ABSTRAK

Otentikasi (authentication) merupakan identifikasi yang dilakukan oleh masing-masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapatkan oleh satu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian informasi yang diterima. Tanda tangan digital adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Skema yang dapat digunakan untuk melakukan proses tanda tangan digital terhadap suatu pesan juga bermacam-macam. Skema otentikasi dan tanda tangan digital Schnorr merupakan skema tanda tangan digital yang mengambil keamanan dari permasalahan menghitung logaritma diskrit. Skema tanda tangan ini menggunakan bilangan prima dan perpangkatan modulo dalam proses pembentukan kuncinya. Skema otentikasi dapat dimodifikasi menjadi skema tanda tangan digital. Proses pembentukan kunci privat dan publiknya sama seperti sekema otentikasi, namun pada skema tanda tangan digital ditambahkan sebuah fungsi hash. Pengembangan sistem yang digunakan dalam membangun perangkat lunak ini adalah metode Luther. Perangkat lunak untuk simulasi skema otentikasi dan tanda tangan digital Schnorr ini akan membantu pemahaman kriptografi terutama mengenai skema otentikasi dan tanda tangan digital Schnorr dan perangkat lunak ini juga dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar mencakup input variabel-variabel, kunci privat, kunci public, pesan, pembentukkan digital signature, proses verifikasi dan proses deskripsi.

Kata kunci : *Key Generation, Authentication, Digital Signature*

ABSTRACK

Otentikasi (authentication) constituting identification that did by each mutually party gets communication, fathom a meaning severally party which get communication shall identify one same another. Information that got by one party of other party shall be identified to ensure accepted information authenticity. Digital signature is an otentikasi's mechanism that enable order maker adds one code which act as signature it. Scheme applicabling to do digital signature process to an order also miscellaneous. otentikasi's scheme and undersign digital Schnorr constitutes digital signature scheme that take security of about problem account diskrit's logarithm.

Undersign scheme this utilize prime number and about rank modulo in processes its key forming. Scheme otentikasi can be modified as digital signature scheme. Forming process keys privat and its public as as sekema otentikasi, but on undersign scheme digital enhanced one hash's function. System development that is utilized in build this software Luther's method. Software for simulated schematic otentikasi and undersign digital Schnorr this will help kriptografi's grasp especially about scheme otentikasi and undersign digital Schnorr and this software can also be utilized as facility of supporting in processes teaching and learning to range variable inputs, privat's key, public's key, send away for, digital pembentukkan signature, process verification and description process.

Key Word : *Key Generation, Authentication, Digital Signature*