Secure Teaching Support System Using FTP Protocol

San Ohnmar Kyaw, Tin Zar Zar
Computer University (Dawei)
heartbeachlay@gmail.com

Abstract

File Transfer Protocol (FTP) is the standard mechanism for copying a file from one host to another. Transferring file from one computer to another is one of the most common tasks expected for networking and internetworking environment. This thesis is intended to implement teaching support system for Computer Universities by using FTP.This system can assist the teachers in Computer Universities to cooperate over the network. It can deliver the ability to manage and access teaching materials. The teaching materials contains sample questions, sample answers, exam scope, lecture plan, postgraduates scope, other solutions and important information .While transferring files over network, it is needed to provide security for some important information. To provide the security, the system is implemented by using ElGamal Algorithm. The system uses a network operation system design to manage the entire network from a centralized point, (server).Sever has to transfer encrypted files over the network. On the receiving site, the encrypted files must be decrypted by the client to get the original data. Therefore the system can transfer files with the help of File Transfer Protocol and provides security using ElGamal algorithm.

1. Introduction

Nowadays, on line system is dramatically successed in providing an easy way for user to share and distribute data. The on-line application enables the users to connect to the system at anytime and anywhere [5]. These on-line applications are used to distribute the required data among Computer Universities. Teaching materials can be transferred over the network in time. The most common method for transferring files over the internet and intranet is provided by File Transfer Protocol (FTP). For transferring files from one host to another, security requirement became essential. So Cryptography was applied to fulfill this requirement. These days, many programmers and system developers develop FTP user agent software for transferring files .They also try to provide secure methods to prevent unauthorized access for transferred files. In sensitive Internet transactions that occur daily, the benefit of securing information using cryptographic processes becomes a major goal for many organizations. This paper cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. For transferring files, client-server two tire architecture is used. The server keeps the encrypted data before receiving requests from the client. When it gets request from the client, it transfers the encrypted data. After receiving these encrypted data, the client decrypts it to get the original message.

The purpose of the system is to intend the teachers to obtain the acquire files are timely by hand and through secure channel over the network.

2. File Transfer Protocol

File Transfer Protocol is the most important protocol in TCP/IP protocol suit. FTP works an application layer of TCP/IP or OSI reference model [1]. Application layer is a layer on which user applications are running. FTP uses TCP and therefore it provides reliable service. It needs two TCP connections: control connection and data connection. The well known port 21 is used for the control connection and the well known port 20 is used for the data connection. How FTP works and overview of FTP configuration is shown in Figure 1.

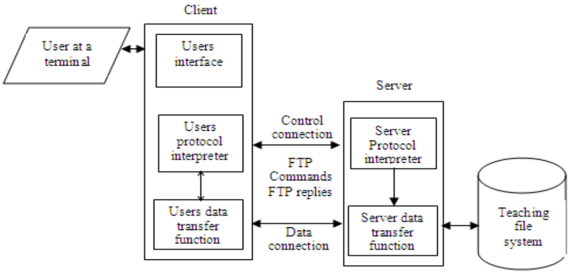


Figure 1: Overview of FTP Configuration

3. Control Connection

The control connection is created in two steps:

1. The server is issued a passive open on the well-known port 21 and waits for the client.
2. The client uses an ephemeral port and issues an active open.

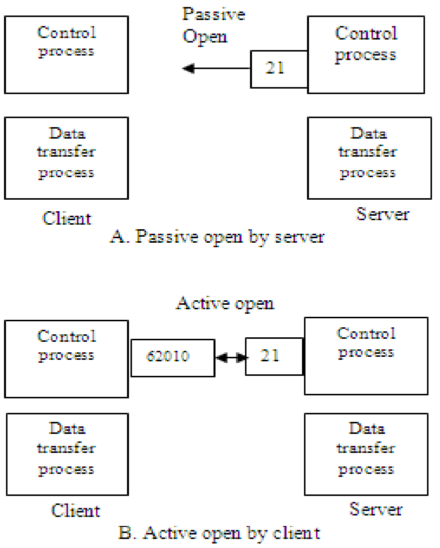
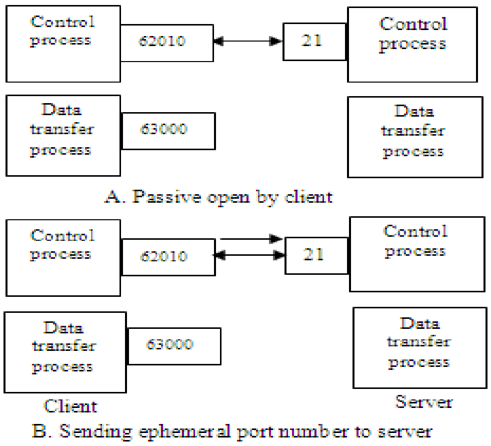


Figure 2: Opening the Control Connection

3.1 Data Connection

The data connection uses the well-known port 20 at the server site. Creating a data connecting by FTP includes three steps.

1. The client issues a passive open using an ephemeral port to send the commands for transferring files.
2. It sends this port number to the sever using the PORT command.
3. The server receives the port number and issues an active open using the well-known port 20 and the received ephemeral port number.



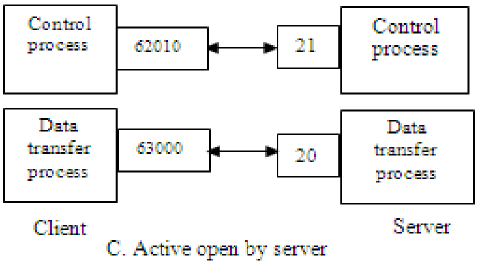


Figure 3: Creation the Data Connection

3.2 FTP Commands

FTP commands, which are sent from FTP client control process, are in the form of ASCII uppercase, which may or may not be followed by an argument. Commands can be divided into six groups: access commands, file management commands, file transferring commands, and miscellaneous commands. e.g. PASS command is decryption the user password. DELETE command is to delete a file. PORT command is used by client chooses a port. RETR command is retrieve file transfer from server and STOR command is use to store transfer file.

3.3 Responds

Every FTP command generates at least one response. A response has two parts: a three digit number followed by text. The numeric part defines the code; the text part defines needed parameters or extra explanations. Three digits will be represented as xyz. e.g. The second digit also defines the status of the command.

1. x2z (Connection)
2. x3z(Authentication and Accounting)
3. x5z(File System)

The third digit provides addition information.

Code No. 125 is the description of the data connection open. 200 is the description of the command OK. 226 is to use closing data connection. 230 is User Login OK. 250 is to describe the Request file action OK, etc.

4. Cryptography

Cryptography, a word with Greek origins, means “secret writing”[3]. The cryptography is physical process scrambles information by rearrangement and substitution of contents making it unreadable to anyone expects the person capable of unscrambling. It so, cryptography consists of two process; encryption and decryption. Cryptography is a method of storing and transmitting data in a form that only those it is intended for to read and process [2]. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths [3]. The ElGamal Encryption algorithm, used in this paper, is a public key algorithm introduced in 1985 by T.ElGamal. These have been no successful attack on this algorithm ever reported. ElGamal, which is based on the difficult of a problem called the discrete logarithm. These types of methods are based on finding the private-key from the public key. This depends on the length of the public/private key pair and the computing difficulty that might be used to "crack" the key pair. The key length of the ElGamal can range from 256- bit to arbitrarily long. Private key can range from 160-bit to 240-bit. The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem [4]. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol. Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

4.1 ElGamal Algorithm

```
ElGamal-Key- Generation
{   Select a large prime p
     Select d to be a member of the group G=<$Z_p$*,
      x> such that $1 \leq d \leq p- 2$
     Select $e_1$ to be a primitive root in the group
      G=< Zp*, x>
      Equation   $e_2 \longleftarrow e_1^d$ mod p
     Public – key $\longleftarrow$ ($e_1$, $e_2$, P)
     Private _ key $\longleftarrow$ d
     Return Public – key and Private –key
}
ElGamal –Encryption ($e_1$, $e_2$, p, P)
{
    Select a random integer r in the group
    G=<Zp*,x>
    $C_1 \longleftarrow e_1^r$ mod p
    $C_2 \longleftarrow$ (P x $e_2^r$) mod p
    return $C_1$ and $C_2$
    P is the plaintext
    $C_1$ and $C_2$ are the cipher text
ElGamal- Decryption (d, p, $C_1$, $C_2$)
{
    P$\longleftarrow$[$C_2$ ( $C_1^d$) $^{-1}$] mod p
     return P
}
```

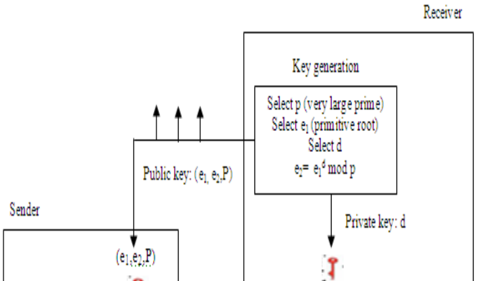

Receiver
Key generation
Select p (very large prime)
Select e_1 (primitive root)
Select d
$e_2= e_1^d$ mod p
Public key: (e_1, e_2,P)
Private key: d
Sender
(e_1,e_2,P)

Figure 4: Key generation, Encryption and Decryption in ElGamal Algorithm

4.2 ElGamal Key Generation

Receiver will take the following steps to generate his key pairs:

Prime and group generation

First receiver needs to generate a large prime p and the generator e_1 of a multiplicative group Zp* of the integers modulo p.

Private Key selection

Receiver selects an integer d from the group G by random and with the constraints $1\leq d\leq p-2$. This will be the private exponent.

Public Keys assembling

Can compute e_2 the public key part e_1^d mod p. The public key of receiver in the ElGamal cryptosystem is the triplet (e_1 ,e_2 , p) and his private key is d.

Public key publishing

The public key now needs to be published using some dedicated key server or other means, so that sender is able to get hold of it.

4.3 ElGamal Encryption

To encrypt a message M to receiver, sender first needs to obtain his public key triplet (e_1, e_2, p) from a key server or by receiving it from him via unencrypted electronic mail. There is no security issue involved in this transmission, as the only secret part d, is sent in e_1^d. ElGamal cryptosystem says that it is infeasible to compute the discrete logarithm. For the encryption of the plaintext message M, sender has to follow these steps [6].

Obtain the public key

Sender has to acquire the public key part (e_1, e_2, p) of receiver from an official and trusted key server.

Prepare M for encoding

M as set of integers (m1, m2, …….) in the range of {1,……,p-1}. These integers will be encoded one by

one.
Select random exponent
Sender will select a random exponent r, sender should choose a different random integer r for each message he sends to receiver.
Compute public key
To transmit the random exponent r to receiver, sender computes $C_1 = e_1^{\ r}$ mod p and combines it with the cipher text that shall be sent to receiver.
Encrypt the plaintext
Alice encrypts the message M to the cipher text C. For this, she iterates over the set created in step2 and calculates for each of the mi.

$$C_i = m_1 * (e_1^{d})^r$$

The cipher text C is the set of all c_i with o<i ≤/M/. The resulting encrypted message C is sent to receiver together with the public key $C_1 = e_1^r$ mod p derived from the random private exponent. ElGamal advises to use a new random r for each f thee single message blocks m_i. This greatly improves security, as knowledge of one message block m_j does not lead the attacker to the knowledge of all other m_i. The reason for this ability is that if $c_1 = m_1 * (e_1^{d})^r$ mod p and $c_2 = m_2 * (e_1^{d})^r$ mod p , from knowing only m_1 the next part of the message m_2 can be calculated by the following formula:

$$m_1/m_2 = c_1/c_2$$

4.4 ElGamal Decryption

After receiving the encrypted message C and the randomized public key e_1^r, receiver has to use the encryption algorithm to be able to read the plaintext M. This algorithm can be divided in a few single steps.
Compute shared key
The ElGamal cryptosystem helped sender to define a shared secret key without receiver's interaction. This shared secret is the combination of receiver's private exponent d and the random exponent r chosen by Alice.
The shared key is defined by the following equation;

$$(e_1^r)^{p-1-d} = (e_1^r)^{-d} = d^{-dr}$$

Decryption
For each of the cipher text parts "ci" receiver now computes the plaintext using:

$$M_i = (C_1)^{-d} * C_i \bmod p$$

After combining all of the " m_i" back to M he can read the message sent by sender.

4.5 Discrete Logarithm Problem

Thus the security of the ElGamal digital signature algorithm is based on the difficult of solving discrete log problem [4].
Let p be a prime and α and β be non zero integers in Zp and suppose.
The problem of finding x is called the discrete logarithm problem.

$$X = \log \alpha\ \beta$$

α is a primitive root mod p
Remainder: Zp is a field { 0,1…..,p-1}
Zp* is a cyclic finite group {1,….p-1}

4.6 System Design and Implementation

This system is client-server two tier architectures system. There are Main University Authorized Group and Sub University in this system. The clients represent the Sub University. The Server represents the main University. There is a database in the server to store encrypted files.

4.6.1 Teaching System for Server Side

In the server side is implemented to have adding files function and updating. The server side Authorized user must first Log in to server. If the Log in is succeed, Authorized user from Main University can add and update teaching material files. The system generates key pairs (public key and private key). Main University (server) encrypts the teaching material files for Sub Universities with public key by using ElGamal Algorithm. After encryption, these encrypted files are stored to the database. Authorized user can create files whenever and whatever they are needed to be sent Sub University.

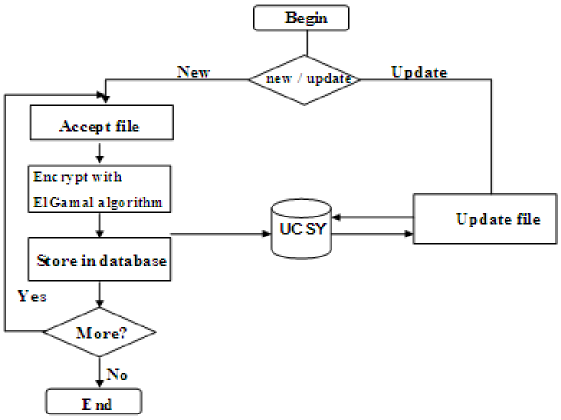


Figure 5: System Design for Server Side

4.6.2 Teaching System for Client Side

In the client side is implemented to retrieve the required encrypted files and then decrypted them. The client side, Sub University (user) must first Log in to client. If the Log in is succeed, the user (client) can request the required files from the FTP server. After receiving the required files, the client decrypts the encrypted teaching files with his private key and produces the plaintext. User can select files whenever and whatever they are needed to be downloaded encrypt file and then decrypted after it has been successfully arrived to client.

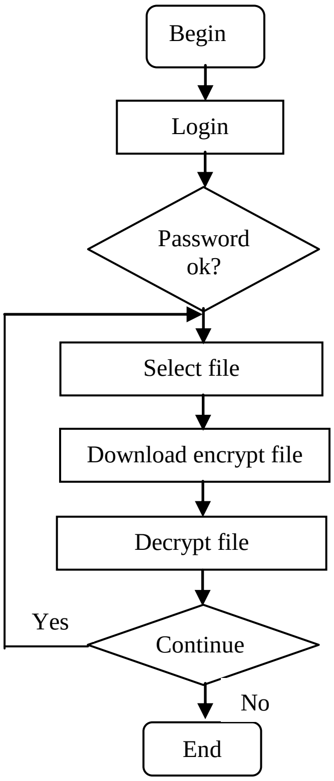


Figure 6: System Design for Client Side

5. Advantages

This system support for transferring files between hosts over the network with easy and effective way. And then support for understanding the File Transfer Protocol Principles. This system provides prevent unauthorized access to files. Security power is stronger than paper - based system for the producing teaching materials and other important information for universities. ElGamal Cryptosystem is as secure as it is hard to solve the Discrete Logarithm Problems, given no weak random exponents or primes are chosen. The same plaintext gives a different ciphertext each time it is encrypted. This system is less time consuming and cost-effective.

6. Conclusion

In this paper, the system for transferring and copying files over the network. File Transfer Protocol (FTP) is a standard mechanism provided by TCP/IP. This paper will also study encryption and decryption algorithm to secure files. This system implements the arrangement of Secure Teaching System based on ElGamal Algorithm. By using ElGamal Algorithm can obtain the security of importance information as well as text data and provide fast and secure way for communication of sensitive data in this system.

7. References

[1] B. A. Forouzan, “TCP/IP Protocol Suit (Second Edition)

[2] Behrouz A. Forouzan , “Cryptography and Network Security” , Principles and Practices ,International Edition, 2008

[3] D.R.Stinson. *Cryptography: Theory and Practice. CRC Press*, Inc., Boca Raton, FL, USA, 1995.
http : // www.daveloz in ski.com / tutorials / ftp/ example 1.gif

[4] Taher El Gamal. *A public key cryptosystem and a signature scheme based on discrete logarithms*. In Proceedings of CRYPTO 84 on Advances in cryptology,pages 10-18. Springer-Verlag New York, Inc., 1985.

[5] W. Stallings “Data and Computer Communications (SixthEdition)”

[6] W.Stallings, “*Cryptography and Network Security*”, Principles and Practices, Fourth Edition, 2006