Perancangan aplikasi instant messenger pada android menggunakan asymmetric key encryption sebagai pengaman pesan dalam jaringan = The development of instant messenger application for android using asymmetric key encryption for message protection in network / Laurentinus Rian

Laurentinus Rian, author

Abstrak

ABSTRAK
Skripsi ini membahas tentang aplikasi Instant Messenger pada smartphone berbasis Android. Aplikasi ini memanfaatkan asymmetric encryption dalam pengamanan pesan. Asymmetric encryption dipilih agar dapat memberikan pengamanan yang baik kepada pengguna aplikasi sehingga pesan yang dikirimkan hanya dapat dibaca oleh pengirim dan penerima. Aplikasi ini menggunakan protokol XMPP yang merupakan salah satu protokol dalam instant messenger yang bersifat open source. Analisa keamanan pesan dilakukan terhadap variasi algoritma enkripsi dan panjang kunci yang digunakan yang mempengaruhi waktu yang diperlukan untuk melakukan proses enkripsi tersebut dan panjang data hasil enkripsi. Variasi-variasi ini dianalisasi untuk menentukan algoritma enkripsi dan panjang kunci yang optimal untuk digunakan pada aplikasi instant messenger pada smartphone berbasis Android dengan memperhatikan batas kemampuan smartphone tersebut. Dari hasil penelitian ini didapatkan bahwa algoritma enkripsi ECIES memiliki performa yang paling baik untuk diterapkan pada aplikasi instant messenger. Pada proses pembuatan kunci memiliki persentase peningkatan sebesar 99.89% dibandingkan RSA dan 93,63% dibandingkan Diffie-Hellman. Pada proses enkripsi algoritma ini tidak sebaik RSA namun pada proses dekripsi memiliki peningkatan sebesar 85, 36 % dibandingkan RSA dan 98,35% dibandingkan Diffie-Hellman
<hr>
ABSTRACT
This paper discussing about Instant Messenger application for Android. This application uses asymmetric encryption for message protection. Asymmetric encryption is used because it will give good protection for application user so that only message sender and receiver who can read the message. This application uses XMPP protocol. XMPP is an open source instant messenger protocol. Message protection is analyzed using encryption algorithms and key lengths variation. An algorithm and a key length will be chosen as the most suitable to use in Android smartphone. In the end, this research shows that ECIES encryption is the best algorithm to be used in instant messenger application. ECIES has 99.89% increment than RSA and 93.63% increment than Diffie-Hellman in creating keys process. Although ECIES does not have increment in encryption process than RSA but it has 85.36% increment than RSA and 98.35% increment than Diffie-Hellman in decryption process.