Advanced Encryption using AES and Diffie Hellman Key Exchange

The motive of the project is to review and implement the Diffie-Hellman key exchange protocol and study its applications especially for the internet key exchange. Create a web page for an electronic business. Encipher sensitive data such as customer credit number, SSN etc. before transporting them from client to server. The idea is simple, the customer access the website powered by our simple http server, our web server will reply with a java servlet. The client will communicate with server by Diffie-Hellman key-exchange protocol to generate the common shared key, which is used in the later communication. After key exchange, both server and client will use the shared key to encipher and decipher the sensitive data such as customer credit number, SSN etc.

- The project is developed using Visual Studio with C# .Net as programming language.
- There is only one entity who will have the access to the system, which is user.
- User first need to login using its login credentials and then only he/she can access the system.
- Encryption is the technique of hiding private or sensitive information within something that appears to be nothing be a usual.
- If a person views that cipher text, he or she will have no idea that there is any secret information.

- What encryption essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them.
- What this system does is, it lets user to send text as secrete message and gives a key or a password to lock the text, what this key does is, it encrypts the text, so that even if it is hacked by hacker it will not be able to read the text.
- Receiver will need the key to decrypt the hidden text.
- User then sends the key to the receiver and then he enters the key or password for decryption of text, he then presses decrypt key to get secret text from the sender.
- By using this method, you can double ensure that your secret message is sent secretly without outside interference of hackers or crackers.
- If sender sends this cipher text in public others will not know what is it, and it will be received by receiver.
- The system uses online database to store all related information.

Modules:

The system comprises of 3 major modules with their sub-modules as follows:

- **Encryption:** Plain text is replaced using mod algorithm. Shared key is generated using Diffie-Hellman algorithm. Shared secret key is used to encrypt the replaced text. Encryption is done using AES. Finally, padding bits are added to left or right of encrypted text.

- **Decryption:** Encrypted text with padding bits is decrypted by removing padding bits from left or right of encrypted text. Shared secret key is generated using Diffie-Hellman

algorithm. Encrypted text is decrypted using AES with shared secret key. Finally, text is replaced using mod algorithm to generate plain text.

- **Key generation:** System will generate key using first primary key and second primary key and users private.

Software Requirements:

- Windows 7 or higher.
- SQL 2008
- Visual studio 2010

Hardware Components:

- Processor – i3
- Hard Disk – 5 GB
- Memory – 1GB RAM
- Internet Connection

Advantages:

- Fast and easy way of to send secure text messages.
- Use two-way encryption technique.
- Easy process to encrypt text on image.
- Uses secured SQL database to store the information.

Limitation:

- Password have to be shared which can be hacked and used.

Application:

Everyone who wants send some confidential text to someone can use this system. Image can be shared by any easy mean like email, WhatsApp, etc.

Reference:

- ✓ http://www.cc.gatech.edu/classes/cs8113e_96_winter/ - Visited on 09/16/2005 – college website
- ✓ http://www.cryptography.com/- Visited on 09/18/2005
- ✓ http://www.cs.purdue.edu/homes/jiangx/02spring/- Visited on 09/18/2005