Mohamad Ivan Janitra, 2014, **Kripografi Kurva Eliptik Elgamal dengan *One Time Pad* (OTP) pada Pesan Teks**. Skripsi ini dibawah bimbingan Drs. Edi Winarko, M.Cs. dan Auli Damayanti, S.Si., M.Si., Departemen Matematika, Fakultas Sains dan Teknologi, Universitas Airlangga, Surabaya.

ABSTRAK

Seiring dengan perkembangan teknologi komunikasi, banyak pekerjaan dapat diselesaikan dengan cepat dan efisien**.** Namun tidak semua perkembangan teknologi komunikasi memberikan dampak positif bagi penggunanya. Dampak negatif yang dapat terjadi adalah penyadapan dan pencurian data. Data atau informasi tersebut dapat berupa teks, gambar, atau video. Data dapat dengan mudah diganti, dimanipulasi, hilang, disalin, atau disalahgunakan. Masalah keamanan data atau informasi tersebut dapat diatasi dengan menggunakan kriptografi. Penulisan pada penelitian ini bertujuan untuk mengetahui proses keamanan menggunakan dua algoritma kriptografi yaitu kurva eliptik elgamal dan *One Time Pad* (OTP). Kriptografi kurva eliptik merupakan algoritma kunci publik berdasarkan pada teori kurva eliptik yang dapat digunakan untuk membuat kunci kriptografi yang lebih cepat, kecil, dan lebih efisien. *One Time Pad* (OTP) merupakan sistem dengan kunci acak hanya digunakan sekali untuk proses enkripsi yang kemudian didekripsi menggunakan kunci yang sama. Proses keamanan dimulai dengan representasi titik, pilih kunci privat dan bangkitkan kunci privat, masukkan pesan teks, enkripsi menggunakan kurva eliptik elgamal, bangkitkan kunci *pad* sepanjang hasil enkripsi kurva eliptik elgamal, enkripsi menggunakan OTP, untuk proses dekripsi diawali dengan menggunakan OTP dan dilanjutkan dengan kurva eliptik elgamal. Berdasarkan hasil pengujian yang telah dicapai, didapatkan bahwa hasil enkripsi dan dekripsi dengan kurva eliptik elgamal dan OTP dengan menggunakan *software* NetBeans IDE 8.2 berhasil mengubah bentuk pesan teks (*plaintext*) menjadi ciperteks yaitu pesan yang tidak dapat dibaca/dipahami, dan dapat diubah kembali menjadi bentuk pesan teks awal.

Kata Kunci : Pesan Teks, Kriptografi Kurva Eliptik Elgamal, *One Time Pad*, Java

Mohamad Ivan Janitra, 2014**, Elgamal Elliptic Curve Cryptography with One Time Pad (OTP) in Text Messages**. This final project is guided by Drs. Edi Winarko, M.Cs. and Auli Damayanti, S.Si., M.Si., Department of Mathematics, Faculty of Science and Technology, Airlangga University, Surabaya.

ABSTRACT

Along with the development of communication technology, many jobs can be completed quickly and efficiently. But not all the developments in communication technology have a positive impact. The negative impact that can occur is tapping and data theft. The data or information can be in the form of text, images, or video. Data can be easily replaced, manipulated, lost, copied, or even misused. Data or information security problems can be overcome by using cryptography. The writing of this paper aims to determine the security process using two cryptographic algorithms namely elliptic curve elgamal and one time pad. Ellitpic Curve Cryptography (ECC) is a public key algorithm based on elliptic curve theory that can be used to create cryptographic keys that are faster, smaller, and more efficient. One Time Pad (OTP) is a system where a randomly generated private key is only used once to encrypt messages which is decrypted by the recipient using a matching pad and key once. The security process begins with a point representation, generates a private key pair and a public key, enter a message, encrypts with elgamal elliptic curve, generate a key of the same length as the result of elgamal elliptic curve , encrypt with One Time Pad, the decryption process begins by using OTP and continued with the elgamal elliptic curve. Based on the test results that have been achieved, it was found that the results of encryption and decryption with elgamal elliptic curve and OTP using NetBeans IDE 8.2 software successfully changed the form of text messages (plaintext) become ciphertext, which can be changed back to the original text messages form.

Keywords : Text message, Elgamal Elliptic Curve Cryptography, One Time Pad, Java