Implementasi Pembangkit Kunci Aman Secara Kriptografi Berbasis RSA Pada Stream Cipher

LELA DAMARIS
(Pembimbing : Erna Zuni Astuti, M.Kom)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201106499@mhs.dinus.ac.id

ABSTRAK

Masalah keamanan merupakan salah satu aspek penting dalam sistem informasi. Dalam komunikasi pasti akan ada pertukaran informasi, maka tentunya pesan tersebut harus dapat didistribusikan dengan aman. Sebuah informasi umumnya hanya ditunjukan bagi golongan tertentu, sehingga sangatlah penting untuk menjamin keamanan pesan agar tidak sampai jatuh kepada pihak-pihak lain yang tidak berkepentingan. Untuk meningkatkan keamanan informasi, maka kriptografi bisa dijadikan solusi yang tepat. Dalam penelitian ini, algoritma CSPRNG RSA akan digunakan untuk membangkitkan kunci yang diperlukan secara acak. Kemudian kunci tersebut diterapkan pada algoritma Stream Cipher. Dengan algoritma CSPRNG RSA tersebut akan dihasilkan kunci yang acak dan sama panjang dengan plainteks pada Stream Cipher. Dari hasil penelitian ini, algoritma CSPRNG RSA dapat mempermudah dalam mengingat kunci yang acak dan sekaligus panjang. Selain itu juga mempermudah dalam distribusi kunci. Penelitian ini juga mengembangkan pada penambahan iterasi sehingga dalam pembangkitan kunci akan menambah variasi dan kemungkinan dalam penebakan kunci. Hasil penelitian menunjukan Algoritma CSPRNG RSA dapat diterapkan pada Stream Cipher dan berjalan dengan baik.

Kata Kunci : kriptografi, pembangkit kunci, CSPRNG, RSA, stream cipher.

IMPLEMENTATION OF SECURE KEY GENERATOR USING CRYPTOGRAPHY BASED ON RSA AT STREAM CIPHER

LELA DAMARIS
(Lecturer : Erna Zuni Astuti, M.Kom)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201106499@mhs.dinus.ac.id

ABSTRACT

A security issue is one of the important aspects of information systems. In communication definitely there will be an exchange of information, then surely the message must be distributed safely. An information generally only shown for certain groups, so it is important to ensure the safety of messages in order not going to the other who are not be concerned. To improve the security of information, then cryptography can be the right solution. In this study, CSPRNG RSA algorithm will be used to generate the necessary of random keys. Then the key is applied on Stream Cipher algorithm One Time Pad. CSPRNG RSA algorithm will generate a random key with the same length as plaintext on Stream Cipher One Time Pad. From these study results, the CSPRNG RSA algorithm simplifies to remember the key which is random and extensive. It also makes it easy for distribution. This study also developed in addition with iteration so it will add more variety and possibilities in key guessing. The result proves that CSPRNG RSA can be applied in Stream Cipher and work well.

Keyword : cryptography, key generator, CSPRNG, RSA, stream cipher