block is encrypted independently. The first block is available for transmission as soon as it has been encrypted.

For a simple block cipher, the value of each block of cipher text does not depend upon the preceding blocks. This constitutes a weakness, since an attacker can recognize repeated patterns and infer their relationship to the plaintext. Nor is the integrity of messages guaranteed unless a checksum or secure digest mechanism is used. Most block cipher algorithms employ Cipher Block Chaining (CBC) to overcome these weaknesses.

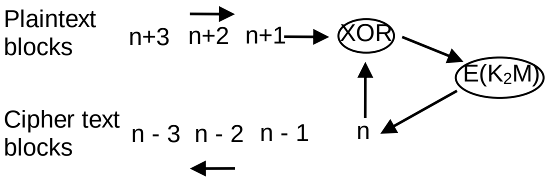

Figure 1. Cipher block chaining

3.4.2. Stream Cipher. For some applications, such as the encryption of telephone conversations, encryption in blocks is inappropriate because the data streams are produced in real time in small chunks. Data samples can be as small as 8 bits or even a single bit, and it would be wasteful to pad each of these to 64 bits before encryption and transmitting them. Stream ciphers are encryption algorithms that can perform encryption incrementally, converting plaintext to cipher text one bit at a time.

This sounds difficult to achieve, but in fact it is very simple to convert a block cipher algorithm for use as a stream cipher. The trick is to construct a key stream generator. A key stream is an arbitrary – length sequence of bits that can be used to obscure the contents of a data stream by XOR-ing the key stream with the data stream. If the key stream is secure, then so is the resulting encrypted data stream.

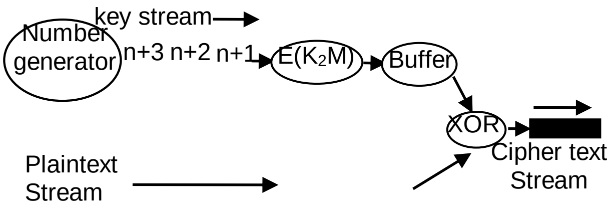

Figure 2. Stream cipher

4. Proposed Diffie-Hellman key exchange and DES algorithms

4.1. Diffie-Hellman key exchange algorithm

Diffie-Hellman Key Exchange algorithm is a cryptographic protocol that allows two parties that have no prior knowledge each other to jointly establish a shared secret key over an insecure communications using a symmetric key cipher.

The Diffie-Hellman (D-H) algorithm is the basis of most modern automatic key exchange methods. The D-H algorithm provides secure key exchange over insecure channels and is frequently used in modern key management to provide keying material for other symmetric algorithms, such as DES, 3DES or AES.

The first published public-key algorithm appeared in the seminal paper by Diffie-Hellman that defined public key cryptography and is generally referred to Diffie-Hellman key exchange. A number of commercial products employ this key exchange technique.

The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values.

4.1.1. Diffie-Hellman key exchange calculation. In order to start a D-H exchange, the two parties must agree on two no secret numbers. The first number is c, the generator, and the second number is d, the modulus. These numbers can be made public and are usually chosen from a table of known values. c is usually a very small number, and d is a very large prime number. Next, every party generates its own secret value. Then, based on c, d, and the secret value of each party, each party calculates its public value. The public value is computed according to the following formula:

$$Y = c^X \bmod d$$

Where, X is the secret value of the entity. Y is the public value of the entity.

After computing the public values, the two parties exchange their public values. Each party exponentiates the received public value with its secret value to compute a common shared secret value. When the algorithm completes, both parties have the same shared secret, which they have computed from their secret value and the public value of the other party.

4.1.2. Basic Function.

- Diffie-Hellman depend on "modular" arithmetic
  - (i) Sometimes know as 'clock' or 'remainder' arithmetic
  - (ii) Residue of a number to a base is the remainder from when that number is divided by base.
- Equivalence notation first developed by Gauss

  $$38 \equiv 14 \pmod{12}$$

  - (i) 38 and 14 are congruent modulo 12 because they have the same remainder (i.e., 2).
- Modulo arithmetic is inherently a one-way function
  - (i) There are an infinite set of numbers that are congruent to 14 (mod 12).
- Concept of Diffie-Hellman Key Exchange Algorithm in Basic Function
  - ▪ General one way function is

    $$Y^X \pmod{P}$$

    The following example uses small prime numbers for demonstration

    i. Assume that 7 and 11 are Y and P agreed beforehand by two parties, thus the one-way function is

    $$7^X \pmod{11}$$

4.1.3. Prime Number. Discrete logarithms are fundamental to a number of public key algorithms, including Diffie-Hellman key exchange and the Digital Signature Algorithm(DSA).

The Powers of an Integer, Modulo n

$$a^{\varphi(n)} \equiv 1 \mod n$$

$$a^{m} \equiv 1 \mod n$$

If a and n are relatively prime, then there is at least one integer m that satisfies, namely, m = φ(n).

- the order of a (mod n).
- the exponent to which a belongs (mod n).
- the length of the period generated by a.

4.1.4. Primitive root. The importance of this notion is that if a is a primitive root of n,

$$a,\ a^2,\ \ldots\ldots,\ a^{\varphi(n)}$$

$$a,\ a^2,\ \ldots\ldots,\ a^{p-1}$$

E.g. 19's primitive roots are 2, 3, 10, 13, 14 and 15.

4.2. Proposed Data Encryption Standard (DES)

DES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of cipher text as output. The decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key used as input to produce the original 8-bit block of plaintext. The encryption algorithm involves five functions; an Initial Permutation (IP), a complex function called f_K which involves both permutation and substitution operations and depends on a key input; a simple permutation function that Switches (SW) the two halves of the data; the function f_K again, and a permutation function that is the inverse of the Initial Permutation (IP^{-1}).

The function f_K takes as input the data passing through the encryption algorithm and an 8-bit key. Consider a 10-bit key from which two 8-bit sub keys are generated. In this case, the key is first subjected to a permutation P10 = [3 5 2 7 5 10 1 9 8 6], then a shift operation is performed. The numbers in the array represent the value of that bit in the original 10-bit key. The output of the shift operation then passes through a permutation function that produces an 8-bit output P8 = [6 3 7 4 8 5 10 9] for the first sub key (K_1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the second sub key (K_2). In all bit strings, the leftmost position corresponds to the first bit.

5. The propose system architecture

To set up the connection, one machine must be running a program that is waiting for a connection, and the other machine must try to reach the first. Transmission Control Protocol/Internet Protocol or TCP/IP is presented in this implementation.

Port numbers in TCP/IP systems are 16-bit numbers and range from 0 to 65535. In practice, port numbers below 1024 are reserved for predefined services, and you should not use them unless want to communicate with one of those services. Client port numbers are allocated by the host OS to something not in use, while server port numbers are specified by the programmer, and are used to identify a particular service.

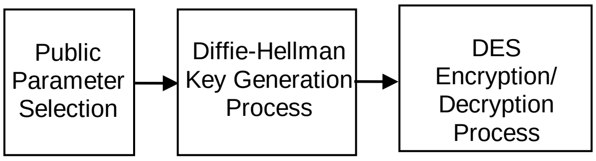
Public Parameter Selection
Diffie-Hellman Key Generation Process
DES Encryption/ Decryption Process

Figure 3. Overview of the propose system

In Figure 3, firstly, users connect to their connection name. And then, users select their public key respectively for their process. Next, Diffie-Hellman Key Exchange Algorithm calculates with public key and then this process gives the secret key as output. And then, getting secret key is needed to use again by DES algorithm for encryption and decryption techniques.

5.2. DES encryption approach

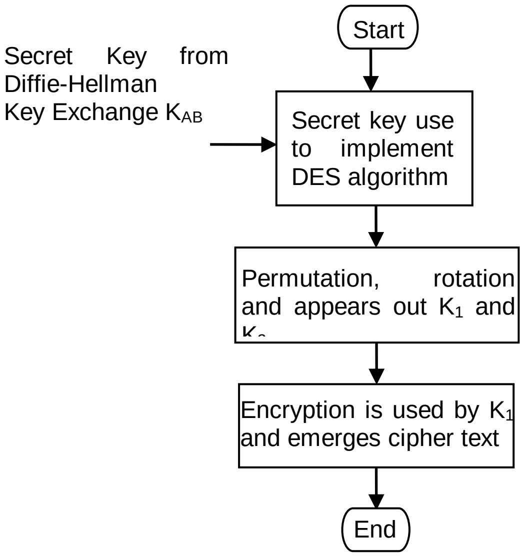
Start
Secret Key from Diffie-Hellman Key Exchange K_{AB}
Secret key use to implement DES algorithm
Permutation, rotation and appears out K_1 and K_2
Encryption is used by K_1 and emerges cipher text
End

Figure 4. Encryption approach of DES

Figure 4 describes encryption approach of Data Encryption Standard (DES). DES algorithm uses secret key from Diffe-Hellman Key Exchange algorithm. This secret key is used to implement DES algorithm. The key is subjected to permutation and shift operation is performed. And then, the keys, K_1 and K_2 are appeared. Then, plaintext is encrypted by using key K_1 to emerge cipher text.

5.3. DES decryption approach

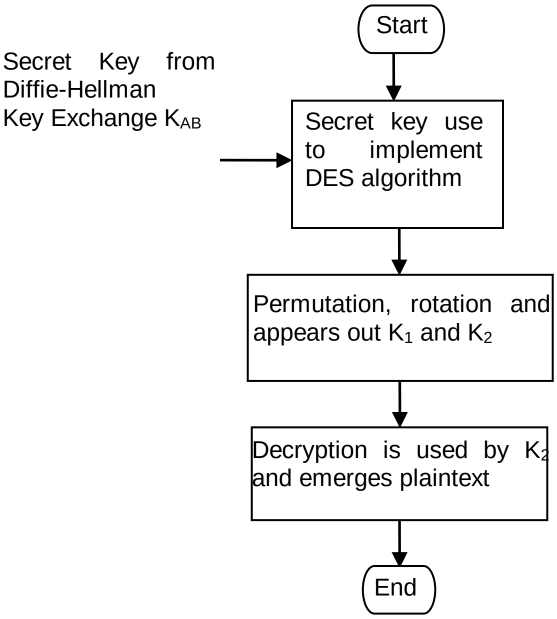
Start
Secret Key from Diffie-Hellman Key Exchange K_{AB}
Secret key use to implement DES algorithm
Permutation, rotation and appears out K_1 and K_2
Decryption is used by K_2 and emerges plaintext
End

Figure 5. Decryption approach of DES

Figure 5 describes decryption approach of Data Encryption Standard (DES). DES algorithm uses secret key from Diffe-Hellman Key Exchange algorithm. This secret key is used to implement DES algorithm. The key is subjected to permutation and shift operation is performed. And then, the keys, K_1 and K_2 are appeared. Then, cipher text is decrypted by using key K_2 to emerge plaintext.

6. Conclusion

In this system, D-H is better security then other algorithm because it relies on discrete logarithm. And then output of secret key is substituted by applying DES algorithm for using encrypted/decrypted messages or text files or images and so on.

Combining of public keys (asymmetric key) and secret key (symmetric key) are more secure than other encryption algorithm.

Prime number is used by this system; the third party does not know where public key and secret key have. So, the prime numbers are difficult to attack by other parties. DES also uses one secret key input. So, combining of Diffie-Hellman and DES are better and secure than other algorithms.

As a matter of fact, one of the objectives of the data security is better and more secure.

In this system, prime number is used to protect for securing online system. In addition, discrete logarithm is also more secure than other algorithms such as RC-4, RC-5, and AES and so on. This system gives knowledge of symmetric and asymmetric key.

7. References

[1] W.C.Barker, "Information Security", May 2008.

[2] E.Biham, “Public Key Cryptography 1”, 2007.

[3] D.Coppersmith, “The Data Encryption Standard (DES) and its Strength against Attacks, 1994.

[4] A.C.David, “A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols”, SANS Institute, 2001.

[5] Federal, “Data Encryption Standard (DES)”, Information Processing Standards Publication, 1999, 46-3.

[6] Forouzan, Behrouz A., "TCP/IP Protocol Site", McGraw-Hill Companies, Inc. ISBN 0-256-24166-x, International Edition, 2000.

[7] B.N.Joshua, B.A.,”The Diffie-Helllman Key Exchange in Matrices over a Field and a Ring”, 2003.

[8] P.Lao, “Diffie-Hellman (D-H) Key Exchange Calculations”, (R&S CCIE/CCSP/CISSP/CISSI) from Learning @ Cisco, 1976.

[9] N.Nalni, et-al., “Cryptanalysis of Simplified Data Encryption Standard via Optimization Heuristics”, 2006.

[10] M.M.Thida, “Development of An E-mail Facility: Personal Mail Assistant”, M.C.Tech(Thesis), May 1997.

[11] K.Z.Win, “Secure Communication Between Two Points Using Triple DES Approach”, M.C.Tech(Thesis), 2008.

[12] C.T.Zan, “Instant Messaging System Over Enterprise Network”, M.C.Tech(Thesis), October 2003.

[13] http://www.thaiopensource.net schwarzwald pdftcpip.pdf

[14] http://en.wikipedia.org/wiki/Jade

[15] http:///www.OSI Seven Layer System.com