

IMPLEMENTASI ALGORITMA RC4 DAN MODE ELECTRONIC CODE BOOK (ECB) PADA PENGAMANAN CITRA DIGITAL

ARIS MULYASANI

(Pembimbing : T. Sutojo, S.Si, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201207113@mhs.dinus.ac.id

ABSTRAK

Penggunaan media gambar sebagai media komunikasi saat ini memang sedang sangat diminati karena dari sebuah gambar dapat menjelaskan semua hal yang akan diinformasikan kepada semua orang ataupun beberapa orang tertentu, oleh sebab itu media gambar dipilih sebagai media komunikasi karena media gambar sangat mudah untuk dipahami. tingginya minat tersebut berdampak positif terhadap para pelaku usaha di dunia desain, fotografi dll, namun tidak semua hal akan berdampak baik saja, pasti akan ada dampak buruknya juga, dampak buruk dalam hal ini juga berhubungan dengan kemajuan teknologi yang memberikan kemudahan dalam segala hal, salah satu contohnya kemudahan dalam memanipulasi gambar dan pencurian file gambar. Ilmu yang mempelajari cara mengamankan suatu informasi salah satunya adalah Kriptografi. Konsep dari kriptografi yaitu Mengubah pesan menjadi bentuk lain yang disamarkan agar tidak dikenali dan proses mengembalikan ciphertext(pesan tersamarkan) menjadi plaintext(pesan asli) dengan menggunakan kunci sebagai parameter pada proses enkripsi dan dekripsi. Algoritma kriptografi RC4 menggunakan metode enkripsi yang dilakukan dilakukan per karakter 1 byte untuk sekali operasi sehingga Algoritma RC4 dinilai lebih sederhana dan mudah diimplementasikan, RC4 juga salah satu chiper yang sering digunakan di internet untuk pengaman SSL/TLS. Mode ECB merupakan mode yang paling sederhana. ECB beroperasi dengan memecah teks asli menjadi blok-blok sesuai dengan ukuran blok sistem penyandian yang kemudian setiap blok akan disandikan dengan kunci dan algoritma enkripsi yang sama.

Kata Kunci : citra digital, kriptografi, RC4, Mode ECB

IMPLEMENTATION OF RC4 ALGORITHM AND ELECTRONIC CODE BOOK (ECB) MODE FOR DIGITAL IMAGE SECURITY

ARIS MULYASANI

(Lecturer : T. Sutojo, S.Si, M.Kom)

*Bachelor of Informatics Engineering - S1, Faculty of Computer
Science, DINUS University*

www.dinus.ac.id

Email : 111201207113@mhs.dinus.ac.id

ABSTRACT

The use of media images as a medium of communication at this time is very attractive because of a picture can explain all the things that will be communicated to all people or certain people, therefore, the media image is selected as a medium of communication since the media image is very easy to understand. the high interest of the positive impact on businesses in the world of design, photography, etc., but not all of it will have an impact okay, definitely there will be bad effects as well, the adverse effects in this case also relates to advances in technology that provides convenience in every respect, one an example of the ease in manipulating images and image file theft. The study of how secure the information one is cryptography. The concept of cryptography that is Changing the message into another form that is disguised to avoid being recognized and the process of restoring the ciphertext (the message obscured) into plaintext (original message) by using the key as a parameter to the encryption and decryption proces. The RC4 cryptographic algorithm uses an encryption method that is done is done one byte per character for all operations so that the RC4 algorithm assessed more simple and easy to implement, is also one of the RC4 ciphers that is often used on the Internet for security SSL / TLS. ECB mode is a mode that Palin is simple. ECB operates by breaking the original text into blocks according to the block size encoding system which then each block is encrypted with a key and the same encryption algorithm.

Keyword : digital image, cryptography, RC4, Mode ECB