

IMPLEMENTASI ALGORITMA DATA ENCRYPTION STANDARD UNTUK PENGAMANAN TEKS

SATRIO WAHYU SETYARSANTO

(Pembimbing : Aris Marjuni, S.Si, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201206851@mhs.dinus.ac.id

ABSTRAK

Penyimpanan data pada media penyimpanan digital semakin banyak dilakukan oleh instansi pemerintahan maupun perusahaan swasta. Banyak dari data tersebut digunakan untuk mengambil suatu kebijakan bagi suatu perusahaan ataupun pada instansi pemerintahan. Beberapa instansi pemerintahan masih menyimpan data tersebut tanpa diamankan sehingga rentan untuk diserang atau diakse oleh pihak yang tidak mempunyai otoritas. Kriptografi merupakan cabang ilmu yang berkonsentrasi dalam pengamanan sebuah file ataupun sistem dengan menggunakan algoritma tertentu, salah satu algoritma kriptografi yaitu Data Encryption Standard dimana algoritma tersebut merupakan algoritma simetris dan menggunakan beberapa kali permutasi serta menggunakan S-Box didalamnya. Bruteforce merupakan serangan yang umum dilakukan terhadap keamanan system dimana bruteforce melakukan percobaan semua kemungkinan kunci yang digunakan untuk mengamankan suatu system atau data.

Kata Kunci : Kriptografi , Data , Data Encryption Standard , S-Box , Bruteforce

DATA ENCRYPTION STANDARD ALGORITHM IMPLEMENTATION FOR TEXT SECURITY

SATRIO WAHYU SETYARSANTO

(Lecturer : Aris Marjuni, S.Si, M.Kom)

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

www.dinus.ac.id

Email : 111201206851@mhs.dinus.ac.id

ABSTRACT

Data storage on digital storage media increasingly carried out by government agencies and private companies. Much of the data used to take a policy for a corporation or the government agency. Some government agencies still save the data without secured so vulnerable to attack or accessed by parties who do not have authority. Cryptography is a branch of science that is concentrating on securing a system or file by using a specific algorithm, a cryptographic algorithm is the Data Encryption Standard algorithm which is a symmetric algorithm and uses several times permutation and using S-Box. Bruteforce is a common attack against the security system where Bruteforce experiment all possible keys used to secure a system or data.

Keyword : Cryptography, Data, Data Encryption Standard, S-Box, Bruteforce