

APPLICATION OF *BRUTE FORCE* ALGORITHM IN ENCRYPTION DATA GUESSING USING *MD5* METHOD

BY

KIKI DIAH WULANDARI

Data security and confidentiality are important aspects in information systems and digital data. Data that contains important information must be kept safe and confidential. Password is one of the important keys for the security information. The password is a determinant for the security data that used to verify its identity in using certain services. Encryption Message Digest5 (MD5) is the process of randomizing passwords. The original messages from the data cannot be read by others. Brute Force Algorithm is an algorithm that can be used to guess passwords which encrypted with MD5. The guessing process is done by encrypting thousands of strings to MD5 so that it gets the same string. Strings are the result of guessed data. This research successfully applied the Brute Force algorithm to encrypt the encrypted data with MD5 method. The result is a utility that can guess passwords number of 1-8 digits and lowercase letters by 1-16 digits.

Keywords: *Algorithme Brute Force, Message Digest 5, MD5, Password, Encryption.*

ABSTRAK

PENERAPAN ALGORITMA BRUTE FORCE PADA PENEBAKAN DATA YANG DIENKRIPSI DENGAN METODE MD5

OLEH

KIKI DIAH WULANDARI

Keamanan dan kerahasiaan data merupakan aspek yang penting dalam sebuah sistem informasi dan data digital. Data yang berisi informasi penting harus dijaga keamanan dan kerahasiaannya. *Password* merupakan salah satu kunci penting dalam keamanan suatu informasi. *Password* menjadi penentu sebuah kemanan data yang digunakan untuk memverifikasi identitasnya dalam menggunakan layanan tertentu. Enkripsi *Message Digest5 (MD5)* adalah proses pengacakan *password* agar pesan asli dari data tersebut tidak dapat dibaca oleh orang lain. Algoritma *Brute Force* merupakan algoritma yang dapat digunakan untuk menebak *password* yang dienkripsi dengan *MD5*. Penebakan yang dilakukan menggunakan algoritma ini adalah dengan cara mengenkripsi ribuan string kedalam *MD5* sehingga didapatkan string yang sama. String tersebut merupakan hasil dari penebakan data. Penelitian ini berhasil menerapkan algoritma *Brute Force* pada penebakan data yang dienkripsi dengan metode *MD5*. Hasilnya adalah sebuah utility yang dapat menebak *password* berupa angka sebanyak 1-8 digit dan huruf kecil sebanyak 1-16 digit.

Kata Kunci:Algoritma *Brute Force*, *Message Digest5*, *MD5*, *Password*, Enkripsi.