Perancangan kriptografi teks menggunakan improvisasi sandi caesar = Text cryptography design using improved caesar code

Albertus Ageng Pratama, author

Abstrak

ABSTRAK
Sandi Caesar merupakan salah satu algoritma kriptografi tertua didunia. Motode yang dimiliki sangat dasar dan sederhana sehingga mudah untuk ditembus. Peningkatan keamanan algoritma disusun dengan memberikan pergeseran angka yang bervariasi serta menggunakan karakter ASCII. Variasi nilai k dinamakan sebagai Countdown yang artinya nilai k menurun hingga k bernilai 1. Kunci Countdown diperoleh melalui panjang masukan. Pengujian dilakukan pada kecepatan dan tingkat keamanan kriptografi. Pada kecepatan keseluruhan proses kriptografi yang paling cepat dimiliki oleh sandi Caesar pada setiap nilai n masukan yaitu masing masing sebesar 22, 38, dan 234 Î¼s. Pada n bernilai 1000 dan 10000, pengembangan algoritma memiliki perbedaan kecepatan yang kecil yaitu sebesar 1 dan 13 Î¼s. Keamanan kriptografi diuji menggunakan uji kerandoman NIST dengan 3 metode yaitu Uji Frekuensi Monobit, Uji Frekuensi Monobit dalam Suatu Blok, dan Uji Runs. Pada uji frekuensi monobit, terdapat 22 barisan random dari 30 plaintext yang diujikan sedangkan ciphertext memiliki 25 barisan random. Pada uji frekuensi dalam suatu blok, terdapat 24 barisan random dari 30 plaintext yang diujikan sedangkan ciphertext memiliki 25 barisan random. Pada uji runs, 24 dari 30 pengujian plaintext disimpulkan bahwa barisan terseebut adalah random. Setelah diujiakan pada ciphertext, didapatkan bahwa 23 dari 30 pengujian merupakan barisan random.
<hr>
ABSTRACT
Caesar password is one of the oldest cryptographic algorithms in the world. The method you have is very basic and simple so it's easy to penetrate. Improved security algorithms are arranged by giving a varying number of shifts and using ASCII characters. Variations in the value of k are called Countdown, which means the value of k decreases to k value 1. The Countdown key is obtained through input length. Tests are carried out at the speed and level of cryptographic security. At the speed of the entire cryptographic process, the fastest is owned by the Caesar password on each input n value, which is 22, 38, and 234 Î¼s respectively. In n values of 1000 and 10000, the development of algorithms has a small difference in speed which is equal to 1 and 13 Î¼s. Cryptographic security was tested using the NIST standard test with 3 methods namely the The Frequency (Monobit) Test, Frequency Test within a Block, and Runs Test. In the monobit frequency test, there were 22 random rows of 30 plaintexts tested while the ciphertext had 25 random sequences. In the frequency test in a block, there are 24 random rows of 30 plaintexts tested while the ciphertext has 25 random rows. In the runs test, 24 of the 30 plaintext tests concluded that the sequence was random. After testing the ciphertext, it was found that 23 of the 30 tests were random sequences.</p>