

Perancangan dan Implementasi Algoritma *Block Cipher 256 bit* dengan Skema *P-Box* Berbasis Pembuatan Lumpia untuk Pengamanan SMS pada *Mobile Platform Android*

¹Ester Carolina Ambarsari, ²Yos Richard Beeh, ³Alz Danny Wowor

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Jl. Gn. Payung Dalam, Blotongan, Sidorejo, Kota Salatiga, Jawa Tengah 50715

Email: ¹672012139@student.uksw.edu, ²yos.fti.uksw@gmail.com,

³alzdanny.wowor@staff.uksw.edu

Abstract

The security of message needed to avoid the modification, inserting or removal some information before it is accepted by the receiver. Cryptography is one of the technic in security of message information that has purpose to solve the security's problem, confidentiality, originality and integrity of data until it is able to protect the information from hijacking. This study is aimed to designing and implementing of cryptography algorithm symmetric with the use of Permutation Box (P-Box) pattern making the Lumpia on Block Cipher 256 bit to secure the Short Message Service (SMS) on android mobile platform. The process of encryption can be done as many as 30 rotations with 4 processes in each rotation. The result of designing of cryptography algorithm is implied on SMS application that can help the user to secure the message.

Keyword: *Cryptography, Short Message Service (SMS), Pattern making the Lumpia*

Abstrak

Keamanan pesan diperlukan untuk menghindari adanya pengubahan, penyisipan, ataupun penghilangan sebagian informasi sebelum diterima oleh pihak yang berhak menerima. Kriptografi merupakan salah satu teknik dalam mengamankan informasi pesan yang bertujuan untuk menyelesaikan masalah keamanan, kerahasiaan, keaslian dan integritas data sehingga dapat menjaga informasi dari pihak yang tidak memiliki otoritas atau hak akses. Penelitian ini merancang dan mengimplementasikan algoritma kriptografi dengan menggunakan skema *Permutation Box* (P-Box) pola pembuatan Lumpia pada *Block Cipher 256 bit* untuk mengamankan SMS (*Short Message Service*) pada *mobile platform* android. Proses enkripsi dilakukan sebanyak 30 putaran dengan 4 proses pada setiap putarannya. Hasil dari perancangan algoritma kriptografi diimplementasikan pada aplikasi SMS yang dapat membantu *user* dalam mengamankan pesan teks.

Kata Kunci: Kriptografi, SMS (*Short Message Service*), Pola Pembuatan Lumpia

¹ Mahasiswa Fakultas Teknologi Informasi Program Studi Teknik Informatika, Universitas Kristen Satya Wacana Salatiga.

² Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga.

³ Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga.