Pengamanan Aplikasi Mobile BluCampus dengan Algoritma AES-128 dan Affine Cipher : Studi Kasus Universitas Budi Luhur

Lia Amellia Putri [1], Achmad Solichin [2]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : liaamelliaputri@gmail.com[1], achmad.solichin@budiluhur.ac.id[2]

Abstrak

Perkembangan teknologi informasi dan komunikasi berkembang pesat. Salah satunya bertujuan mempermudah dalam melakukan transaksi administrasi contoh layanan surat keterangan pada BAAK Universitas Budi Luhur yang bersifat lokal, untuk membuat surat mahasiswa harus mengantri di BAAK dan menunggu untuk mencetak surat yang dibutuhkan hal ini menjadi kurang efisien. Namun penerapan teknologi berbasis mobile menjadi alternatif untuk mengatasi permasalahan ini. Maka dibuat fitur BluAcademic pada aplikasi BluCampus yang bertujuan mempermudah proses pembuatan layanan surat keterangan yang dapat dilakukan secara online sehingga memudahkan mahasiswa dan staf BAAK dalam proses pembuatan surat keterangan yang dibutuhkan secara cepat, dalam fitur BluAcademic juga di tambahkan metode kriptografi untuk keamanan data karena pada proses pengiriman dan penerimaan data harus melalui jaringan internet yang rawan terhadap penyadapan, pencurian data, pemalsuan informasi oleh pihak yang tidak bertanggung jawab. Metode kriptografi yang digunakan adalah AES 128 dan Affine Cipher. Hasil pengujian rata-rata waktu proses enkripsi adalah 0,67 detik dan proses dekripsi memerlukan waktu 0,58 detik, sedangkan berdasarkan hasil kuesioner dari 22 pengguna fitur BLuAcademic yang mengisi kuesioner untuk dari 4 aspek penilaian sebagai berikut: aspek penilaian functionality sebesar 83%, aspek penilaian reliability sebesar 81%,aspek penilaian usability sebesar 86%, aspek penilaian efficiency sebesar 88% dan total skor aktual keseluruhan sebesar 84%.

Kata kunci : Kriptografi,AES, *Affine Cipher*, Enkripsi, Dekripsi

1. PENDAHULUAN

Sistem layanan pembuatan surat keterangan di BAAK Universitas Budi Luhur masih bersifat lokal namun sudah komputerisasi,sehingga untuk membuat surat keterangan mahasiswa masih harus mengantri di BAAK dan harus menunggu beberapa waktu untuk mencetak surat yang dibutuhkan hal ini menjadi kurang efisien. Untuk mengatasi permasalahan ini salah satu pilihan alternatifnya adalah menerapan teknologi berbasis mobile, tetapi hal ini memiliki dampak negatif yaitu permasalahan keamanan data, karena jaringan sebagai sarana komunikasi sangat rawan terhadap penyalahgunaan dari pihak yang tidak berhak mengakses data tersebut.

Berdasarkan permasalahan tersebut maka dibuat fitur BluAcademic pada aplikasi BluCampus yang bertujuan mempermudah pembuatan surat keterangan di BAAK Universitas Budi Luhur secara cepat , di dalam fitur aplikasi BluAcademic ini juga menggunakan algoritma kriptografi AES 128 dan Affine Cipher yang dibutuhkan untuk. mengamankan data yang di input oleh pengguna dalam bentuk enkripsi untuk mencegah penyalahgunaan dari pihak-pihak yang tidak berwenang dan juga dapat mengembalikan data yang sudah terenkripsi menjadi data yang asli sehingga tidak mengubah data antara web service dengan android (*mobile*).

Dari uraian di atas apabila permasalahan tersebut dapat terselesaikan, maka akan sesuai dengan tujuan yang ingin dicapai dari penelitian ini yaitu mengimplementasikan metode algoritma kriptografi AES 128 dan Affine Cipher untuk mengamankan data agar tidak disalahgunakan oleh pihak-pihak yang tidak berwenang dan mengembalikan data yang sudah terenkripsi menjadi data asli *(plaintext)* tanpa mengalami perubahan.

Dalam penelitian ini metode peneliltian yang digunakan meliputi studi literatur, analisis data, perancangan sistem dan pengujian sistem.

2. TINJAUAN PUSTAKA

2.1. Definisi Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli [1].

Kriptografi adalah ilmu mengubah, atau *encoding*, informasi menjadi bentuk yang tidak dipahami bagi siapa saja yang tidak mengetahui kunci yang tepat. Dalam bentuk seperti informasi dapat dengan aman dikirimkan melalui setiap saluran komunikasi ataupun disimpan dalam arsip data dengan akses terbatas atau bahkan dilarang untuk diakses (dengan alasan tertentu) [2]. Kriptografi dapat diterapkan pada berbagai jenis file, termasuk file teks, dokumen, gambar [7], audio dan video.

2.2. Algoritma Kriptografi Klasik

Algoritma ini merupakan algoritma kriptografi yang biasa digunakan orang sejak berabad-abad yang lalu. Dua teknik dasar yang biasa digunakan, yaitu:teknik substitusi adalah menggantikan karakter dalam plaintext menjadi karakter lain yang hasilnya adalah ciphertext. Sedangkan transposisi adalah teknik mengubah plaintext menjadi ciphertext dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern [3].

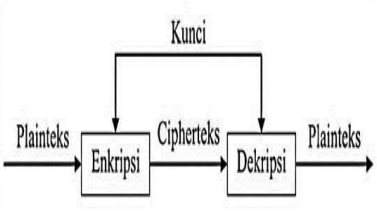
2.3. Algoritma Kriptografi Modern

Algoritma kriptografi modern beroperasi dalam mode bit ketimbang mode karakter. Operasi dalam mode bit berarti semua data dan informasi dinyatakan dalam rangkaian bit biner 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plainteks dienkripsi menjadi cipherteks dalam bentuk rangkaian bit, demikian sebaliknya. Karena enkripsi modern sudah menggunkan komputer untuk pengoperasiannya. Berfungsi untuk mengamankan data baik yang di transfer melalui jaringan komputer maupun yang bukan. Hal ini sangat berguna untuk melindungi privacy data, integrity, authentication dan non-repudiation. Perkembangan algoritma kriptografi modern berbasis bit didorong oleh penggunaan komputer digital yang merepresentasikan data dalam bentuk biner [4].

2.4. Algoritma Kriptografi Simetris

Algoritma ini disebut simetris karena memiliki *key* atau kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini juga sering disebut algoritma kunci tunggal atau algoritma satu kunci. *Key* dalam algoritma ini bersifat rahasia atau *private key* sehingga algoritma ini juga disebut dengan algoritma kunci rahasia [5].

Pada Gambar 1 dapat dilihat bahwa kunci yang digunakan pada proses enkripsi dan deskripsi adalah kunci yang sama.

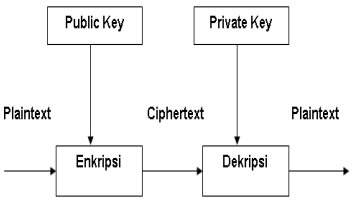


Gambar 1. Algoritma Kriptografi Simetris

2.5. Algoritma Kriptografi Asimetris

Algoritma ini disebut asimetris karena kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Kunci yang digunakan untuk enkripsi adalah kunci publik sehingga algoritma ini juga disebut dengan algoritma kunci publik. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia [5].

Pada Gambar 2 dapat dilihat bahwa kunci yang digunakan pada proses enkripsi dan deskripsi adalah kunci yang berbeda, pada saat akan mngenkripsi *plaintext* digunakan *public key* dan saat akan mendekripsi *ciphertext* digunakan *private key*.



Gambar 2. Algoritma kriptografi Asimetris

2.6. Algortima AES 128

Advanced Encryption Standard adalah sebuah algoritma kriptografi simetris yang dapat digunakan untuk mengamankan data. Algoritma ini merupakan standar enkripsi dengan kunci-simetris. Algoritma AES dengan blok *ciphertext* simetris dapat mengenkripsi dan dekripsi sebuah informasi. Jenis Algoritma ini terbagi menjadi 3 yaitu AES-128, AES-192 dan AES-256 [6].

Tabel 1. Parameter AES

	AES-128	**AES192**	**AES-256**
Key size	4word (16byte)	6word (24byte)	8word (32byte)
Plaintext block size	4word (16byte)	4word (16byte)	4word (16byte)
Number of rounds	10	12	14
Round key size	4word (16byte)	4word (16byte)	4word (16byte)
Expanded key size	44word (176byte)	52word (208byte)	60 word (240byte)

Dari Tabel 1 menjelaskan panjang kunci Nk= 4 word yang digunakan pada AES-128, sedangkan pada AES-192 panjang kunci Nk=6 word dan pada AES-256 panjang kunci Nk=8word,setiap kata terdiri dari 32 bit sehingga total kunci pada AES-128, AES-192, dan AES-256 masing-masing adalah 128bit,192bit, dan 256bit. Ukuran *plaintext block* AES-128, AES-192, dan AES-256 memiliki ukuran yang sama yaitu 128 bit (4x32 bit), namun pada AES-128, AES-192, dan AES-256 masing-masing jumlah *round* adalah 10 putaran,12 putaran,dan 14 putaran. Sedangkan *Expanded key* masing-masing berjumlah 44*word*, 52*word* dan 60 *word*.

Garis besar Algoritma *Rijndael* yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut : *AddRoundKey* adalah melakukan *XOR* antara *state* awal (*plainteks*) dengan *cipher key*. Tahap ini disebut juga *initial round*. Putaran sebanyak *Nr* – 1 kali. Proses yang dilakukan pada setiap putaran terdiri atas *SubBytes, ShiftRows,*

MixColumns, dan AddRoundKey. *SubBytes* adalah fungsi substitusi *byte* dengan menggunakan tabel substitusi (*S-box*). *ShiftRows* adalah pergeseran baris-baris *array state* secara *wrapping*. *MixColumns* adalah mengacak data di masing-masing kolom *array state.* Pada *final round* (proses untuk putaran terakhir) terdiri dari *SubBytes, ShiftRows, dan AddRoundKey* [6].

2.7. Algortima Affine Cipher

Enkripsi yang digunakan Julius Caesar (*Caesar cipher*) menggunakan transformasi yang sederhana yaitu *shift transformation* yang sangat rentan terhadap analisa frekuensi. Untuk mencoba mempersulit analisa frekuensi, enkripsi *affine* menggunakan *affine transformation*, dengan rumus:
Enkripsi :
C =((a∗ P)+b) MOD n
Dekripsi :
P =(a^{-1} ∗ (C– b)) MOD n
Keterangan:

1. kunci untuk enkripsi *affine cipher* terdiri dari dua parameter: *a* dan *b*.
2. *n* adalah ukuran alfabet
3. *a* bilangan bulat yang relatif prima dengan *n* ,m harus mematuhi gcd(*a; n*) = 1
4. *b* adalah jumlah pergeseran (bilangan bulat positif)
5. a^{-1} adalah inversi *a* (mod *n*), yaitu $a \cdot a^{-1} \equiv 1$ (mod *n*) .

Dengan *shift transformation*, untuk setiap percobaan kita mencari satu parameter kunci menggunakan satu persamaan, jadi untuk setiap percobaan kita pasangkan satu kode asli dengan satu kode acak yang sesuai berdasarkan statistik dari pengamatan empiris. Strategi pencarian adalah menggunakan pasangan dimana karakter aslinya mempunyai statistik penggunaan terbesar. Karena *affine transformation* menggunakan dua parameter, setiap percobaan kita harus mencari kedua parameter sedikitnya menggunakan dua persamaan dengan dua pasangan. Strategi pencarian adalah dengan mencoba dua pasangan dimana dua karakter aslinya merupakan dua karakter dengan statistik penggunaan terbesar. Analisa frekuensi terhadap enkripsi *affine* memang lebih sulit dibandingkan analisa frekuensi terhadap enkripsi yang menggunakan *shift transformation*, namun analisa frekuensi terhadap enkripsi *affine* masih tergolong mudah untuk dilakukan [1].

3. METODE PENELITIAN

3.1. Metode Penelitian

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Adapun metode – metode ini sebagai berikut :

a. Studi literatur

Metode ini digunakan untuk memperoleh pembelajaran data atau informasi dengan cara mengumpulkan berbagai refensi baik itu dalam bentuk makalah, jurnal, serta referensi lainnya untuk mendapatkan informasi yang dibutuhkan.

b. Analisis Data

Metode ini digunakan untuk menganalisis Algoritma kriptografi yang digunakan yaitu metode algoritma kriptografi AES 128 dan Affine Cipher, serta teknik-teknik yang digunakan.

c. Perancangan Sistem

Metode ini digunakan untuk merancang sistem aplikasi untuk mengimplementasikan metode algoritma kriptografi AES 128 dan Affine Cipher dengan menggunakan bahasa pemrograman JAVA berbasis Android.

d. Pengujian Sistem

Metode ini dilakukan dengan menguji dan mengecek jalannya program.

3.2. Analisis dan Penyelesaian Masalah

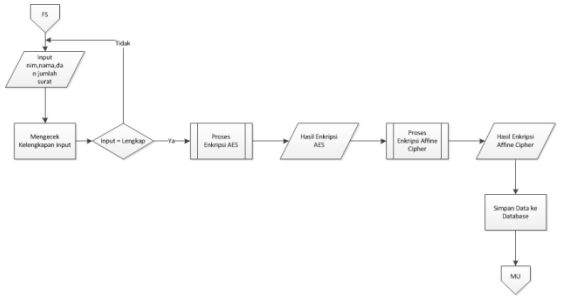
Masalah layanan surat keterangan pada BAAK Universitas Budi Luhur adalah pembuatan surat masih bersifat lokal sehingga tidak efisien oleh karena itu di buat fitur BluAcademic aplikasi Blucampus untuk mengatasi masalah tersebut, dengan adanya fitur BluAcademic mahasiswa dapat melakukan permintaan pembuatan surat keterangan secara *mobile.* Namun saat pengiriman data yang di input ke *web service* melalui jaringan internet pada fitur BluAcademic bisa sangat rawan terhadap penyalahgunaan dari pihak-pihak yang tidak berhak mengakses data tersebut. Jika data yang di kirim tidak dijaga keamanan datanya dengan baik dapat berakibat merugikan terutama bagi pengguna fitur BluAcademic.

Dari permasalahan yang ada maka diperlukan sistem keamanan data pada fitur BluAcademic aplikasi BLuCampus yang mampu menjaga kerahasiaan data sehingga data tersebut tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak atas data tersebut. Untuk dapat membuat data tersebut terjaga kerahasiaannya, aplikasi ini akan memanfaatkan ilmu pengamanan data yaitu kriptografi.

Aplikasi kriptografi ini menggunakan algoritma *AES* dengan kunci 128 bit dan algoritma Affine Cipher. Algortima *AES* 128 termasuk dalam kriptografi kunci simetris sedangkan *Affine Cipher* termasuk kunci asimetris. Dengan mengunakan dua algortima kriptografi yaitu AES-128 dan *Affine Cipher* dapat meningkatkan keamanan data dari pihak yang tidak berhak mengakses data tersebut karena untuk memecahkan ciphertext, mereka harus mengetahui tiga buah bilangan yang digunakan yaitu kunci enkripsi, kunci dekripsi dan pergeseran karakter yang digunakan pada algoritma *Affine Cipher* dan satu kunci menggunakan algoritma AES-128.

3.3. Flowchart dan Algoritma Program

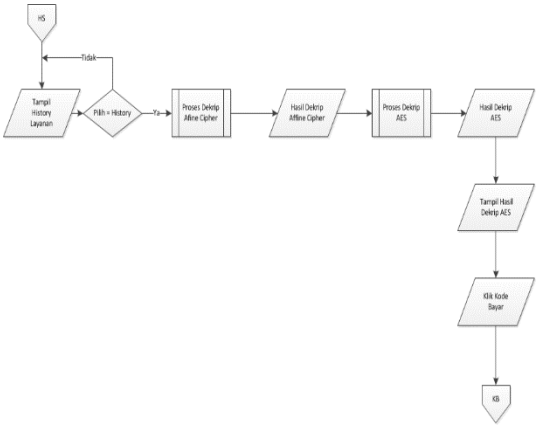
Berikut ini merupakan rancangan *flowchart* dan algoritma pemrograman pada form layanan dan history surat serta *flowchart* dan algoritma untuk proses enkripsi dan dekripsi data menggunakan AES128 dan Affine Cipher, berikut *flowchart* dan algoritmanya :



Gambar 3. Flowchart Form Layanan Surat

Flowchart pada Gambar 3 menjelaskan alur proses dari menginput data sampai menyimpan data yang telah di enkripsi pada *form* layanan surat yang tampil ketika pada menu layanan jenis surat yang dipilih kecuali surat keterangan magang, surat keterangan riset TA, surat keterangan riset KKP, sedangkan untuk alur proses surat keterangan magang, surat keterangan riset TA, surat keterangan riset KKP hampir sama dengan Gambar 3 hanya berbeda pada data yang di input pengguna. Algoritma proses form layanan surat dari *flowchart* di atas :

1. Input nim,nama,dan jumlah surat
2. Cek kelengkapan inputan
3. If inputan = lengkap Then
4. Jalankan proses enkripsi AES
5. Tampilkan hasil enkripsi AES
6. Jalankan proses enkripsi Affine Cipher
7. Tampilkan hasil enkripsi Affine Cipher
8. Simpan hasil enkripsi Affine Cipher ke database
9. Tampilkan pesan"Berhasil *Request* Surat"
10. Else
11. Kembali ke baris 2
12. End If

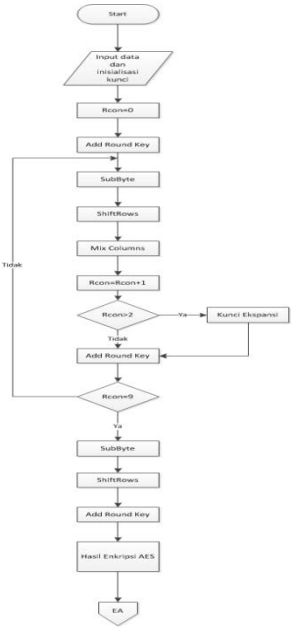


Gambar 4. Flowchart Form History Surat

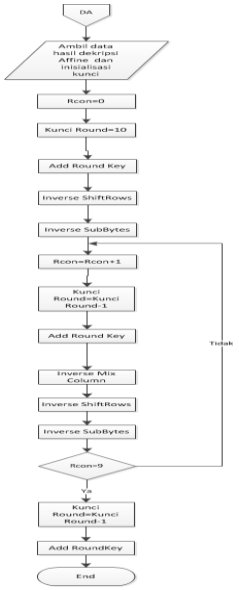
Flowchart pada Gambar 4 menjelaskan alur proses mendekripsi data pada *form history* surat yang tampil ketika pada menu *history* yang dipilih kecuali *history* surat keterangan magang, surat keterangan riset TA, surat keterangan riset KKP, sedangkan untuk alur proses surat keterangan magang, surat keterangan riset TA, surat keterangan riset KKP hampir sama dengan Gambar 4 hanya berbeda pada isi data yang di tampilkan. Algoritma proses form layanan surat dari *flowchart* di atas :

1. Tampil History Layanan
1. Pilih Action
2. If Action = buka history Then
3. Jalankan proses dekripsi Affine Cipher
4. Tampilkan hasil dekripsi Affine Cipher
5. Jalankan proses dekripsi AES
6. Tampilkan hasil dekripsi AES
7. Pilih *button* Kode Bayar
8. Else
9. Kembali ke baris 1
10. End If

Flowchart pada Gambar 5 menjelaskan alur. proses dari enkripsi algoritma AES 128 dan *Flowchart* pada Gambar 6 menjelaskan alur proses dari dekripsi algoritma AES 128



Gambar 5. Flowchart Proses Enkripsi AES 128



Gambar 6. Flowchart Proses Dekripsi AES 128

Algoritma dibawah ini menjelaskan bagaimana proses enkripsi AES-128 terjadi.

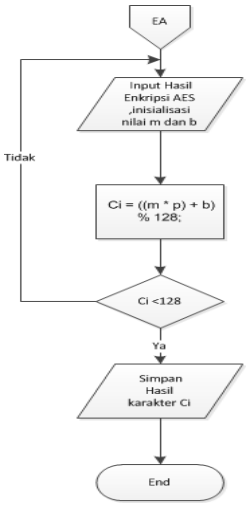
1. Start
2. Input data dan inisialisasi kunci
3. Rcon=0
4. Lakukan *AddRoundKey*
5. Lakukan *SubBytes*
6. Lakukan *ShiftRows*
7. Lakukan *MixColumns*
8. Rcon=Rcon+1
9. If Rcon>2 Then
10. Kunci Ekspansi
11. Lakukan *AddRoundKey*
12. *Else*
13. Kunci Ekspansi
14. If Rcon=9 Then
15. Lakukan *SubBytes*
16. Lakukan *ShiftRows*
17. Lakukan *AddRoundKey*
18. Ambil hasil enkripsi AES
19. Jalankan proses enkripsi Affine
20. *Else*
21. Kembali Ke baris 5
22. *End If*

Algoritma dibawah ini menjelaskan bagaimana proses dekripsi AES-128 terjadi.

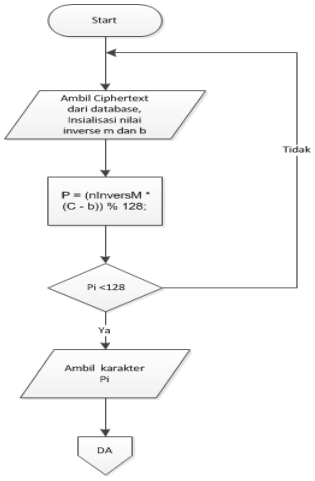
1. Ambil data hasil dekripsi Affine
2. Rcon=0
3. Kunci Round=10
4. Lakukan *AddRoundKey*
5. Lakukan Inverse*ShiftRows*
6. Lakukan *Inverse SubBytes*
7. Rcon=Rcon+1
8. Kunci Round= Kunci Round-1
9. Lakukan *AddRoundKey*
10. Lakukan *Inverse Mix Columns*
11. Lakukan Inverse *ShiftRows*
12. Lakukan *Inverse SubBytes*
13. If Rcon=9 Then
14. Kunci Round= Kunci Round-1
15. Lakukan *AddRoundKey*
16. *Else*
17. Kembali Ke baris 8
18. *End If*
19. *End*

Flowchart pada Gambar 7 menjelaskan alur proses dari enkripsi Affine Cipher dan *Flowchart* pada Gambar 8 menjelaskan alur proses dari dekripsi algoritma Affine Cipher.

.



Gambar 7. Flowchart Proses Enkripsi Affine Cipher



Gambar 8. Flowchart Proses Dekripsi Affine Cipher

Algoritma dibawah ini menjelaskan bagaimana proses enkripsi Affine Cipher terjadi.

1. Ambil data hasil enkripsi AES dan inisialisasikan nilai m dan b
2. Hitung Ci =((m*p)+b)% 128
3. If Ci<128
4. Simpan Hasil Karakter Ci
5. Else
6. Kembali ke baris 1
7. End If
8. End

Algoritma dibawah ini menjelaskan bagaimana proses dekripsi Affine Cipher terjadi.

1. Start
2. Ambil chipertext dan inisialisasikan nilai inverse m dan b
3. Hitung Pi =((nInversm *(C-b))% 128
4. If Pi<128
5. Ambil Hasil Karakter Pi
6. Jalankan Enkripsi AES
7. Else
8. Kembali ke baris 2
9. End If
10. End

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Layar

4.1.1 Tampilan Layar Menu Layanan

Gambar 9. Tampilan Layar Menu Layanan

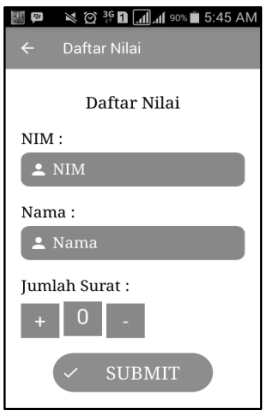
Tampilan layar menu layanan muncul pada saat menu layanan dijalankan. Dalam menu layanan terdapat 13 pilihan jenis layanan yang dapat dipilih oleh pengguna seperti: Daftar Nilai, Surat Keterangan Mahasiswa Aktif ,Fotocopy Sertifikat Akreditasi, Surat Keterangan Mengundurkan Diri, Kutipan Prestasi Akademik ,Surat Keterangan Lulus ,Surat Keterangan Pernah Tercatat Sebagai Mahasiswa, Surat Keterangan Pengganti Ijazah,Surat Pengantar Ijazah,Surat Pengantar Kuesioner,Surat Pengantar Studi Pustaka, Surat Pengantar Riset KKP, Surat Pengantar Riset TA.

4.1.2. Tampilan Layar Menu History

Gambar 10. Tampilan Layar Menu History

Tampilan layar Menu History muncul pada saat menu *history* dijalankan. Pada menu *history* menampilkan laporan history layanan yang telah diinputkan oleh pengguna pada menu layanan .

4.1.3. Tampilan Layar Form Layanan Surat



Gambar 11. Tampilan Layar Form Layanan Surat

Gambar 11 merupakan tampilan layar form layanan surat dimana data yang diinput pengguna akan di enkripsi dengan algoritma AES 128 dan Affine Cipher saat *button submit* di tekan hal ini juga terjadi pada form layanan surat keterangan magang, surat keterangan riset TA, surat keterangan riset KKP yang berbeda hanya pada data yang perlu diinput pengguna.

4.1.4. Tampilan History Form History Surat

Gambar 12. Tampilan Layar Form History Surat

Gambar 12 merupakan tampilan layar form *history* surat dimana data yang sudah diinput pengguna pada form layanan akan di dekripsi dengan algoritma Affine Cipher dan AES 128 saat *history* tersebut di pilih hal ini juga terjadi pada form *history* surat keterangan magang, surat keterangan riset TA, surat keterangan riset KKP yang berbeda hanya pada isi data yang ditampilkan.

4.2. Pengujian Program

Tabel 2. Hasil Pengujian Proses Enkripsi dan Dekripsi

Input	Output AES128 dan Affine Cipher	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
Data Layanan Surat NIM: 1411502477 Nama: Lia Amellia Putri	NIM: 6$6'C$!'C6:60!=470$9$C=:'*@!=399 Nama: -@*!<*0@$4*$=!'69$=7!-$49'!@4<C<'!9'@0'9!<'0*6*C$3C*97!-4<*6!7<	0,54	0,50
Data Layanan Surat Keterangan Magang Nama Instansi :PT. Sinar Surya Alamat Instansi : Jalan Ciledug Raya Telepon Instansi :0215853753	Nama Instansi : 3!'73C<09@!*'<0$0<:<@4<!:!990@-- Alamat Instansi : <@!C7@-<06=!7=0<-$7!$40$0--*3CC3-"6C'340=:!67!<3<!3$7<$7<40$7!' Telepon Instansi : 'C0:6@$06C763!69@46@<3$$:4:=:-@@	0,63	0,57
Data Layanan Surat Keterangan Riset TA Prodi : Teknik Informatika	Prodi: =!-*='0:C@$*<!9=!*94<999$$'CC3*CCC$9-:37:!-0$4<99-9$6'9C:3:'99*6	0,71	0,62
Data Layanan Surat Keterangan Riset KKP NIM2: 1411503541 Nama2: Tomi Hartanto NIM3: 1411501211 Nama3: Destriyani	NIM2: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama2: $407':=$!7*'C=!03<-0C-<@-C4@!$4* NIM3 :04!=39-33!6'!'9@3:77=@!C7@*77-=- Nama3: C:4'@:*C0<9**4:6$33:767!0*6:4*@-	0,78	0,71
	Rata-Rata	0,67	0,58

Hasil pengujian pada Tabel 2 diketahui bahwa jumlah persentase keberhasilan pada proses enkripsi dan dekripsi mencapai 100% dengan waktu yang tidak mempengaruhi banyak sedikitnya data inputan yang akan dienkripsi atau didekripsi. Rata-rata waktu yang dibutuhkan untuk proses enkripsi adalah 0,67 detik dan proses dekripsi memerlukan waktu 0,58 detik. Jadi waktu proses enkripsi sedikit lebih lama daripada proses dekripsi.

4.3. Tanggapan Pengguna

Dari 4 kategori aspek penilaian yaitu functionality, reliability, usability, dan efficiency skor dari 22 responden dapat dilihat pada Tabel 3 sebesar 96 jawaban sangat setuju, 135 jawaban setuju, 27 jawaban ragu-ragu , 5 jawaban tidak setuju dan 1 jawaban sangat tidak setuju.

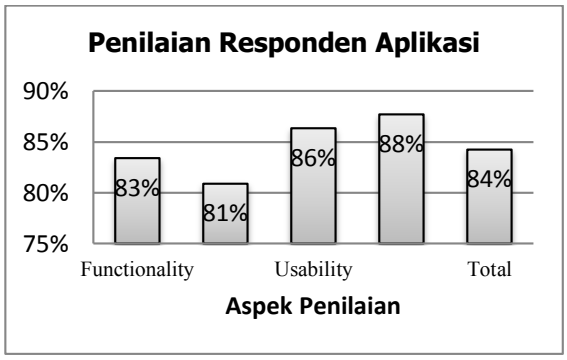
Tabel 3. Tabel Skor Responden

Aspek Penilaian	**Skor Responden**				
	5	**4**	**3**	**2**	**1**
	SS	**S**	**R**	**TS**	**STS**
Functionality	24	57	6	0	1
Reliability	29	16	16	5	0
Usability	24	39	3	0	0
Efficiency	19	23	2	0	0
Jumlah	**96**	**135**	**27**	**5**	**1**

Pada Tabel 4 hasil penilaian responden terhadap aplikasi dari 4 kategori aspek penilaian yaitu *functionality, reliability, usability, dan efficiency*. Total skor aktual untuk aspek *functionality* sebesar 83% ,aspek *reliability* 81%, aspek *usability* 86%,dan aspek *efficiency* 88%, dan total skor aktual keseluruhan sebesar 84%. Gambar 13 menunjukkan diagram penilaian responden aplikasi dari 4 aspek penilaian dan total keseluruhan.

Tabel 4 .Tabel Penilaian Responden Aplikasi

Aspek Penilaian	Skor Aktual					Total Skor Aktual	Skor Ideal	%
	5	4	3	2	1			
	SS	S	R	TS	STS			
Functionality	120	228	18	0	1	367	440	83%
Reliability	145	64	48	10	0	267	330	81%
Usability	120	156	9	0	0	285	330	86%
Efficiency	95	92	6	0	0	193	220	88%
Total						**1112**	**1320**	**84%**



Gambar 13.Diagram Penilaian Responden Aplikasi

4.4. Kelebihan Program

a. Aplikasi lebih aman karena menggunakan 2 algoritma kriptografi yaitu AES-128 dan Affine Cipher yang merupakan algoritma kriptografi kunci simetris dan asimetris.
b. Isi data dari hasil dekripsi tidak mengalami perubahan atau kembali seperti data asli.
c. Proses Enkripsi dan Dekripsi berlangsung cepat.

4.5. Kekurangan Program

a. Hasil enkripsi akan sama apabila data yang diinputkan sama karena kunci sudah diinsialisasikan pada program .
b. Pengguna tidak dapat menginpukan kunci sendiri.
c. Data inputan hanya akan tersimpan ke database apabila jaringan internet baik.

5. KESIMPULAN

a. Dengan mengimplementasikan kriptografi dengan metode algoritma AES-128 dan Affine Cipher pada aplikasi ini, data input yang akan dikirim dan disimpan dalam database akan lebih terjaga keamanannya karena hanya pengguna dan admin yang dapat mengetahui data tersebut tersebut.
b. Proses enkripsi dan proses dekripsi pada algoritma Affine cipher membutuhkan dua kunci dan satu nilai pergeseran, sedangkan proses enkripsi dan dekripsi menggunakan AES-128 membutuhkan satu kunci. Gabungan dari algoritma Affine cipher dan AES-128 akan menghasilkan tiga kunci sehingga keamaanan menjadi lebih aman .
c. Jumlah data yang disimpan ke dalam *database* dan dibaca dari *database* mempengaruhi lama proses kerja enkripsi maupun dekripsi.
d. Hasil pengujian rata-rata waktu proses enkripsi adalah 0,67 detik dan proses dekripsi memerlukan waktu 0,58 detik. Jadi waktu proses enkripsi sedikit lebih lama daripada proses dekripsi.
e. Dari hasil tanggapan 22 pengguna yang mengisi kuesioner untuk 12 pertanyaan dari 4 aspek penilaian di dapatkan hasil berikut: aspek *functionality* sebesar 83%, aspek *reliability* sebesar 81%, aspek *usability* sebesar 86%, aspek *efficiency* sebesar 88%, dan total skor aktual keseluruhan sebesar 84%. Hal ini menunjukkan bahwa fitur BluAcademic aplikasi BluCampus dapat diterima dengan baik oleh 22 responden karena nilai keseluruhan dari keempat aspek tersebut sebanyak 1112 (84%) dari nilai yang ideal 1320 .

6. DAFTAR PUSTAKA

[1] S. Kromodimoeljo, *Teori & Aplikasi Kriptografi*. SPK IT Consulting, 2010.
[2] C. Kościelny, M. Kurkowski, and M. Srebrny, *Modern Cryptography Primer*. 2013.
[3] Y. Kurniawan., *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*. Bandung: Informatika, 2004.
[4] R. Munir., *Kriptografi*. Bandung: Informatika, 2006.
[5] I. Halik and Y. Prayudi, "Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data," *Stud. Dan Anal. Algoritm. Rivest Code 6 Dalam Enkripsi/Dekripsi Data*, vol. 6, no. D, pp. 149–158, 2005.
[6] A. M. Abidin, F. Hardianti, and I. N. Setiani, "Analisa Dan Implementasi Proses Kriptografi Encryption-Decryption Dengan Algoritma Advanced Encryption Standard (Aes-128)," *J. Sarj. Tek. Inform. Keamanan Komput.*, p. `, 2016.
[7] A. Solichin and E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," *2017 3rd International Conference on Science in Information Technology (ICSITech)*, Bandung, 2017, pp. 618-621.