SKRIPSI

KOMBINASI KRIPTOGRAFI KURVA ELIPTIK ATAS LAPANGAN BERHINGGA DAN MASALAH *KNAPSACK*

(THE COMBINATION OF ELLIPTIC CURVE CRYPTOGRAPHY OVER FINITE FIELD AND KNAPSACK PROBLEM)

DIAN PUTRI PANGESTU

24010119130108

DEPARTEMEN MATEMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

SEMARANG

2024

HALAMAN PENGESAHAN

SKRIPSI

KOMBINASI KRIPTOGRAFI KURVA ELIPTIK ATAS LAPANGAN BERHINGGA DAN MASALAH *KNAPSACK*

Telah dipersiapkan dan disusun oleh:

DIAN PUTRI PANGESTU

24010119130108

Telah dipertahankan di depan Tim Penguji

pada tanggal 18 Januari 2024

Susunan Tim Penguji

Pembimbing II/Penguji,	Penguji,
Abdul Aziz, S.Si., M.Sc.	Solikhin, S.Si., M.Sc.
NIP. 198502062015041003	NIP. 198506302012121001

Mengetahui,

Ketua Departemen Matematika,	Pembimbing I/Penguji,
Dr. Susilo Hariyanto, S.Si., M.Si.	Dr. Nikken Prima Puspita, S.Si., M.Sc.
NIP. 197410142000121001	NIP. 198604132009122007

ABSTRAK

KOMBINASI KRIPTOGRAFI KURVA ELIPTIK ATAS LAPANGAN BERHINGGA DAN MASALAH *KNAPSACK*

oleh

Dian Putri Pangestu

24010119130108

Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika untuk menjaga keamanan suatu pesan. Pada kriptografi terdapat dua jenis kunci, yaitu algoritma kunci simetri yang hanya memiliki satu kunci (pada proses enkripsi dan dekripsi) dan algoritma kunci publik yang memiliki dua kunci berbeda (pada proses enkripsi dan dekripsi). Algoritma kunci publik memiliki tingkat keamanan yang lebih kuat dibandingkan dengan algoritma kunci simetri. Pada Tugas Akhir ini membahas tentang proses enkripsi dan dekripsi menggunakan algoritma kunci publik, yaitu algoritma kriptografi kurva eliptik atas lapangan berhingga dan masalah *knapsack*. Sebelum dienkripsi, pesan asli dikonversi ke dalam bilangan *ASCII*. Pesan yang sudah dikonversi ke dalam bilangan *ASCII* dienkripsi menjadi suatu titik di dalam grup eliptik. Setelah pesan dienkripsi menggunakan algoritma kriptografi kurva eliptik, pesan dienkripsi kembali menggunakan algoritma masalah *knapsack* untuk mendapatkan titik yang baru. Pesan yang sudah terenkripsi disebut cipherteks. Sebaliknya, pada proses dekripsi cipherteks didekripsi menggunakan algoritma masalah *knapsack*. Kemudian, pesan didekripsi kembali menggunakan algoritma kriptografi kurva eliptik sedemikian sehingga diperoleh pesan asli dengan bantuan tabel *ASCII*.

Kata kunci : Kriptografi, kurva eliptik, masalah knapsack, enkripsi, dekripsi.

ABSTRACT

THE COMBINATION OF ELLIPTIC CURVE CRYPTOGRAPHY OVER FINITE FIELD AND KNAPSACK PROBLEM

by

Dian Putri Pangestu

24010119130108

Cryptography is the mathematical techniques to maintain the security of a data. In cryptography, there are two types of keys, namely symmetric key algorithms that only have one key (in the encryption and decryption process) and public key algorithms that have two different keys (in the encryption and decryption process). Public key algorithms have a stronger security level than symmetric key algorithms. This undergraduate discusses the encryption and decryption process using elliptic curve cryptography algorithm over finite field and knapsack problem algorithm. Before encryption, the original message is convert into ASCII numbers. The messages that has been converted into ASCII numbers are encrypted into a point in the elliptic group. After the messages are encrypted using the elliptic curve cryptography, the messages are encrypted again using the Knapsack problem algorithm to get a new point. The encrypted message is called the ciphertext. In the decryption process, the ciphertext are decrypted using the knapsack problem algorithm. Moreover, the messages are decrypted again using the elliptic curve cryptography such that the original message is obtained with the ASCII table.

Keyword : Cryptography, elliptic curve, knapsack problem, encryption, decryption.