

ABSTRACT

Ssh is a service which use TCP/IP port 22 connection to remote a distance host. The access use an ssh application named ssh client. With this ssh, whenever data is sent by a computer to the network, SSH automatically encrypts it. When the data reaches its intended recipient, SSH automatically decrypts (unscrambles) it. The result is *transparent* encryption: users can work normally, unaware that their communications are safely encrypted on the network.

In this final assignment will be developed an application of SSH client in the cellular phone. So, it is hoped the program can bring the features and benefits of SSH in the phone that connect to internet by GPRS, and we can use the program just like we use the SSH client program on a PC that connect to a network by a wire or a wireless connection.

Ssh client application, developed by using J2ME, and it is compiled by using sun WTK 2.2 (plug-in proguard) and ant apache (plug-in antenna) on a mobile device which have Mobile Information Device Profile (MIDP) 1.0 / 2.0 specification. A running test and cipher algorithm comparison are held to analyze this application, to choose the most optimal algorithm which can be implemented in the application.

From the implementation and the result of comparative analysis, it is concluded that ssh client can be implemented in a mobile device, and the keypad limitation in a phone can handled by using vt320 terminal emulator. From delay comparative analysis, Blowfish algorithm is chosen as the most optimal algorithm which can be implemented in the application, because it provides the smallest delay.

Keyword : ssh, J2ME, encryption algorithm, mobile device