

## **PENERAPAN TEORI CHAOS PADA KRIPTOGRAFI MENGGUNAKAN ALGORITMA STREAM CIPHER DAN ELECTRONIC CODE BOOK (ECB) UNTUK KEAMANAN PESAN TEKS**

**ERVYN YOGA INDRA KURNIAWAN**

*Program Studi Teknik Informatika - S1, Fakultas Ilmu  
Komputer, Universitas Dian Nuswantoro Semarang*

*URL : <http://dinus.ac.id/>*

*Email : 111201005658@mhs.dinus.ac.id*

### **ABSTRAK**

Masalah keamanan merupakan salah satu aspek terpenting dalam sistem informasi. Dalam komunikasi pasti akan ada pengiriman pesan kepada orang lain, maka tentunya pesan tersebut harus sampai dengan aman. Sebuah informasi umumnya hanya ditunjukkan bagi golongan tertentu, sangatlah penting untuk mencegah agar keamanan pesan tidak sampai jatuh kepada pihak-pihak lain yang tidak berkepentingan. Untuk mengurangi tindak kejahatan dalam keamanan data, maka kriptografi bisa dijadikan solusi yang tepat. Dalam penelitian ini, teori Chaos dengan Logistic Map akan digunakan untuk membangkitkan kunci secara acak dan panjang. Kemudian kunci tersebut diterapkan pada algoritma Stream Cipher dan Electronic Code Book (ECB). Dengan teori Chaos tersebut, akan dihasilkan kunci yang acak dan panjang kunci sama dengan panjang plainteks pada Stream Cipher. Sedangkan pada ECB akan menambah jumlah panjang kunci yang acak sehingga dapat menutup kelemahan. Dari hasil penelitian ini, teori Chaos dengan Logistic Map dapat mempermudah dalam mengingat kunci yang acak dan sekaligus panjang. Selain itu penelitian ini juga mengembangkan pada nomor iterasi tertentu yang dihasilkan oleh Logistic Map dapat dipilih menjadi nomor iterasi pertama kunci sehingga dalam pembangkitan kunci akan menambah variasi dan kemungkinan dalam penebakan kunci.

Kata Kunci : kriptografi, chaos, logistic map, pembangkit kunci, stream cipher, electronic code book

## **CHAOS THEORY CRYPTOGRAPHY USING STREAM CIPHER ALGORITHM AND ELECTRONIC CODE BOOK (ECB) FOR SECURING TEXT MESSAGE**

**ERVYN YOGA INDRA KURNIAWAN**

*Program Studi Teknik Informatika - S1, Fakultas Ilmu*

*Komputer, Universitas Dian Nuswantoro Semarang*

*URL : <http://dinus.ac.id/>*

*Email : 111201005658@mhs.dinus.ac.id*

### **ABSTRACT**

Security problem is one of many important aspect in information system. In communications will be message sending to another people. So, definitely those message must arrive safely. An information generally should only be shown for certain people, it is very important to prevent message's security to fall to the wrong hands. To lessen criminal activity within data security, so cryptography can be use as the right solution. In this research, Chaos theory with logistic Map will be use to generate keys randomly and long. Then those keys implemented to Stream Cipher algorithm and Electronic Code Book (ECB). With these Chaos theory, random keys will be generated and key's length will be same with the plaintext in Stream Cipher. While in ECB, a random key's length will be added so weakness can be covered. From this research's result, Chaos theory with Logistic Map can make remembering random and long keys easier. Other than that, this research also developing in some certain iteration number which was generated by Logistic Map can be chosen as key's first iteration number, so in keys generation, variation and possibility in keys guessing will be increased.

**Keyword** : cryptography, chaos, logistic map, generate key, stream cipher, electronic code book