INTISARI

SISTEM KRIPTOGRAFI RSA MENGGUNAKAN GRUP $GL_t(\mathbb{Z}_n)^*$ DAN APLIKASINYA PADA SKEMA TANDA TANGAN DIGITAL

Oleh

RIZKY NUR AFIFAH

19/445709/PA/19533

Sistem kriptografi RSA (Rivest Shamir Adleman) merupakan salah satu sistem kriptografi asimetris yang masih dikembangkan sampai saat ini. Salah satu contoh pengembangannya, yaitu sistem kriptografi RSA menggunakan grup $GL_t(\mathbb{Z}_n)^*$. Grup $GL_t(\mathbb{Z}_n)^*$ adalah grup terhadap operasi perkalian matriks yang beranggotakan matriks-matriks invertibel berukuran $t \times t$ atas $\mathbb{Z}_n$, dengan entri-entri diagonalnya merupakan unit di ring $\mathbb{Z}_n$. Sebagaimana sistem kriptografi RSA, sistem kriptografi RSA menggunakan grup $GL_t(\mathbb{Z}_n)^*$ juga dapat diaplikasikan pada skema tanda tangan digital. Dengan demikian, skripsi ini ditujukan untuk mempelajari sistem kriptografi RSA menggunakan $GL_t(\mathbb{Z}_n)^*$ dan aplikasinya pada skema tanda tangan digital.

ABSTRACT

AN RSA CRYPTOSYSTEM USING GROUP $GL_t(\mathbb{Z}_n)^*$ AND ITS APPLICATION ON A DIGITAL SIGNATURE SCHEME

By

RIZKY NUR AFIFAH

19/445709/PA/19533

RSA (Rivest Shamir Adleman) cryptosystem is an asymmetric cryptosystem that is still being developed today. One example of its development is RSA cryptosystem using the $GL_t(\mathbb{Z}_n)^*$ group. The group $GL_t(\mathbb{Z}_n)^*$ is a group under the matrix multiplication operation consisting of invertible matrices of size $t \times t$ over $\mathbb{Z}_n$, with its diagonal entries are unit in ring $\mathbb{Z}_n$. Similar to RSA cryptosystem, RSA cryptosystem using the $GL_t(\mathbb{Z}_n)^*$ group can also be applied to digital signature scheme. Therefore, this thesis is aimed at studying RSA cryptosystem using $GL_t(\mathbb{Z}_n)^*$ and its application on digital signature scheme.