INTISARI

SERANGAN KLEPTOGRAFI BERBASIS RASIO ARITMETIKA PADA SISTEM KRIPTOGRAFI RSA

Oleh

Amrul Fadhil Yofan

20/455491/PA/19706

Serangan kleptografi berbasis rasio aritmetika merupakan ancaman yang cukup serius bagi pengguna sistem kriptografi RSA. Dalam serangan ini, penyerang memanfaatkan kelemahan dalam proses pembuatan kunci publik dengan menyisipkan informasi tersembunyi yang hanya dapat diakses oleh penyerang. Serangan ini memanfaatkan beberapa sifat-sifat matematis sehingga terbentuk algoritma yang menerapkan pendekatan baru dalam merepresentasikan bilangan bulat. Pada skripsi ini, diberikan penjelasan lebih lanjut mengenai serangan kleptografi terhadap sistem kriptografi RSA. Skripsi ini dimulai dengan mendeskripsikan sistem kriptografi RSA berserta serangannya, lalu dilanjutkan dengan menjelaskan konsep kleptografi dan pintu belakang. Selanjutnya, diberikan pembahasan utama mengenai pendekatan rasio aritmetika dan penerapannya dalam serangan kleptografi pada RSA. Kemudian, dilakukan simulasi dan analisis perbandingan untuk melihat lama waktu jalannya algoritma kleptografi pada RSA.

ABSTRACT

ARITHMETIC RATIO BASED KLEPTOGRAPHIC ATTACK ON RSA CRYPTOSYSTEM

By

Amrul Fadhil Yofan

20/455491/PA/19706

Arithmetic ratio based kleptographic attacks pose a significant threat to users of RSA cryptographic systems. In this attack, the attacker exploits weaknesses in the public key generation process by embedding hidden information that can only be accessed by the attacker. This attack leverages several mathematical properties to create an algorithm that introduces a new approach to represent integers. This final project provides a more detailed explanation of kleptographic attacks on RSA cryptographic system. It begins by describing the RSA cryptographic system and its vulnerabilities, followed by an explanation of kleptography and backdoors. The main discussion focuses on the arithmetic ratio approach and its application in kleptographic attacks on RSA. Finally, simulations and comparative analyses are conducted to evaluate the execution time of the kleptographic algorithm on RSA.