Perangkat Lunak Visualisasi Kriptografi Metode MMB (Modular Multiplication-based Block Cipher)

HARYO RASYID
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : haryorasyid@yahoo.com

ABSTRAK

Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data, sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak salah. Terdapat banyak sekali metode kriptografi yang dapat digunakan, salah satunya adalah MMB (Modular Multiplication-based Block cipher). Kriptografi metode MMB menggunakan plaintext 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang dapat dibalik. Substitusi ini ditentukan oleh sebuah operasi perkalian modulo 232 - 1 dengan faktor konstan. MMB menggunakan 32 bit subblock text (x0, x1, x2, x3) dan 32 bit subblock kunci (k0, k1, k2, k3). Sebuah fungsi non linier, f, diterapkan enam kali bersama dengan fungsi XOR. Kerumitan algoritma ini, yang terletak pada proses operasi perkalian modulo 232 - 1, perhitungan fungsi non linier f pada proses enkripsi dan dekripsi, serta operasi invers pada proses dekripsi, menyebabkan algoritma ini sulit diproses secara manual. Visualisasi perlu dilakukan agar mahasiswa lebih mudah memahami kriptografi metode MMB. Perangkat Lunak Visualisasi Kriptografi Metode MMB di bangun dengan menggunakan metode pengembangan Waterfall. Penelitian ini bertujuan menampilkan visualisasi yang baik supaya mahasiswa memahami Kriptografi Metode MMB melalui visualisasi. Dengan adanya perangkat lunak bantu pemahaman ini, maka mahasiswa dapat mempelajari metode kriptografi MMB secara tahap demi tahap.

Kata Kunci : Kriptografi, MMB (Modular Multiplication-based Block cipher), cipher block, enkripsi, dekripsi

Software Visualization Cryptography Methods MMB (Modular Multiplication-based Block Cipher)

HARYO RASYID
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : haryorasyid@yahoo.com

ABSTRACT

Cryptography aiming at maintaining the confidentiality of the information contained in the data, so that information cannot be known by the parties is not wrong. There are an awful lot of cryptographic methods that can be used, one of which is the MMB (Modular Multiplication-based Block cipher). Plaintext cryptographic methods using MMB 128 bit and iterative algorithm consists of linear measures (such as XOR and key applications) as well as parallel applications of the four major non-linear substitution can be reversed. This substitution is defined by an operation multiplication modulo 232 - 1 with a constant factor. MMB uses 32 bit subblock text (x0, x1, x2, x3) and 32 bit subblock keys (k0, k1, k2, k3). A non-linear function, f, applied six times along with the XOR function. The complexity of this algorithm, which is located on the process of the operation multiplication modulo 232 - 1, calculation of non-linear function f on the process of encryption and decryption, as well as the inverse operation on the process of decryption, cause this algorithm difficult to be processed manually. Visualization needs to be done in order for students to understand more easily the cryptographic methods of MMB. Visualization method of Cryptographic software in the wake of MMB by using methods of development of the Waterfall. This study aims at showing good visualization so that students understand the methods of Cryptography through visualization MMB. With this understanding of assistive software, students can learn the methods of cryptography in MMB step-by-step.

Keyword : Kriptografi, MMB (Modular Multiplication-based Block cipher), cipher block, enkripsi, dekripsi