Uji Ketahanan Algoritma AES 256-bit dan Algoritma RSA Menggunakan Metode Brute Force Attack Serta Membandingkan Nilai Avalanche Effect

MUHAMMAD FARDAN FAUZAN
(Pembimbing : Aisyatul Karima, S.Kom, MCS)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201307707@mhs.dinus.ac.id

ABSTRAK

Penelitian uji ketahanan algoritma enkripsi AES (Advanced Encryption Standard) dan RSA (Rivest Shamir Adleman) menggunakan metode brute force attack serta menghitung nilai avalanche effect merupakan aspek yang perlu dilakukan. Penelitian terdahulu hanya menguji dengan menggunakan brute force attack sehingga hasil yang didapat hanya sebuah prediksi dan tidak pasti, maka tujuan penelitian ini adalah untuk menguji ketahanan algoritma AES 256-bit dan RSA dengan menggunakan perhitungan nilai avalanche effect. Langkah pengujian dengan melakukan 2 cara yaitu pengujian brute force attack, dan pengujian dengan nilai avalanche effect. Setelah diuji didapatkan waktu rata-rata prediksi brute force attack AES 256-bit 3.809 x ?10?^36 tahun dan rata-rata prediksi waktu untuk RSA 3,937 x ?10?^68 tahun, adapun untuk nilai avalanche effect AES 256-bit lebih baik dibandingkan RSA, dengan rata-rata AES 256-bit 39,85 % sedangkan RSA 23,68%.

Kata Kunci : Brute Force Attack, Kriptografi, AES, RSA, Avalanche Effect

Robustness Test of AES 256-bit Algorithm and RSA Using Brute Force Attack Method And Compare The Value Of Avalanche Effect

MUHAMMAD FARDAN FAUZAN
(Lecturer : Aisyatul Karima, S.Kom, MCS)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201307707@mhs.dinus.ac.id

ABSTRACT

The research of AES encryption algorithm (Advanced Encryption Standard) and RSA (Rivest Shamir Adleman) endurance test using brute force attack method and calculating valanche effect value are the aspects that need to be done. Previous research is only tested by using brute force attack so that the results obtained only a prediction and uncertain, Then the purpose of this research was to test the robustness of AES 256-bit algorithm and RSA by using the calculation of avalanche effect, itâ€™s can be tested by brute force attack and calculate the percentage of avalanche effect. After has been tested , then obtained by the average of brute force attack prediction time of AES 256-bit is 3,809 x ?10?^36 years and the average of predictive time for RSA 3,937 x ?10?^68 years, as for the percentage of avalanche effect for AES 256-bit is better than RSA, with an average of AES 256-bit 39.85% and whilst RSA 23.68%.

Keyword : : Brute Force Attack, Kriptografi, AES, RSA, Avalanche Effect