

PENERAPAN ALGORITMA SKIPJACK DALAM SISTEM APLIKASI PENYANDIAN FILE GAMBAR DENGAN PYTHON

Ibrahim¹, M. Akbar², Usman Ependi³, Kurniati⁴

Universitas Bina Darma

Jalan Jendral A. Yani No. 12 Palembang

Email: ibrahimboem123@gmail.com¹, muhamad.akbar@binadarma.ac.id²,
u.ependi@binadarma.ac.id³, kurniati@binadarma.ac.id⁴

Abstract: Data security is a very important thing. Therefore, it is very important to pay attention to sending data to other parties. Modern cryptographic algorithms are made so complex that it is very difficult to solve ciphertext without knowing the key. Skipjack is one type of algorithm with data security methods developed by the National Security Agency (NSA) and published in 1998. (Kim J., 2009). The Skipjack algorithm has an 80-bit key, known as cryptovariable, to encrypt or decrypt 64-bit data blocks. Current information exchange is not only in the form of text / strings but also involves graphic objects such as photos, animations, banners, etc. Existing problems can be solved by the presence of steganography and cryptography. This is necessary to prevent information easily accessed by other parties that can violate the privacy of the owner.

Keywords: Skipjack Algorithm, Encoding, Image File, Python.

Abstrak: Keamanan data merupakan suatu hal yang sangat penting. Oleh karena itu, sangat penting untuk memperhatikan pengiriman data kepada pihak lainnya. Algoritma kriptografi modern dibuat sedemikian kompleks sehingga sangat sulit memecahkan *ciphertext* tanpa mengetahui kunci. Skipjack merupakan salah satu jenis dari algoritma dengan metode pengamanan data yang dikembangkan oleh *National Security Agency* (NSA) dan dipublikasikan pada 1998. (Kim J., 2009). Algoritma *Skipjack* memiliki kunci 80-bit yang dikenal sebagai *cryptovariable*, untuk mengenkripsi atau mendekripsi blok data 64-bit. Pertukaran informasi saat ini tidak hanya berupa teks/string melainkan juga melibatkan objek grafik misalnya foto, animasi, banner, dsb. Permasalahan yang ada dapat diselesaikan dengan adanya steganografi dan kriptografi. Hal tersebut diperlukan untuk mencegah informasi mudah diakses oleh pihak lain yang dapat melanggar privasi sang pemilik.

Kata kunci: Algoritma Skipjack, Penyandian, File Gambar, Python

1. Latar Belakang

Keamanan data merupakan suatu hal yang sangat penting. Oleh karena itu, sangat penting untuk memperhatikan pengiriman data ke lainnya. Mungkin kepada pihak yang dituju terjadi tidak sengaja ke tujuan yang salah. Oleh sebab itu, data tersebut terlindungi dari pihak yang tidak memiliki izin untuk membaca dan mengetahui isi dari data yang dikirimkan tersebut. Metode kriptografi, yaitu berubah bentuk teks benar (*plaintext*) menjadi teks acak (*ciphertext*). Algoritma kriptografi modern dibuat sedemikian kompleks

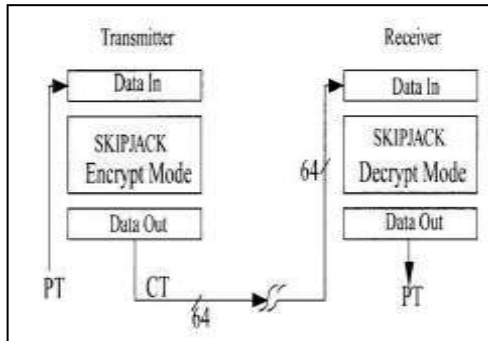
sehingga sangat sulit memecahkan *ciphertext* tanpa mengetahui kunci. Berdasarkan antara algoritma. *Skipjack* merupakan salah satu jenis dari algoritma simetri dengan metode pengamanan data yang dikembangkan oleh National Security Agency (NSA) dan dipublikasikan pada 1998. (Kim J., 2009).

Algoritma *Skipjack* memiliki kunci 80-bit yang dikenal sebagai *cryptovariable*, untuk mengenkripsi atau mendekripsi blok data 64-bit. Dalam proses enkripsi dan dekripsinya arti utama diputar sebanyak sehingga kombinasi dari 32 putaran tersebut membuat algoritma *Skipjack* memiliki

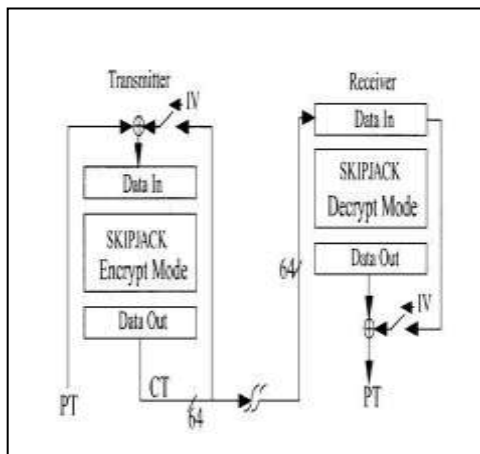
tingkat keamanan yang tinggi (Suprianto, 2007). Akan tetapi, algoritma *Skipjack* telah memiliki kriptanalisis (Granboulan, 2002) yang membuat pihak ketiga atau pihak yang

ingin melihat data dapat mengetahuinya. Dengan menggunakan algoritma *Skipjack*, maka keamanan pesan lebih terjamin.

2. METODOLOGI PENELITIAN



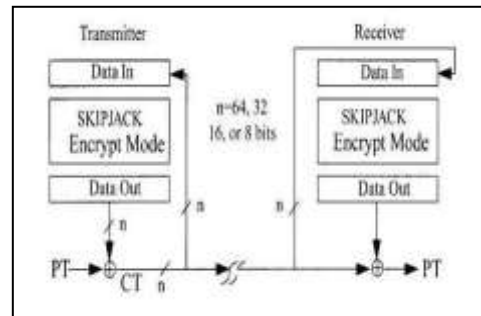
Gambar 2.1. Mode ECB



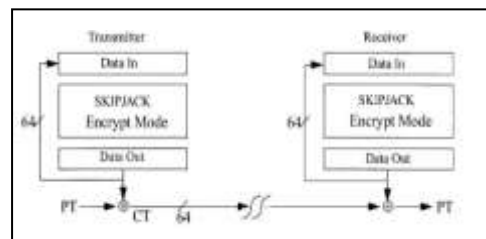
3. HASIL DAN PEMBAHASAN

Halaman utama merupakan halaman yang menampilkan menu-menu utama yang terdapat pada aplikasi. Pada halaman ini juga menampilkan menu Enkripsi Gambar dan Dekripsi Gambar yang masing-masing menggunakan algoritma Skipjack. Berikut adalah :

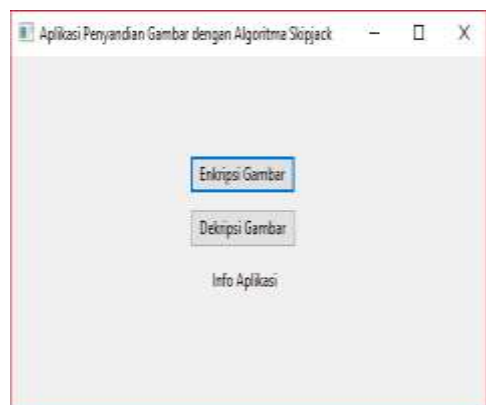
Gambar 2.2. Mode CBC
menambahkan beberapa dummy byte ke akhir file sebelum melakukan enkripsi.



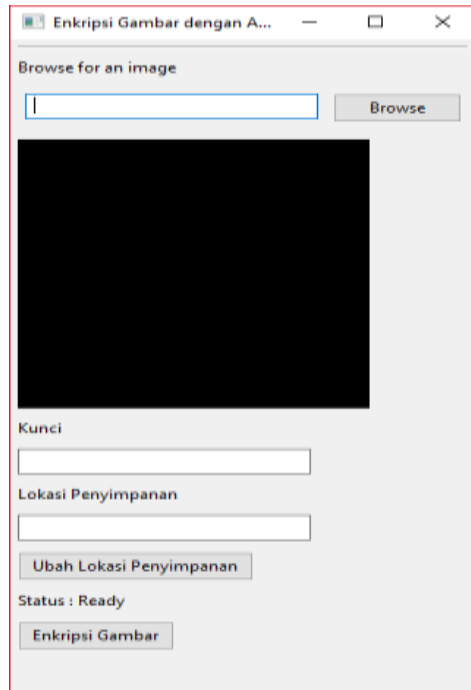
Gambar 2.3 Mode CFB



Gambar 2.4 Mode OFB



Gambar 4.1. Tampilan Halaman Utama



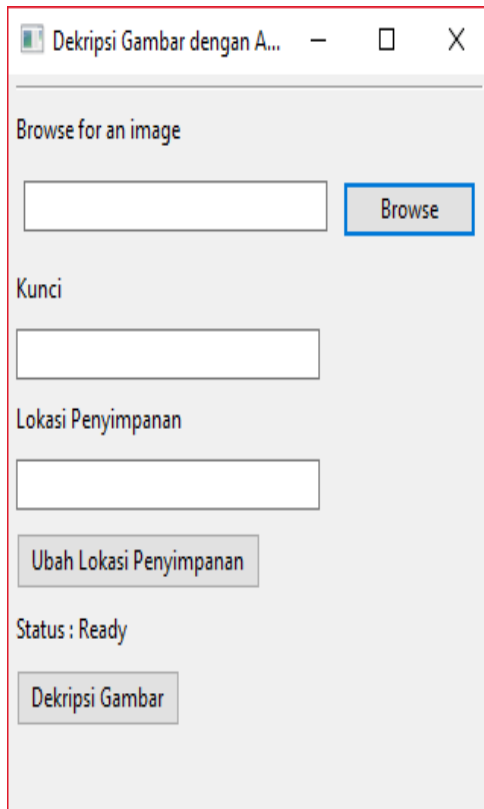
Gambar 4.2. Tampilan Halaman Enkripsi Gambar

Halaman enkripsi gambar berhasil merupakan rancangan setelah melakukan enkripsi gambar dengan Skipjack. Setelah pengguna dapat memilih gambar, memasukkan kunci dan menyimpan gambar maka status akan menampilkan bahwa enkripsi gambar berhasil. Berikut adalah tampilan halaman enkripsi gambar berhasil:

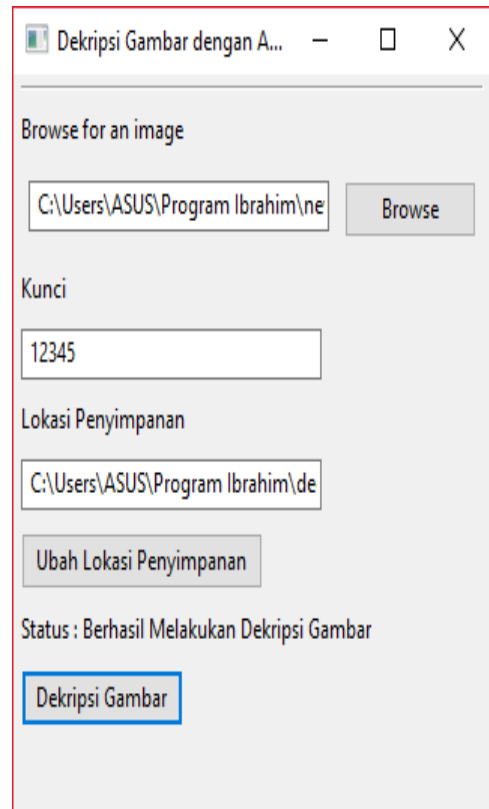


Gambar 4.3. Tampilan Halaman Enkripsi Gambar Berhasil

Halaman dekripsi gambar merupakan rancangan untuk melakukan dekripsi gambar dengan Skipjack. Pada halaman ini, pengguna dapat memilih gambar, memasukkan kunci dan menyimpan gambar, kemudian menekan tombol gambar dan melihat status dekripsi. Berikut adalah tampilan halaman dekripsi gambar:



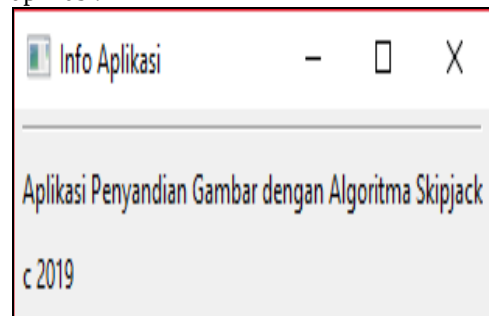
Gambar 4.4. Tampilan Halaman Dekripsi Gambar



Gambar 4.5. Tampilan Halaman Dekripsi Gambar Berhasil

Halaman dekripsi gambar berhasil merupakan rancangan setelah melakukan dekripsi gambar dengan Skipjack. Setelah pengguna dapat memilih gambar, memasukkan kunci dan menyimpan gambar maka status akan menampilkan bahwa dekripsi gambar berhasil. Berikut adalah tampilan halaman dekripsi gambar berhasil:

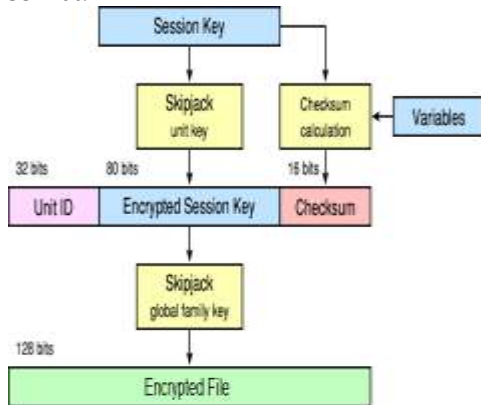
Halaman info aplikasi merupakan halaman yang menampilkan judul aplikasi disertai tahun pembuatannya dan logo aplikasi tersebut. Pada halaman ini, terdapat keterangan aplikasi yang telah dibuat. Berikut adalah tampilan halaman info aplikasi:



Gambar 4.6. Tampilan Halaman Info Aplikasi

4.3 Proses Enkripsi dan Dekripsi

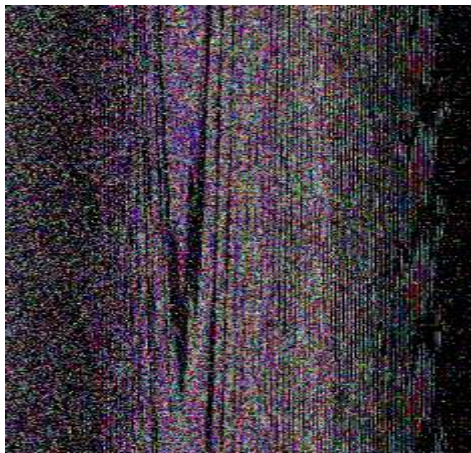
Cara kerja algoritma skipjack baik enkripsi maupun dekripsi adalah sebagai berikut:



Gambar 4.7. Cara Kerja Enkripsi Gambar

Dimulai dari session key yaitu ketika pengguna menekan tombol Enkripsi Gambar. Kemudian membuat Skipjack unit key dan diikuti perhitungan checksum yang diisi variable (pada form Kunci). Kemudian akan menjadi Skipjack global family key yang dimasukkan ke dalam file yang terenkripsi.

Berikut adalah perbandingan antara gambar yang setelah dienkripsi dan setelah didekripsi:



Gambar 4.8 Gambar bunga.png yang telah dienkripsi



Gambar 4.9 Gambar bunga.png yang telah didekripsi dan kembali ke bentuk asli



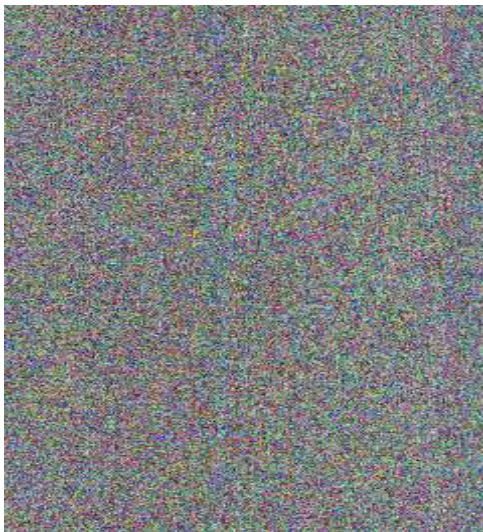
Gambar 4.10 Gambar bunga.png yang telah didekripsi



Gambar 4.11 Gambar bunga.png yang telah didekripsi dan kembali ke bentuk asli



Gambar 4.13 Gambar bunga.png yang telah didekripsi dan kembali ke bentuk asli



Gambar 4.12 Gambar bunga.png yang telah dienkrpsi

4. KESIMPULAN

:

1. Aplikasi penerapan algoritma *Skipjack* dalam sistem aplikasi penyandian gambar dengan *Phyton* ini membantu mengimplementasikan suatu sistem keamanan data gambar dengan algoritma *Skipjack*.
2. Aplikasi ini mempermudah pengguna mengakses penerapan algoritma *Skipjack* dalam sistem aplikasi penyandian gambar dengan *Phyton* dengan menggunakan metode pengembangan aplikasi *Prototype*.
3. Aplikasi ini dibangun untuk meningkatkan keamanan dokumen yang bersifat rahasia khususnya *file* grafik, dan dibuat dengan bahasa pemrograman *Python*.

DAFTAR PUSTAKA

- Hall, James. 2001. ” *Information System* ”
Yogyakarta : Salemba Empat.
- Kusrini. 2007. Konsep dan Aplikasi Sistem
Pendukung Keputusan. Jakarta:
Andi
- Pressman, R.S. (2010), *Software
Engineering: a practitioner's
approach*, McGraw - Hill, New
York,
- Sinaga, N. 2018. Penerapan Algoritma
Skipjack Untuk Menyandikan
Short Message Service. Medan:
STMIK Budidarma.
- Suprianto. 2007. Sistem Pengkodean Data
Pada File Teks Pada Keamanan
Informasi dengan Menggunakan
Metode Skipjack. Bandung:
STMIK Mardira Indonesia.
- Maria. 2014. *Metode pengembangan
Prototyping dalam
pengembangan*. Jakarta :
Anwar. (Tersedia :
<http://abhique.blogspot.com/2012/11/metode-prototyping-dalam-pengembangan.html>diakses2
Mei 2018)