INTISARI

SKEMA TANDA TANGAN DIGITAL SIMPLEMATRIX

Oleh

NISA AYU AZZAHRA

20/462292/PA/20264

Kriptografi multivariat merupakan salah satu jenis kriptografi *post-quantum* yang sedang berkembang saat ini. Kriptografi multivariat menggunakan permasalahan untuk mencari solusi dari sistem persamaan multivariat untuk menjamin keamanannya. Pada tulisan ini akan dibahas salah satu kriptografi multivariat yaitu sistem kriptografi SimpleMatrix dan aplikasinya pada tanda tangan digital. Tulisan ini dimulai dengan mendeskripsikan sistem kriptografi SimpleMatrix dan dilanjutkan dengan aplikasinya pada tanda tangan digital. Selain itu, dilakukan simulasi untuk mengetahui perbedaan waktu yang dibutuhkan untuk menandatangani pesan dengan beberapa parameter berbeda.

ABSTRACT

A SIMPLEMATRIX DIGITAL SIGNATURE SCHEME

By

NISA AYU AZZAHRA

20/462292/PA/20264

A multivariate cryptography is one of the emerging types of post-quantum cryptography. Multivariate cryptography uses the problem of finding the solution of a multivariate system of equations to guarantee its security. This paper discussed one of the multivariate cryptography, SimpleMatrix cryptography systems and its application to digital signature. This paper began by describing the SimpleMatrix cryptographic system and continues with its application to digital signatures. In addition, simulations were carried out to determine the difference in the time required to sign a message with several different parameters.