Implementation of Diffie – Hellman Key Exchange Algorithm for Secure Key Transmission

Nang Hnin Lae Wai
University of Computer Studies (Mandalay)
nanghninlaiwai@gmail.com

Abstract

Information Security is essential when communicating over any untrusted medium and information system. When data are transmited over insecure communications channel, key is used to encrypt or decrypt data. The attacker tries to know that key which can transform the original form. So, the secure key is the most important in cryptographic system. This paper explains about to encrypt data using Diffie-Hellman key exchange algorithm for secure key. Diffie-Hellman algorithm depends on discrete logarithm to determine the key. After obtaining secure key, this key is used to encrypt or decrypt data with RC4 algorithm which is a key stream cipher algorithm requiring a secure exchange of shared key developed by Ronald Rivest of RSA. Diffie-Hellman is paid deep attention because it is one of the most common protocols used in networking today. Therefore, this algorithm is also used in banking system, military and communication to report proposal or important data.

1. Introduction

The privacy requirements normally encountered in the traditional paper document world are increasingly expected in Internet transactions today. Secure digital communications are necessary for web-based e-commerce, mandated privacy for medical information, etc. In general, secure connections between parties communicating over the Internet is now a requirement. Diffie-Hellman is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. A shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. As such, it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSec) [1]. Computer security is an important field of study for most day-to-day transactions. Cryptography provides the basis for authentication of messages as well as their security and integrity; carefully designed security protocols are required to exploit it.

There are different types of encryption algorithms used to protect sensitive data including symmetric, asymmetric encryption techniques. In symmetric key cryptography, there are two methods: block and stream. The block method divides a large data set into blocks based on predefined size or the key size, encrypts each block separately and finally combines blocks to produce encrypted data. The stream method encrypts the data as a stream of bits without separating the data into blocks.

This paper is aimed to implement Diffie-Hellman key exchange algorithm and RC4 encryption algorithm. Diffie-Hellman key exchange algorithm is used to secure key exchange. And then, RC4 is used for encryption and decryption process.

The rest of this paper is organized as follows: Section 2 presents related work of this system. Section 3 discusses introduction to cryptography and cryptographic goals. Section 4 expresses the overview of the proposed system and then briefly discusses Diffie-Hellman key exchange and RC4 encryption/decryption algorithm. Section 5 depicts the design and implementation of the system. Finally, section 6 points out conclusion and future work.

2. Related work

Diffie-Hellman is commonly used when one encrypts data on the Web using either SSL or TLS (Secure socket layer and Transport Layer Security respectively). The Secure Shell (SSH) protocol also utilizes Diffie-Hellman because Diffie-Hellman is part of the key exchange mechanism for IP sec; any VPN based on that technology utilizes Diffie-Hellman as well [2].

A.Hodjat and I.Verbauwhede explore the energy cost of a key agreement process between two parties of an ad-hoc network using public-key encryption techniques and compare the results with regular networks which use secret-key based key exchange protocols. Elliptic Curve public-key and Rijndael AES secret-key algorithms are chosen to explore the energy cost of Diffie-Hellman and Kerberos key agreement protocols on a Wireless Integrated Network Sensors(WINS) [3].

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. E.Bresson, O.chevassut, D. Pointcheval and J.Quisquater present a security model and use it to precisely define AKE (with "implicit" authentication)as the fundamental goal, and the entity-authentication goal as well [4].

3. Cryptography

To keep information secret, there are two possible strategies: hide the existence of the information, or make the information unintelligible. An original message is known as the plaintext, while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is known as encryption: restoring the plaintext from the ciphertext is decryption. This process is also known as cryptography. Modern cryptography uses mathematical equations (algorithms) and secret keys to encrypt and decrypt data.

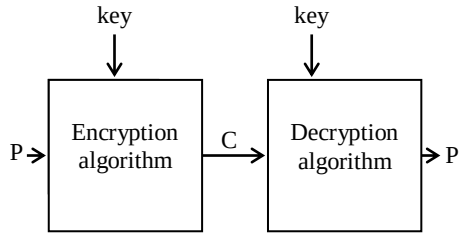

Figure 1: Basic Encryption and Decryption

Figure 1 shows the basic process of encryption and decryption. In Figure 1, P means plaintext and C means ciphertext.

- There are two types of operations used for transforming plaintext to ciphertext.
  (1) Substitution
  (2) Transposition
- Two types of key
  (1) Same key or symmetric key
  (2) Different key or asymmetric key
- The way in which plaintext is processed.
  (1) Block cipher
  (2) Stream cipher

3.1. Symmetric Key Cryptosystem

Symmetric key algorithms are algorithms where the encryption key can be calculated from the decryption key.

In most symmetric key algorithms, the encryption key and decryption key are the same.

These algorithms are also called secret key algorithms. RC4 is a symmetric key algorithm.

3.2. Stream Cipher

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. RC4 uses stream cipher process.

3.3. Cryptographic Goals

The main use of cryptography is to provide the following as mentioned earlier.

(1) privacy or confidentiality
(2) data integrity
(3) authentication and
(4) non-repudiation

4. Overview of the Proposed System

This system is implemented by the Diffie-Hellman key exchange algorithm and the popular symmetric key algorithm RC4. There are two parts which contain the following system:

-key exchange [Diffie-Hellman key exchange]
-data encryption/decryption algorithm [RC4]

4.1. Diffie-Hellman Key Exchange

Diffie-Hellman is a mathematical algorithm that allows two computers to generate an identical shared secret on both systems. That shared secret can then be used to securely exchange a cryptographic encryption key. That key then encrypts traffic between the two systems.

Diffie-Hellman is not an encryption mechanism in that we do not typically use it to encrypt data. Diffie-Hellman accomplishes this secure exchange by creating a “shared secret” (sometimes called a “Key Encryption Key” or KEK) between two devices [5].

Diffie-Hellman key exchange processes are as follows:

- Diffie-Hellman key agreement
- Diffie-Hellman key establishment
- Diffie-Hellman key negotiation
- Exponential key exchange

4.1.1. Diffie-Hellman Key Exchange Basic Protocol. At the start of Diffie-Hellman key exchange, the two users agree prime number p and primitive g. In Table 1,

(1) Alice picks large integer a and sends Bob $g^a \bmod n$
(2) Bob picks large integer y and sends Alice $g^b \bmod n$
(3) Alice computes $(g^b \bmod p)^a \bmod p$
(4) Bob computes $(g^a \bmod p)^b \bmod p$

Finally, Alice and bob obtain the shared secret key.

Table 1. Diffie-Hellman Key Exchange

Alice		
Sec		Calc
	p,g	
a		
		g^a mod p
	…	
	$(g^b \bmod p)^a \bmod p$	

Bob		
Calc		Sec
	p,g	
		b
	…	
g^b mod p		
	$(g^a \bmod p)^b \bmod p$	

p=prime number
g=primitive root

sec = secret
calc = calculate

4.1.2. Primitive Roots. The Diffie-Hellman key exchange algorithm starts with the selection of a prime number plus one of its primitive roots (sometimes called "primitives generators").

If the prime number is p, a primitive roots g is a number, when n goes from 1 to p-1, a^n mod p means the remainder when you raise a to n and divide by p.

The set of remainders reproduces the set of integers 1 to p-1 (in order needs not be identical), then 'a' is primitive of p. In Table 2, 2 and 3 are primitive roots of 5.

Table 2. Power of Integers, Modulo 5

a	a^2	a^3	a^4
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

4.2. RC4 Algorithm

Algorithm : Symmetric key
Key size : (8-2048) bits
Cipher : stream cipher
Encryption / Decryption : byte by byte (one byte)
Structure : Pseudo Random Number Generator
Operation : S-box, Modulus, Addition, Permutation, X-OR

4.2.1. Stream Generation. In stream cipher structure, a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random and using the following process.

Initialization of S

```
for i=0 to 255 do
S [i]= i;
T [i]=K [ i mod keylen ];
Initial Permutation of S
j =0;
for i=0 to 255 do
j=( j+ S [i] + T [i] ) mod 256;
Swap (S [i] ,S [j] );
Stream Generation
i, j=0;
While (true)
i = (i+ 1) mod 256;
j = (j+ S [i] ) mod 256;
Swap ( S [i] ,S [j]);
t= (S [i] +S [j]) mod 256;
k=S [t];[6]
```

A pseudorandom stream is one that is unpredictable without knowledge of input key .The output of the generator, called a keystream , is combined one byte at a time with the plaintext stream using the bitwise exclusive OR(X-OR) operation [7].

	Encryption	Decryption
	11001100 plaintext	10100000ciphertext
⊕	01101100 key stream	01101100keystream
	10100000 ciphertext	11001100 plaintext

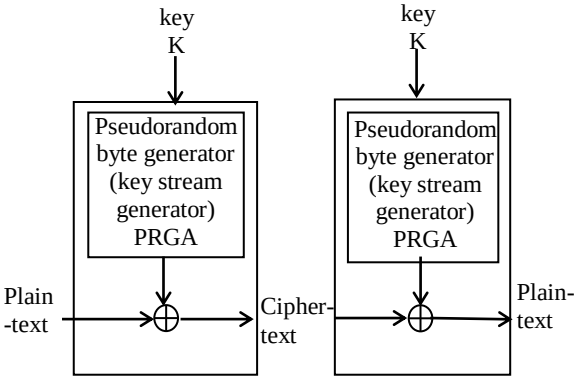

Figure 2. Stream Cipher Diagram

4.2.2. Benefits of RC4. RC4 is faster than RC2, DES, and 3DES. It can be used in variable key length. It can run very quick in software. It is the most widely used and secure symmetric algorithm.

5. Design and Implementation

5.1. Implementation of the System

In Figure 3 shows flow of the system. According to Diffie-Hellman key exchange algorithm, program user A and B start to select prime number p and then choose the primitives root of p, g < p in both side. If the primitive is correct, user A and B select random

number less than p. Later, they calculate their public number. A sends public number to B and B sends public number to A .Both users can calculate the secret key and it must be identical.

Example of Diffie-Hellman key exchange algorithm

1.Alice and Bob agree to use a prime number p=23 and base g=5.

2.Alice chooses a secret integer a=6, then sends Bob (g^a mod p)

5^6 mod 23 = 8.

3.Bob chooses a secret integer b=15, then sends Alice (g^b mod p)

5^{15} mod 23 = 19.

4.Alice computes (g^b mod p)^a mod p

19^6 mod 23 = 2.

5.Bob computes (g^a mod p)^b mod p

8^{15} mod 23 = 2.

After Diffie-Hellman key exchange, using shared secret key RC4 encryption is processed, the output stream generation is XOR with plaintext. Finally, they can encrypt and decrypt data securely.

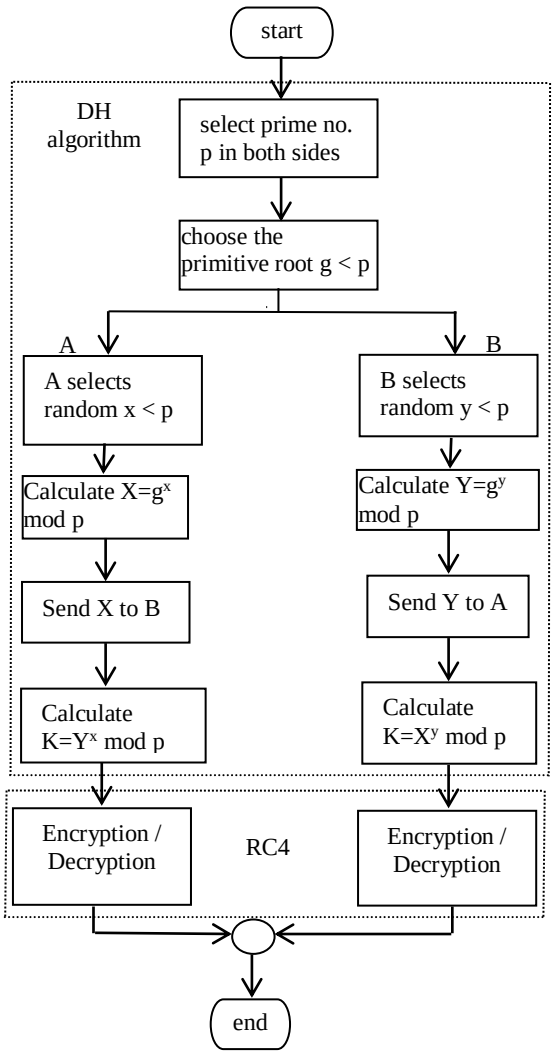

Figure 3. System Flow Diagram

5.2. Security of the System

Table 3. Security of Diffie-Hellman Key Exchange

knows	doesn't know
p=23	a=6
base g=5	b=15
	s=2
5^a mod 23=8	
5^b mod 23=19	
19^a mod 23=s	
8^b mod 23=s	
19^a mod 23=8^b mod 23	

In Table 3, the eavesdropper only learns p and g but doesn't know a and b, then cannot calculate s.

5.3. Advantages of the System

The system can provide the secure way for data encryption and key exchange. By using this system, the security of text data can be obtained. This system applies the Diffie-Hellman key exchange algorithm; therefore, the user can exchange key securely at a fast encryption speed and can solve the key announcement problem. And then, RC4 algorithm is used in order to achieve the speed advantages; the system applies the symmetric key cryptosystem because of stream cipher encryption.

6. Conclusion and Future Work

In this paper, RC4 encryption algorithm is implemented by using Diffie-Hellman Key Exchange Algorithm. In many application areas, Diffie-Hellman Key Exchange system is widely used. Specifically, Diffie-Hellman key exchange is required to use for securing information. RC4 algorithm is faster and more secure than other algorithm because of using Pseudo Random Generation Algorithm (PRGA).

The user can exchange Key securely at a fast encryption speed and can solve the key announcement problem. This system can also satisfy confidentiality (prevent eavesdropping), authenticity (the sender is really who he says he is), and integrity (the message has not been changed) that are the cryptographic goals.

The system could have been excellent if there had been much time to implement. Therefore, if this system is expected to extend, it can be optimized using CA (Certificate Authorities), Certifies Public Key, to prevent Man In the Middle (MIM) attacks.

7. References

[1] D.A.Carts ,"A Review of the Diffie-Hellman Algorithm and its use in Secure Internet Protocols",SANS Institute 2001

[2] K.Palmgren, CISSP, Security +, TICSA "Diffie-Hellman key Exchange A Non-Mathematician's Explanation"

[3] A.Hodjat and I.Verbauwhede,"The Enery cost of Secerts in Ad-hoc Networks",Los Angeles CA-90024

[4] E.Bresson,O.Chevassut, D.Pointcheval , J.Quisquater, "Provably Authenticated Group Diffie-Hellman Key Exchange ",Computer and communications Security - Proc.of ACM CCS '01,p-255-264

[5] http:// www.wikipedia.en

[6] http://www.vocal.com.RC4.html

[7] S.William, *"Cryptography and Network Security"* principles and practices, 3rd Edition, ISBN 0-13-084370-9