

IMPLEMENTASI KRIPTOGRAFI PADA FILE DOKUMEN MENGUNAKAN KOMBINASI ALGORITMA SHIFT CIPHER DAN RSA

ADITIA WANDHA RISTANTO

(Pembimbing : L.Budi Handoko, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201206959@mhs.dinus.ac.id

ABSTRAK

Internet pada era ini berfungsi sebagai penghantar informasi yang digunakan dalam segala aspek bidang kehidupan. Informasi yang didistribusikan berupa informasi dalam bentuk digital. Bagi pelaku usaha, informasi dalam bentuk digital mampu meningkatkan daya saing pasar dan memperluas distribusi barang maupun jasa. Bagi militer, kekurangan informasi dapat dijadikan penentu dalam kekalahan perang. Bagi wartawan, informasi memiliki daya jual dengan nilai yang tinggi. Bagi perorangan, informasi menjadi sesuatu yang sangat pribadi. Pentingnya informasi tersebut dijadikan sasaran dari beberapa orang yang tidak bertanggung jawab, seperti kasus penjualan informasi ilegal di pasar gelap yang dilakukan oleh cracker. Oleh karena itu, keamanan data merupakan sesuatu hal yang wajib dijaga dengan baik. Data yang disimpan atau didistribusikan dapat dilindungi dengan cara kriptografi. Kriptografi adalah teknik untuk menyandikan pesan. Teknik tersebut diimplementasikan dalam Bahasa pemrograman JAVA dan dibuat menggunakan kombinasi Algoritma Shift cipher dan RSA. Hasil yang didapatkan dari proses penyandian tersebut adalah data yang teracak atau tersandikan, data tersebut tidak dapat dipahami oleh pihak yang tidak memiliki kunci untuk melakukan dekripsi ulang pesan tersebut.

Kata Kunci : keamanan data, kriptografi, enkripsi, dekripsi, shift cipher, RSA

CRYPTOGRAPHIC IMPLEMENTATION ON DOCUMENT FILE USING SHIFT CIPHER AND RSA ALGORITHM

ADITIA WANDHA RISTANTO

(Lecturer : L.Budi Handoko, M.Kom)

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

www.dinus.ac.id

Email : 111201206959@mhs.dinus.ac.id

ABSTRACT

The Internet in information era used to be conductor information in all aspects of the life. The information is distributed in the form of digital information. For businesses, the information in digital form can improve market competitiveness and expand the distribution of goods and services. For the military, lack of information can be decisive in the defeat of the war. For journalists, the information has selling power with high value. For individuals, the information to be something very personal. The importance of such information was targeted from some people who are not responsible, such as the case of the sale of illegal information on the black market conducted by crackers. Therefore, data security is something that must be maintained properly. The data stored or distributed can be protected by cryptographic means. Cryptography is a technique for encrypting messages. The technique is implemented in JAVA programming language and created using a combination of Shift cipher and RSA Algorithm. Results obtained from the encryption process is data that is scrambled or encrypted, data can't be understood by those who do not have the key to decrypt the message.

Keyword : data security, cryptography, encryption, decryption, shift cipher, RSA