IMPLEMENTASI ALGORITMA TWOFISH PADA KEAMANAN DATA BERBASIS APLIKASI ANDROID

Erfan Hasmin
Teknik Informatika, STMIK Dipanegara Makassar
e-mail: erfan.hasmin@dipanegara.ac.id

Abstrak

Penyalahgunaan data-data rahasia perusahaan tersebut oleh pihak tertentu tentunya bisa saja menimbulkan kerugian yang sangat besar pada perusahaan tersebut. Kemungkinan pihak lain untuk mencuri informasi yang disampaikan lewat komunikasi elektronik tersebut sangat besar mengingat belum adanya sekuritas khusus terhadap aplikasi tersebut. Karenanya, salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang tidak bermakna. Hal tersebut dapat dilakukan dalam kriptografi. Permasalahan tersebut dapat diatasi dengan proses enkripsi. Salah satu enkripsi yang cukup dikenal adalah dengan metode enkripsi twofish. Aplikasi enkripsi ini nantinya akan dibangun pada perangkat mobile berbasis Android sehingga diharapkan akan dapat memproteksi masyarakat yang mengirimkan file dan folder menggunakan perangkat mobile. Tujuan dari aplikasi ini adalah untuk menghasilkan file terenkripsi yang tetap aman saat file tersebut dikirim melalui perangkat android. Twofish merupakan salah satu algoritma yang diajukan untuk mengikuti program penetapan Advanced Encryption Standard (AES). Algoritma ini dirancang oleh Bruce Schneier. Meskipun algoritma ini tidak memenangkan program tersebut, namun tetap terdapat banyak kelebihan dengan prinsip kerja untuk menyandikan data sesuai dengan prinsip kriptografi. hasil penelitian ini membangun Aplikasi untuk keamanan file menggunakan metode enkripsi Algoritma Twofish. Hasil penelitian ini aplikasi yang dibangun dapat melakukan enkripsi dan dekripsi data ayng dikirim melalui perangkat android.

Kata kunci Enkripsi Data, Algoritma Twofish, Mobile, Android

1. PENDAHULUAN

Pada zaman sekarang ini, menjaga kerahasiaan informasi merupakan hal yang sangat penting. Sebagai contoh bagi perusahaan besar, penyimpanan dokumen serta data-data penting adalah kewajiban yang mesti dilakukan. Penyalahgunaan data-data rahasia perusahaan tersebut oleh pihak tertentu tentunya bisa saja menimbulkan kerugian yang sangat besar pada perusahaan tersebut. Contoh lainnya adalah komunikasi suara lewat jaringan internet. Kemungkinan pihak lain untuk mencuri informasi yang disampaikan lewat komunikasi elektronik tersebut sangat besar mengingat belum adanya sekuritas khusus terhadap aplikasi tersebut. Karenanya, salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang tidak bermakna. Hal tersebut dapat dilakukan dalam kriptografi.

Permasalahan tersebut dapat diatasi dengan proses enkripsi. Salah satu enkripsi yang cukup dikenal adalah dengan metode enkripsi twofish. Aplikasi enkripsi ini nantinya akan dibangun pada perangkat mobile berbasis Android sehingga diharapkan akan dapat memproteksi masyarakat yang mengirimkan file dan folder menggunakan perangkat mobile. Tujuan dari aplikasi ini adalah untuk menghasilkan file terenkripsi yang tetap aman saat file tersebut dikirim

melalui perangkat android, dikarenakan Pada penelitian saya sebelumnya telah berhasil membangun aplikasi enkripsi twofish yang dapat melakukan enkripsi file dan folder [1]

Twofish merupakan salah satu algoritma yang diajukan untuk mengikuti program penetapan Advanced Encryption Standard (AES) pada tahun 1997. Algoritma ini dirancang oleh Bruce Schneier. Meskipun algoritma ini tidak memenangkan program tersebut, namun tetap terdapat banyak kelebihan dengan prinsip kerja untuk menyandikan data sesuai dengan prinsip kriptografi. Penelitian tentang penerapan algoritma Twofish pada enkripsi dan dekripsi data text dan gambar dengan kunci berupa karakter sepanjang 128 bit (16 byte) dan fleksibilitas dalam panjang kunci yang dimasukkan, serta keluaran hexadecimal sebagai hasil enkripsi.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi masuk dalam kategori bidang ilmu dan seni dalam menjaga kerahasiaan berita. Selain yang diartikan tersebut dikatakan pula kriptografi ilmu yang mempelajari teknik-teknik matematika yang memiliki hubungan pada aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data , dan juga tahapan autentikasi data. Namun dikatakan tidak semua aspek keamanan informasi dapat ditangani oleh kriptografi. Terdapat empat tujuan penggunaan kriptogtafi [2].

1. Kerahasiaan , melindungi informasi data dari siapapun kecuali dari seorang yang telah diberi otoritasi kepada isi data tersebut
2. Integritas data , kesesuaian data jika mengalami perpindahan atau perubahan data
3. Autentikasi , proses mengidentifikasi pengirim dan penerima informasi data.
4. Penyangkalan , mencegah penyangkalan jika terjadi penyangkalan dari pengirim setelah mengirim informasi

Kriptografi dikenal dengan 2 modul yang digunakan untuk dapat dijadikan 1 aplikasi maupun sistem utuh, modul Enkripsi dimana mengubah data menjadi chipperText (hasil perubahan data yang tidak dapat dimengerti maknanya) , modul Deskripsi merupakan proses perubahan kembali Chippertext kembali menjadi data yang dapat dimengerti maknanya [3].

2.2 Algoritma Twofish

Algoritma twofish bermodel block chipper yang memiliki ukuran 128 bit .Berikut tahapan dalam Twofish.

1. Bit diinput sebagai P0, P1, P2, dan P3, P0 dan P1 akan menjadi sis kiri, dua lainnya akan menjadi masukan pada sis kanan.
2. Dilanjutkan pada proses whitening.
3. Sisi kiri akan menjadi inputan awal untuk fungsi f, P0 akan langsung diinput sebagi fungsi g, sementara P1 akan di-rotate 8-bit sebelum diproses lanjut oleh fungsi g .
4. Didalam fungsi g ini, bit-bit tersebut akan melalui hitungan S-box dan matriks didalam MDS, kemudian kedua keluaran akan digabungkan oleh PHT.
5. Setelah melalui PHT, kedua sisi bagian tersebut akan ditambah dengan bagian dari key sesuai dengan iterasi yang telah dilewati. Untuk hasil dari fungsi f dengan inputan P0 akan dimasukkan dengan K2r + 8. Untuk hasil dari fungsi f dengan input P1 akan ditambah dengan K2r + 9, dimana variabel r adalah jumlah perulangan yang telah di *miss*. Masing-

masing varibel ditambah delapan dan sembilan karena terdapat delapan urutan awal sudah digunakan untuk proses whiteningbaik input dan output.

6. Keluaran dari fungsi f dengan input P0 akan di-XORdengan P2, kemudian hasilXOR tersebut akan di-rotate1-bit.
7. Output dari fungsi f dengan input P1 akan di proses XOR dengan P3, namun P3 sebelumnya di rotasi dengan 1-bit dahulu.
8. Jika perhitungan bit selesai, hasil sisi kanan akan menjadi bagian sisi kiri , dan bagian sisi kiri yang belum terhitung akan berada bagian sisi kanan.
9. Setelah setelah 16 kali perulangan, akan dilakukan proses whitening kembali pada output. Whitening pada output akan mengembalikkan hasil pertukaran sisi kanan dan sisi kiri pada perulangan akhir, dan melakukan proses XOR data dengan menggunakan 4 bagian kunci.

Bagian kunci yang digunakan disini berbeda dengan bagian kunci yang digunakan saat whitening pada input. Oleh karena itu urutan bagian kunci yang dipakai ditambah empat, karena empat urutan bagian kunci satu sampai empat sudah terlebih dahulu digunakan untuk whitening pada input [4].

2. 3 Aplikasi Mobile

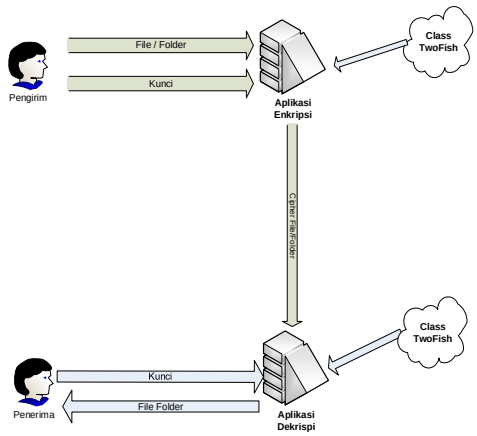
Peminat pengguna Android semakin tahun memperlihatkan semakin meningkat. Diketahui Android pertama kali dikembangkan oleh perusahaan bernama Android Inc. , dan pada tahun 2005 di ambil alih melalui oleh penyedia mesin pencari terbesar yaitu Google. Android berbasis kernel Linux yang telah dimodifikasi, dan untuk setiap kali mengeluarkan versi baru diberi kode nama berdasarkan nama hidangan makanan kecil favorit. Keunggulan utama para pengembang aplikasi Android adalah gratis dan open source. Open source (salah satu keunggulan terbaik yang dimiliki), banyak pengembang perangkat lunak yang bisa melihat dan memanfaatkan kode itu serta bisa membuat aplikasi baru di dalamnya. Berbagai aplikasi android difasilitasi melalui Android Market [5], [6], sehingga pengguna aplikasi tinggal memasang aplikasi pilihannya.

1. Pengembangan sistem operasi dan aplikasi Android sendiri mengacu pada empat prinsip yaitu terbuka. Android dibangun untuk menjadi benar-benar dapat digunakan .Sebagai contoh, sebuah aplikasi dapat mengambil dan mengakses fungsi utama *smartphone* seperti membuat panggilan, mengirim pesan teks, membuka dan menutup portal kamera. Hal ini memungkinkan pengembang untuk membangun aplikasi yang lebih baik dan mudah.
2. Aplikasi dibuat sama Android tidak membedakan antara aplikasi inti ponsel dan aplikasi pihak ketiga. Kedua jenis aplikasi ini dapat dibangun untuk memiliki akses yang sama ke ponsel. Pengguna dapat sepenuhnya mengatur telepon sesuai kepentingan mereka.
3. Membuka batasan-batasan aplikasi Android serta membuang berbagai batasan untuk membangun aplikasi baru yang inovatif. Misalnya pengembang dapat menggabungkan informasi dari WEB dengan data individu dari ponsel. Contoh data kontak, kalender, atau lokasi geografis(membuka akses GPS). Sehingga memberikan informasi yang lebih relevan. Dengan android pengembang juga dapat membangun aplikasi yang memungkinkan para pengguna untuk melihat lokasi dan terkoneksi dengan teman-temannya.

3. HASIL DAN PEMBAHASAN

2.1. Rancangan Sistem

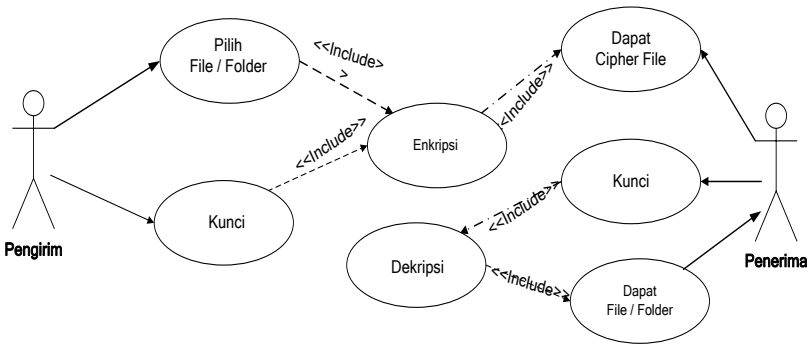
Penelitian ini menghasilkan 2 modul yang diterapkan pada aplikasi yaitu modul enkripsi dan model deskripsi , adapun data yang dapat dienkripsi adalah berupa File dan Folder yang akan diubah kedalam bentuk ChipperText. Hasil bentukan ChipperText ini tidak dapat dibuka tanpa kunci yang telah dibangun. Berikut gambar arsitektur sistem yang telah buat.



Gambar 1. Arsitektur Sistem yang dibuat .

Untuk menggunakan sistem ini dibutukan 2 pengguna sistem, 1 orang sebagai pengirim dan 1 orang sebagai penerima , dimana kedua pengguna ini harus menggunakan sistem yang sama. Prinsip kerja dari sistem berawal dari pengirim yang akan mengekripsi data , ketika data akan di enkripsi oleh sistem pengirim juga harus menginput kata kunci atau *identic keys* , data dan *key* akan diproses oleh sistem secara bersama menggunakan Algoritma Twofish . Begitu pula ketika akan mendeskripsi data yang diterima , si penerima harus menggunakan *key* yang telah dikomunikasikan oleh pengirim data . Sistem ini dibangun berbasis android menggunakan bahasa pemrograman Java dan HTML . Java memiliki banyak *library* yang tersedia secara gratis , penulis menggunakan *library Class Twofish* dalam membangun sistem ini.

Penulis merancang sistem menggunakan model *Unified Modelling Language* , hasil rancangan sistem dapat dilihat diagram uses case.

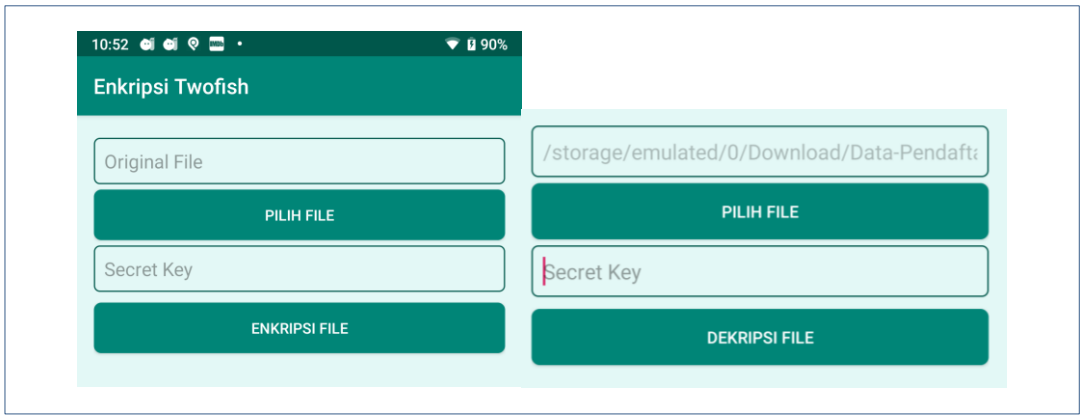


Gambar 2. Diagram uses case enkripsi dan deskripsi TwoFish.

Hasil diagram uses case merupakan cerminan dari arsitektur yang dirancang sebelumnya. Diagram uses case memperlihatkan lebih detail bagaimana sistem ini bekerja sesuai rancangan. Terdapat 7 uses case dimana uses case ini akan menjadi sub program dalam sistem, ke 2 user memiliki kunci yang sama untuk mengenkripsi dan mendeskripsi data , penerima memiliki data berupa Chipper File dan *key* yang akan di inputkan kedalam sistem untuk dapat memilhat data. Data perusahaan sangat penting , data yang dimiliki perusahaan terdapat beberapa macam , seperti file doc , file pdf , file video , dan file lainnya. Yang tidak dapat dielakkan yaitu data perusahaan kadang harus disiapkan atau diarsipkan dalam 1 penyimpan identik , berangkat dari permasalah tersebut sistem yang dirancang ini dapat menerima bentuk file yang berbeda dan folder yang akan digunakan .

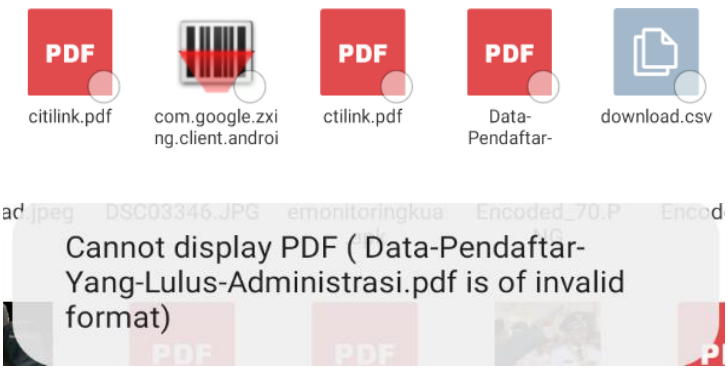
2.2. Implementasi Sistem Algoritma TwoFish

Penulis membangun sistem berbasis android , dimana sistem android lebih mudah diraih dalam genggaman dibandingkan program atau sistem yang berbasis desktop . Terdapat 2 fungsi unggulan pada sistem ini yaitu fungsi Enkripsi Data dan fungsi Deskripsi Data . Interface untuk fungsi Enkripsi Data dapat dilihat sebagai berikut.



Gambar 3 Interface fungsi pemilihan Data dan Enkripsi Data

Tampilan sistem diatas menampilkan bagaimana pengirim data dapat menginputkan file yang akan di enkripsi dan menginput key yang akan digunakan secara bersama dengan penerima data.



Gambar 4 Hasil sistem jika file gagal di buka.

Gambar 5 Interface fungsi penerimaan file Ekripsi dan Deskripsi Data.

Dari sisi penerima data yang telah di Enkripsi (berupa *block chipper*) , tampilan sistem diatas memperlihatkan penerima data harus menginput *Block Chipper* yang diberikan pengguna dan telah menyepakati *Key* yang telah ditentukan sebelumnya. Aplikasi yang digunakan harus sama dengan yang digunakan oleh pengirim data.

Gambar 6 Hasil deskripsi data penerima dari sistem.

2.3. Pengujian Balck Box

Tabel 1 Rekapitulasi pengujian Black Box sistem Enkripsi dan Deskripsi Twofish

No	Spesifikasi	Status	Hasil pengujian
1	Memilih Dokumen asli	✓	Dapat memilih Dokumen Asli dari Memory Handphone yang masih dapat terbuka
2	buka file yang telah di enkripsi	✓	Fiel tidak dapat dibuka, denta tampil pesan invalid
3	buka file yang telah di enkripsi	✓	Fiel tidak dapat dibuka, denta tampil pesan invalid

4	Memilih DokumenCipher file	✓	Dapat memilih Dokumen cipher file dari Memory Handphone yang masih dapat terbuka
5	Mengedekripsi file	✓	Sukses menfdekripsi file dengan indicator tampil pesan berhasil
6	buka file yang telah di dekripsi	✓	File dapat dibuka

Dari tabel diatas dapat disimpulkan bahwa hasil keseluruhan pengujian input output dari aplikasi serta validasi aplikasi yang dibuat sudah sesuai dengan spesifikasi yang diinginkan, ini bisa dilihat dari keenam fungsi input output proses serta validasi sistem fungsional yang diinginkan dapat bekerja sesuai dengan spesifikasi yang diharapkan

2.4. Pengujian White Box

Berikut adalah tabel hasil rekapitulasi pengujian menggunakan metode white box:

Tabel 5.6 Hasil Pengujian *White Box*

No	Flowgraph	Independen Path	Region	Komplesitas Siklomatis
1	*Flowgraph* enkripsi	3	3	3
2	*Flowgraph* dekripsi	2	2	2
TOTAL		**5**	**5**	**5**

Berdasarkan hasil pengujian perangkat lunak yang terdapat pada tabel 5.6 maka, sistem dikatakan sudah bebas dari kesalahan logika, karena *Cyclomatic Complexity*, *Region* dan *Independent Path* adalah sama.

4. KESIMPULAN

Berdasarkan hasil yang dicapai dari proses penelitian dengna judul Penerapan Metode Enkripsi Twofish Untuk Keamanan File Dan Folder Berbasis Android kami maka kami menarik kesimpulan bahwa bahwa :

1. Berdasarkan 6 spesifikasi hasil pengujian *blackbox*, keempat fungsi dapat berfungsi sesuai dengan spesifikasi yang dinginkan. Dan berdasarkan pengujian white box, proses encode dan decode .
2. Berhasil membangun Aplikasi untuk keamanan file berbasis android
3. Berhasil menerapkan metode Twofish untuk keamana file berbasis android.

5. SARAN

Berdasarkan kesimpulan tersebut di atas, maka ada beberapa saran yang akan diajukan dalam penelitian ini, Penulis menyadari bahwa sistem yang dibangun masih membutuhkan

penyempurnaan yang lebih baik. Oleh karena itu, penulis menyarankan agar skripsi ini dapat dijadikan sebagai bahan referensi untuk mengembangkan sistem yang lebih sempurna. Penerapan Metode Twofish Untuk Aplikasi Enkripsi File Dan Folder

DAFTAR PUSTAKA

[1] E. Hasmin, "PENERAPAN METODE TWOFISH UNTUK APLIKASI ENKRIPSI FILE DAN FOLDER," *Konf. Nas. Sist. Inf.*, 2016.

[2] K. Sentot, "Teori & Aplikasi Kriptografi: SPK IT Consulting," 2010.

[3] N. Aini, "APLIKASI PENANDA DIGITAL (WATERMARKING) FILE VIDEO DENGAN METODE LAST SIGNIFICANT BIT (LSB) IMPLEMETASI: JAVA PROGRAMMING," *SEMNASTEKNOMEDIA ONLINE*, vol. 4, no. 1, pp. 2–9, 2016.

[4] D. A. Trianggana and H. L. Sari, "Analisis Perbandingan Kinerja Algoritma Blowfish Dan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi," *Pseudocode*, vol. 2, no. 1, pp. 37–44, 2015.

[5] M. S. Natsir and W. Rusdi, "Perancangan Aplikasi Papan Informasi Berbasis Android Pada STMIK Dipanegara Makassar," presented at the SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, 2019, vol. 8.

[6] A. Rauf, "Implementasi Sistem Rekomendasi Barang Customer pada E-Commerce MTC Karebosi Menggunakan Metode K-Means Clustering dan Metode Decision Tree," presented at the SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, 2019, vol. 7.