IMPLEMENTASI PENGAMANAN PESAN BERTIPE TEKS MENGGUNAKAN ALGORITMA ONE TIME PAD DENGAN PEMBANGKIT KUNCI BLUM BLUM SHUB YANG TELAH DIVARIASI

Ardea Yoga Oktarya Gamma[1], Aisyatul Karima[2]
[1,2] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11, Semarang, Jawa Tengah 50131 - (024) 3517261
E-mail : ardeayg99r@gmail.com[1], aisyatul.karima@gmail.com[2]

Abstrak

Seiring perkembangan zaman, kegiatan menyimpan data dan informasi dalam bentuk digital memiliki banyak resiko. Diantaranya terdapat resiko keamanan yang merupakan salah satu aspek terpenting dalam sistem. Untuk mengurangi tindak kejahatan yang terkait dengan keamanan data, maka kriptografi dapat dijadikan salah satu solusi. Teknik Blum Blum Shub sebagai pembangkit kunci diterapkan pada algoritma One Time Pad yang divariasi pada pesan bertipe teks pada penelitian nanti. One Time Pad merupakan algoritma cipher dengan persyaratan sebagai unbreakable cipher yang mewajibkan kunci harus acak, dan panjang kunci harus sama dengan plainteks yang dienkripsikan. Sehingga diperlukan algoritma pembangkit kunci untuk memudahkan mengingat kunci. Alasan teknik BBS sebagai pembangkit kunci pada algoritma OTP, karena BBS merupakan CSPRNG (Cryptographically Secure Pseudorandom Generator) yang tahan terhadap serangan serius dan teruji lolos uji keacakan statistik. Penelitian khusus untuk pesan bertipe teks, karena informasi berjenis teks banyak digunakan oleh masyarakat untuk berkomunikasi. Metode yang diusulkan meliputi pembangkitan kunci Blum Blum Shub, dan penerapan kunci pada algoritma One Time Pad. Kunci dari BBS menjadi pembahasan utama beserta variasi kunci menggunakan iterasi, dan wrapping. Hasil penelitian ini, menunjukan bahwa BBS mempermudah dalam mengingat kunci acak yang panjang, sehingga mampu mengatasi kelemahan algoritma OTP pada bagian kunci serta mampu memenuhi syarat unbreakable cipher.

Kata Kunci: *kriptografi, one time pad, blum blum shub, teks, pembangkit kunci*

Abstract

Along with the times, the activities of storing data and information in digital form has many risks. Among them there is a security risk is one of the most important aspects of the system. To reduce crime related to the security of the data, then cryptography can be one solution. Blum Blum Shub as key generation algorithm is applied to the One Time Pad is varied in type text messages on research later. One Time Pad is a cipher algorithm with an unbreakable cipher requirements which require keys to be random, and the key length should be the same as the plaintext encrypted. So, we need the key generation algorithm for easy recall key. BBS technical reasons as the key generation for OTP, because BBS is CSPRNG (Cryptographically Secure Pseudorandom Generator) which is resistant to a serious attack and passed the test of statistical randomness. Research specifically to type a text message, because the text-type information is widely used by people to communicate. The proposed method includes key generation Blum Blum Shub, and the key for One Time Pad. BBS into a discussion of the key and its lock using a variety of iterations, and wrapping. The results of this study, show that BBS easier to remember a long random key , so it can overcome the weaknesses of OTP algorithms on the key and be able to qualified unbreakable cipher.

Keywords: *cryptography, one time pad, blum blum shub, text, key generator*