ABSTRAK

Skripsi ini membahas secara teoretis Sistem Kriptografi Rabin, yaitu sebuah skema kriptografi asimetris yang diperkenalkan oleh Michael O. Rabin. Fokus utama penelitian adalah mekanisme enkripsi dan dekripsi serta dasar keamanan yang bergantung pada kesulitan faktorisasi bilangan bulat besar menjadi dua bilangan prima. Metode penelitian yang digunakan adalah studi pustaka dengan mengkaji berbagai literatur terkait teori bilangan dan kriptografi. Pembahasan meliputi proses pembentukan kunci publik $n = pq$ berdasarkan kunci privat (p, q), proses enkripsi $c \equiv m^2 \pmod{n}$, perhitungan akar kuadrat $\sqrt{c}$ modulo p dan q, serta penggabungan hasil menggunakan Teorema Sisa Cina. Hasil kajian menunjukkan bahwa keamanan algoritma Rabin setara dengan kesulitan faktorisasi n, dan proses dekripsi menghasilkan empat kemungkinan pesan sehingga diperlukan aturan tambahan agar teks asli dapat diidentifikasi dengan benar. Penelitian ini juga menjelaskan pentingnya pemilihan bilangan bulat Blum $p \equiv q \equiv 3 \pmod{4}$ untuk menyederhanakan proses dekripsi.

Kata kunci: Kriptografi Rabin, kriptografi asimetris, faktorisasi bilangan bulat, bilangan bulat Blum.

ABSTRACT

This thesis discusses the Rabin Cryptosystem from a theoretical perspective. Rabin is an asymmetric cryptographic scheme introduced by Michael O. Rabin. The main focus of this study is the encryption and decryption mechanisms and the security basis, which relies on the difficulty of factoring a large integer into two prime numbers. The research method used is a literature study by reviewing various sources related to number theory and cryptography. The discussion includes the construction of the public key $n = pq$ based on the private keys (p, q), the encryption process $c \equiv m^2 \pmod{n}$, the computation of square roots $\sqrt{c}$ modulo p and q, and the combination of results using the Chinese Remainder Theorem. The findings show that the security of the Rabin algorithm is equivalent to the difficulty of factoring n, and the decryption process produces four possible messages, so additional rules such as redundancy are required to correctly identify the original plaintext. This study also explains the importance of selecting Blum integers $p \equiv q \equiv 3 \pmod{4}$ in order to simplify the decryption process.

Keywords: Rabin Cryptosystem, asymmetric cryptography, integer factorization, Blum integers