# INTISARI

Implementasi Tanda Tangan Digital Berbasis Algoritma Elgamal Pada Perangkat Bergerak

Oleh

Thoriq Az Zuhri Yunus

11/316928/PA/14047

Dewasa ini, perkembangan ilmu dan teknologi telah mempengaruhi segala aspek kehidupan. Tak terkecuali aspek komunikasi, seperti dalam pengiriman pesan. Semakin berkembangnya teknologi, pengiriman suatu pesan juga menjadi kurang aman. *Digital Signature* (tanda tangan digital) adalah suatu tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim pesan dan juga untuk memastikan isi asli dari pesan sudah dikirim tanpa perubahan. Tanda tangan digital memberikan hal-hal seperti otentikasi pesan, integritas pesan, dan *non-repudiation* (tak bisa disangkal).

*ElGamal signature scheme* adalah salah satu skema tanda tangan digital yang diperkenalkan oleh Taher ElGamal pada tahun 1985. Skema tanda tangan digital ini berbasis pada sulitnya menghitung logaritma diskrit. Penelitian ini mengimplementasikan algoritma tanda tangan digital ElGamal ke dalam aplikasi perangkat bergerak. Aplikasi dibangun untuk dapat membuat tanda tangan digital dari pesan teks dan mampu memverifikasinya. Pengembangan dilakukan pada platform android karena merupakan platform yang paling banyak digunakan saat ini.

Hasil pengujian yang dilakukan dalam penelitian ini menunjukkan bahwa sistem yang dibangun berdasarkan algoritma tanda tangan digital ElGamal mampu menandatangani pesan secara digital serta memverifikasinya. Meskipun proses ini membuat pesan yang dikirim oleh pengguna menjadi lebih panjang karena disisipi kunci serta tanda tangan digital, tapi hal ini adalah sebuah keharusan untuk proses verifikasi pesan oleh penerima. Sistem sangat cocok untuk perangkat bergerak karena kecepatannya dalam menandatangani dan verifikasi pesan.

Kata kunci : Tanda Tangan Digital, ElGamal, Android, Verifikasi Pesan

# ABSTRACT

*Implementation of Elgamal Digital Signature*

*Algorithm on Mobile Devices*

By

Thoriq Az Zuhri Yunus

11/316928/PA/14047

Today, technology and science development has influenced every aspect in our life. Communication is not an exception, such in messaging. The more technology develops, the more unsafe it is for us to deliver a message. Digital Signature is an electronic signatures that could be used both to authenticate sender's identity and to make sure that messages sent without changes. Digital Signature gives us message authentication, message integration, and non-repudiation.

ElGamal signature scheme is one of digital signature scheme that introduced by Taher ElGamal in 1985. This Digital Signature scheme is based on how hard it is to count discrete logarithm. This research implements Digital Signature algorithm ElGamal on a mobile device application. This application is built for making digital signature of text message and verified them. Development is done for android platform because it's the most used platform nowadays.

The result in this research shows us that a system build based on ElGamal digital signature algorithm could sign a message digitally and verify it. Even though this process made messages sent by user longer than it should be, but this is a must for verification process on the receiving side. This system is very recommended for mobile device because it is very fast at sign and verify message.

Keywords: Digital Signature, ElGamal, Android, Message verification