Majalah Ilmiah Teknologi Elektro, Vol. 18, No. 1, Januari - April 2019
DOI: https://doi.org/10.24843/MITE.2019.v18i01.P01

Rancang Bangun Sistem Enkripsi Dan Dekripsi SMS Menggunakan AES dan *Blowfish Cipher* serta Kombinasinya Pada Telepon Seluler Berbasis Android

I Putu Warma Putra[1], Made Sudarma[2], Nyoman Pramaita[3]
[Submission: 13-09-2019, Accepted: 19-01-2019]

Abstract*— One of the facilities provided by cellular phones is to send data in the form of short messages via Short Message Service (SMS). Most people use SMS services more often than phone services because they are cheap and easy to use. Open networks, easy access, standard platform and open source development bring security threats such as viruses, phishing, spam on SMS. Security information in SMS can be done by encrypting messages to be sent. The AES (Advanced Encryption Standard) algorithm is a standard for data encryption, suitable for scenarios where memory and processing capabilities are very limited as in mobile devices. Encryption for text data types can also use the Blowfish algorithm, where the Blowfish algorithm can perform encryption and decryption with better performance compared to other symmetric algorithms if packet data size changes. The results of the study showed that the AES method was the fastest in SMS encryption and decryption while the Blowfish method changed the number of characters from the SMS sent at least.

Keyword— AES, Android, Blowfish, Enkripsi, SMS

***Intisari*—SMS merupakan salah satu layanan pada telepon seluler. Jaringan yang terbuka, akses yang mudah, platform standar dan pengembangan *open source* membawa ancaman keamanan seperti virus, *phishing, spam* pada SMS. Pengamanan infomasi dalam SMS dapat dilakukan dengan cara mengenkripsi pesan yang akan dikirim. Algoritma AES (*Advanced Encryption Standard*) merupakan standar untuk enkripsi data, cocok digunakan untuk skenario dimana *memory* dan kemampuan memproses sangatlah terbatas seperti pada perangkat telepon seluler. Enkripsi untuk tipe data text dapat juga menggunakan algoritma *Blowfish*, dimana algoritma *Blowfish* dapat melalukan enkripsi dan dekripsi dengan performa lebih baik dibandingkan dengan algoritma simetris lainnya apabila ukuran paket data berubah-ubah.**

Penelitian ini berhasil merancang sistem yang dapat dimanfaatkan oleh pengguna yang ingin mengirimkan suatu informasi rahasia kepada seseorang melalui SMS tanpa takut informasi dari pesan tersebut akan diketahui
oleh pihak lain. Hasil pengujian penelitian menunjukkan
metode AES merupakan yang tercepat dalam melakukan enkripsi dan dekripsi SMS sedangkan metode Blowfish yang paling sedikit merubah jumlah karakter dari SMS yang dikirim.

Kata Kunci— AES, Android, Blowfish, Enkripsi, SMS

I.PENDAHULUAN

Sebagian besar orang lebih sering menggunakan layanan SMS dari pada layanan telepon karena biayanya yang tergolong murah dan mudah digunakan. SMS dapat dikembangkan untuk berbagai kegiatan seperti *e-voting*[1], *mobile banking*[2], *m-commerce*[3], sistem keamanan rumah berbasis SMS[4], sistem keamanan mobil[5] dan lain-lain.

SMS akan memainkan peran penting dalam bidang bisnis masa depan, yang dikenal sebagai *m-commerce*, *mobile banking*, penggunaan oleh pemerintah, dan komunikasi kehidupan sehari-hari. Jaringan yang terbuka, akses yang mudah, platform standar dan pengembangan open source membawa ancaman keamanan seperti virus, phishing, spam pada SMS. Semua serangan yang muncul di PC akan bermigrasi ke platform komunikasi ini[6]. Oleh karena itu keamanan SMS menjadi perhatian utama bagi organisasi bisnis dan pelanggan[7].

Pengamanan infomasi dalam SMS dapat dilakukan dengan cara mengenkripsi pesan yang akan dikirim[8]. Algoritma AES (*Advanced Encryption Standard*) merupakan standar untuk enkripsi data cocok digunakan untuk skenario dimana memory dan kemampuan memproses sangatlah terbatas seperti pada perangkat telepon seluler[9]. Pada studi komparasi kunci simetris dan asimetris menunjukkan bahwa enkripsi dengan kunci simetris unggul dalam hal kecepatan dan konsumsi power. Dalam enkripsi dengan kunci simetris menunjukkan algoritma AES lebih baik dalam hal biaya, keamanan dan implementasi[10] Enkripsi untuk tipe data text dapat juga menggunakan algoritma Blowfish, dimana algoritma Blowfish dapat melalukan enkripsi dan dekripsi dengan performa lebih baik dibandingkan dengan algoritma simetris lainnya apabila ukuran paket data berubah-ubah[11]. Algoritma Blowfish memanfaatkan sumber daya komputasi yang minimum sehingga sebagian besar pengguna komputer dan bahkan pengguna awam dapat memanfaatkan algoritma ini untuk mengamankan informasi di masa depan[12]. Untuk lebih meningkatkan keamanan pesan yang dikirimkan, proses enkripsi pesan dilakukan sebanyak dua kali atau lebih dengan teknik enkripsi yang berbeda dan dengan kunci yang berbeda [13].

II. LANDASAN TEORI

Berikut ini akan dijelaskan mengenai teori pendukung yang menjadi landasan penelitian ini, diantaranya:

A. *Advanced Encryption Standard*

Advanced Encryption Standard (AES) didasarkan pada teknik enkripsi simetris. AES merupakan standar enkripsi lanjutan yang memberikan keamanan yang lebih baik daripada 3DES dan kekuatan keamanan jauh lebih baik daripada metode enkripsi lainnya. Ukuran kunci AES lebih kecil

[1]*Mahasiswa, Magister Teknik Elektro, Program Pasca Sarjana Universitas Udayana(e-mail: warma28@yahoo.co.id)*
[2, 3] *staff pengajar Magister Teknik Eletro, Program Pasca Sarjana Universitas Udayana, JL PB. Sudirman Denpasar Bali (0361-239599); email : [2]msudarma@unud.ac.id, [3]pramaita@ee.unud.ac.id*

p-ISSN:1693 – 2951; e-ISSN: 2503-2372

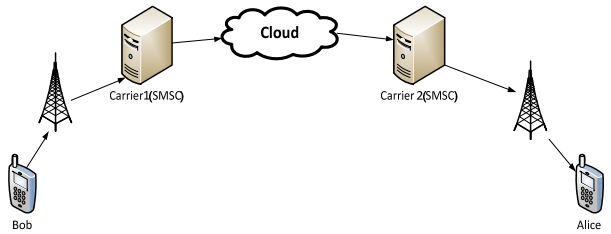
dibandingkan dengan skema yang lain. AES terdiri dari substitusi byte dan pergeseran baris dan ini membentuk transformasi lingkaran[14].

B. Blowfish

Blowfish adalah salah satu algoritma enkripsi publik yang paling umum digunakan dikembangkan oleh Bruce Schneier salah satu dari *cryptologists* terkemuka di dunia, dan presiden dari Sistem Counterpane, sebuah perusahaan konsultan yang mengkhususkan diri dalam kriptografi dan keamanan komputer. Blowfish menggunakan kunci dengan ukuran bervariasi, mulai dari 32 bit hingga 448 bit dimana secara default menggunakan 128 bit. Blowfish tidak dipatenkan, berlisensi bebas, dan tersedia gratis untuk semua penggunaan [15].

C. SMS

Short Message Services (SMS) atau layanan pesan singkat merupakan sebuah revolusi di media penyebaran informasi, dimana layanan yang digunakan tidak berbasis suara tetapi berbasis teks singkat. SMS adalah protokol layanan pertukaran pesan text singkat (sebanyak 160 karakter per pesan) antar telepon. SMS ini pada awalnya adalah bagian dari standar teknologi seluler GSM, yang kemudian juga tersedia di teknologi CDMA, telepon rumah PSTN, dan lainnya. Proses pengiriman sebuah SMS diawali saat perangkat mengirimkan SMS ke *Short Sessage Service Centre* (SMSC) operator seluler seperti yang terlihat pada gambar 1. SMS tersebut akan disimpan dan operator mencoba mengirimnya selama beberapa kali. Selanjutnya pengirim mendapatkan konfirmasi dari SMSC tentang status dari SMS yang dikirimkan.



Gambar 1. Proses pengiriman SMS

D. Android

Android adalah sebuah sistem operasi untuk perangkat *mobile* berbasis linux yang mencakup sistem operasi, *middleware*, dan aplikasi[16]. Sistem operasi Android untuk perangkat seluler dikembangkan oleh Open Handset Alliance, yang dipimpin oleh Google. Google meluncurkan distribusi Android pada November 2007. Sebagian besar inti Android dirilis di bawah lisensi opensource Apache tetapi sejumlah besar perangkat lunak aktif Android (seperti seperti Play Store, Google Search, Layanan Google Play, Google Music, dan sebagainya) adalah hak milik dan berlisensi. android saat ini merupakan sistem operasi mobile yang paling banyak digunakan dengan menguasai 76% pasar telepon seluler di seluruh dunia.

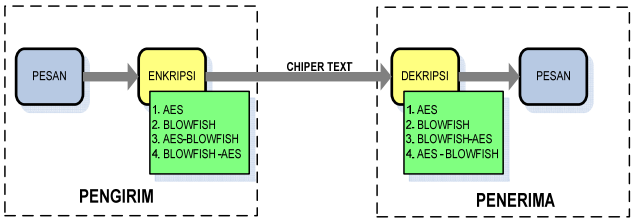
III. METODELOGI PENELITIAN

E. Gambaran Umum Sistem

Aplikasi ini berfungsi untuk mengirim dan menerima SMS yang dinekripsi. Pesan yang akan dikirimkan melalui SMS terlebih dahulu dienkripsi dengan menggunakan AES dan *Blowfish Cipher*, dari proses enkripsi ini akan diperoleh *Ciphertexts*. Untuk dapat membaca SMS penerima harus mendekripsi *cipherteks* dengan kunci yang sama.

Gambaran umum dari sistem yang dibangun dapat dilihat pada Gambar 2. Berikut adalah gambaran sistem secara umum:

1. Pengirim akan mengirim pesan menggunakan layanan SMS.
2. Pesan akan dienkripsi menggunakan AES dan Blowfish.
3. SMS nantinya akan diterima oleh penerima SMS dalam keadaan terenkripsi.
4. Untuk mengetahui makna dari SMS yang di terima penerima harus melakukan enkripsi terlebih dahulu.



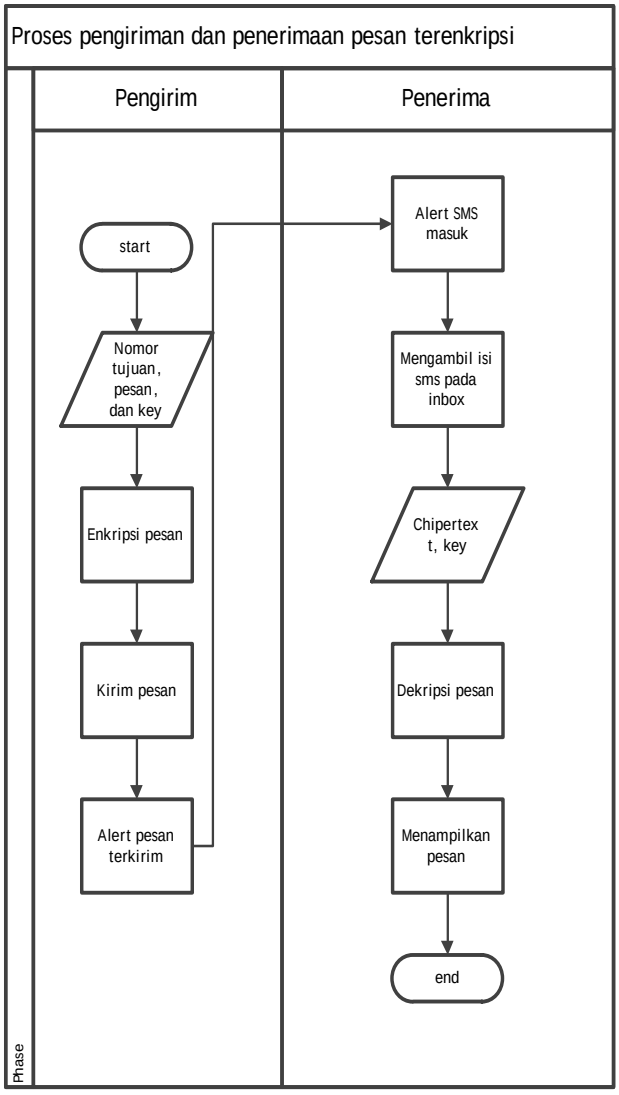
Gambar 2. Gambaran Umum Sistem

Cara kerja sistem ini akan dibagi ke dalam beberapa proses utama seperti terlihat dalam Gambar 2. Proses ini dibagi menjadi empat tahapan yaitu enkripsi pesan, pengiriman pesan, pembacaan pesan, dan dekripsi pesan. Dimana pada perangkat pengirim terjadi proses enkripsi pesan SMS dengan 4 pilihan skenario enkripsi pesan, setelah proses enkripsi selesai barulah cipher text dikirimkan ke perangkat penerima. Pada perangkat penerima user mengambil pesan dari *inbox* memilih skenario dekripsi pesan SMS selanjutnya sistem akan menampilkan hasil dekripsi pesan. Proses untuk enkripsi dan dekripsi pesan dengan skrenario pertama

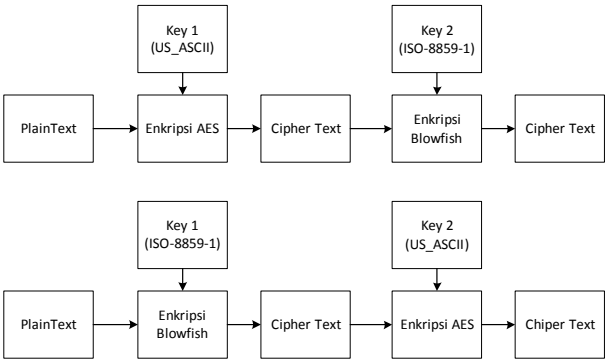
1. Proses Enkripsi

Ekripsi menggunakan pesan SMS sebagai *plaintext* dan password sebagai *Key.* Terdapat 2 password yang diinputkan dimana password ke 1 digunakan sebagai *key* ke 1 dan password ke 2 digunakan sebagai *key* ke 2. Key ke 1 berfungsi sebagai key untuk enkripsi AES dan Blowfish. Untuk proses enkripsi menggunakan 1 algoritma dapat di lihat pada gambar 4.

Key ke 1 juga berfungsi sebagai *key* untuk algoritma pertama yang digunakan proses enkripsi AES -Blowfish dan Blowfish – AES. *Key* ke 2 digunakan sebagai *key* untuk algortima ke 2 dalam enkripsi AES-Blowfish dan Blowfish-AES. Proses enkripsi dengan 2 algoritma dapat di lihat pada gambar 5.



Gambar 3. Proses Pengiriman dan Penerimaan Pesan Terenkripsi

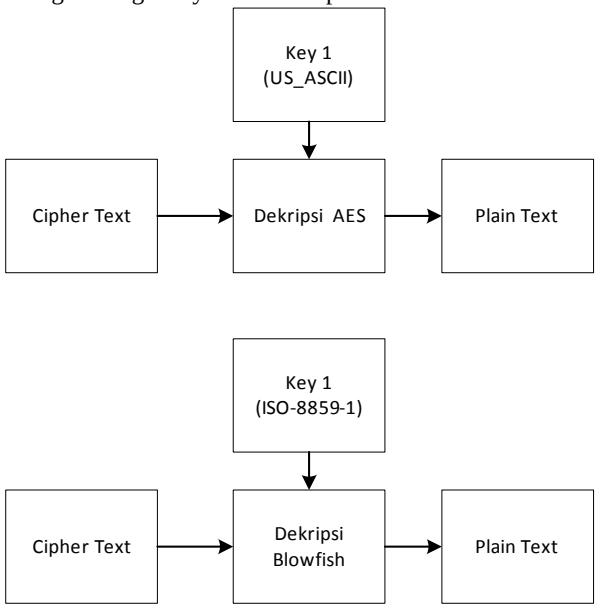


Gambar 5. proses enkripsi dengan 2 algoritma

Password yang di inputkan nantinya akan di rubah ke format *byte* dan hanya 16 karakter pertama yang digunakan sebagai key karena AES dan blowfish menggunakan *key* berukuran 128 bit. Untuk algorima AES menggunakan set karakter US_ASCII sedangkan Blowfish menggunakan set karakter ISO-8859-1. Pesan SMS yang di inputkan user akan menjadi plaintext di dalam sistem. Proses selanjutnya adalah melakukan enkripsi plaintext dengan key yang sudah di masukkan. Proses enkripsi menggunakan javax.crypto yang merupakan library yang disediakan java untuk proses enkripsi dan dekripsi data. *Cipher* text hasil enkripsi inilah yang nantinya akan di kirimkan ke penerima

2. Proses Dekripsi

Dekripsi menggunakan pesan SMS yang diterima sebagai *chipertext* dan password sebagai *Key*. Terdapat 2 password yang diinputkan dimana password ke 1 digunakan sebagai *key* ke 1 dan password ke 2 digunakan sebagai *key* ke 2. Key ke 1 berfungsi sebagai key untuk enkripsi AES dan Blowfish.

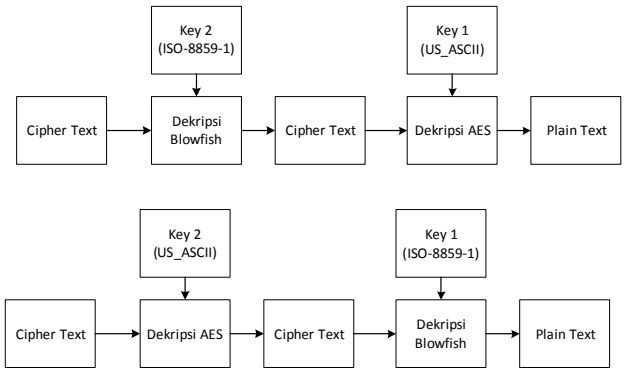


Gambar 6. proses dekripsi dengan satu algoritma

Key ke 1 berfungsi sebagai *key* untuk algoritma kedua yang digunakan proses enkripsi AES - Blowfish dan Blowfish – AES. *Key* ke 2 digunakan sebagai *key* untuk algortima

Gambar 4. proses enkripsi dengan satu algoritma

pertama dalam enkripsi AES-Blowfish dan Blowfish-AES. Proses dekripsi SMS dapat di lihat pada gambar berikut ini.



Gambar 7. proses dekripsi dengan dua algoritma

Password yang di inputkan nantinya akan di rubah ke format *byte* dan hanya 16 karakter pertama yang digunakan sebagai *key* karena AES dan blowfish menggunakan *key* berukuran 128 bit. Untuk algorima AES menggunakan set karakter US_ASCII sedangkan Blowfish menggunakan set karakter ISO-8859-1. Pesan SMS yang diterima *user* akan menjadi *ciphertext* di dalam sistem. Proses selanjutnya adalah melakukan dekripsi *ciphertext* dengan key yang sudah di masukkan. Proses dekripsi menggunakan javax.crypto yang merupakan library yang disediakan java untuk proses enkripsi dan dekripsi data. Hasil dari proses dekripsi berupa *plaintext* SMS yang isinya dapat dipahami pengguna.

IV.HASIL DAN PEMBAHASAN

A. Implementasi Sistem

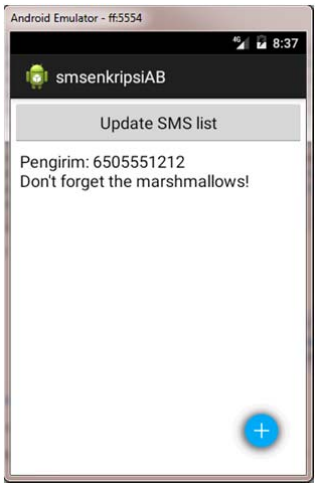
Aplikasi enkripsi sms ini membutuhkan beberapa *Permission* yang di ijinkan oleh pengguna perangkat android. *Permission* ini deperlukan agar aplikasi yang di buat dapat menggunakan beberapa fungsi dasar yang dimiliki oleh telepon selular berbasis android seperti fungsi mengirim dan menerima pesan. Berikut adalah *permission* yang digunakan dalam aplikasi:

TABEL 1.
DAFTAR *PERMISSION*

No	*Permission*	Keterangan
1	WRITE_SMS	Mengizinkan aplikasi menulis pesan SMS
2	READ_SMS	Mengizinkan aplikasi membaca pesan SMS.
3	RECEIVE_SMS	Mengizinkan aplikasi menerima pesan SMS.
4	SEND_SMS	Mengizinkan aplikasi mengirim pesan SMS.
5	READ_CONTACTS	Mengizinkan aplikasi membaca data kontak pengguna.

1. Halaman Utama

Halaman Utama (main) merupakan tampilan awal pertama kali user menjalankan aplikasi.Halaman ini menampilkan dua buah pilihan yaitu, pada pilihan pertama adalah tombol kirim pesan dimana berfungsi sebagai pembuka ke tampilan halaman kirim pesan.Sedangkan pilihan yang kedua adalah tombol Update SMS List dimana berfungsi untuk menampilkan pesan yang diterima.



Gambar 8.Tampilan Halaman Utama

2. Halaman Kirim Pesan

Halaman kirim pesan merupakan form dimana user menginputkan nomor penerima, password dan pesan plaintext yang akan dikirimkan pada bagian-bagian yang telah disediakan dan terdapat pula tombol send SMS untuk mengirimkan pesan. Pesan secara otomatis akan dienkripsi ketika user menekan tombol send SMS. Uji coba pengiriman pesan menggunakan data berikut :

isi pesan : ia
Key ke 1 : Kunci
Key ke 2 : Rahasia

Proses pengiriman pesan pada aplikasi ini dilakukan sebanyak 4 kali yaitu menggunakan algoritma AES, Blowfish, AES Blowfish dan Blowfish AES dimana algoritma AES dan Blowfish melakukan enkripsi menggunakan hanya 1 Key yaitu Key pertama sebagai *Password.* Algoritma AES-Blowfish dan Blowfish-AES menggunakan 2 buah key dimana Password 1 sebagai key untuk algoritma pertama dan password 2 sebagai key untuk algoritma ke 2.

Gambar 9. Tampilan Halaman kirim pesan

Seperti yang terlihat pada gambar yang dilakukan pada emulator android adalah mengirimkan pesan "ia" dengan password "Kunci" dan password ke 2 "Rahasia" ke nomor penerima. Selanjutnya dilakukan proses pengiriman SMS dimana data yang dikirimkan adalah hasil enkripsi yang tersimpan pada variabel pesan

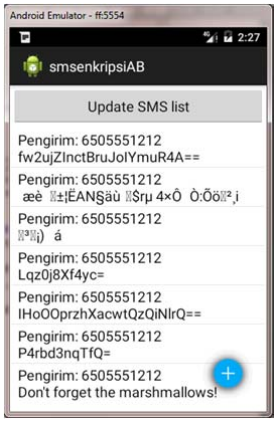
Untuk proses enkripsi metode AES- Blowfish dan Blowfish-AES dilakukan dengan cara melakukan enkripsi terlebih dahulu untuk algoritma pertama dan dilanjutkan dengan enkripsidengan metode ke 2. Hasil enkripsi SMS tersebut dapat di lihat pada tabel 1. Berikut

TABEL 2.
HASIL ENKRIPSI

Metode	Hasil Enkripsi
AES	IHoOOprzhXacwtQzQiNlrQ==
Blowfish	™³‹¡)á
AES - Blowfish	æè ±¦ËAN§äù œ$rµ 4×Ô Ò:Õöš²¸i
Blowfish - AES	MquOpVAr+iXxAdXq4lOalg==

3. Halaman Baca Pesan

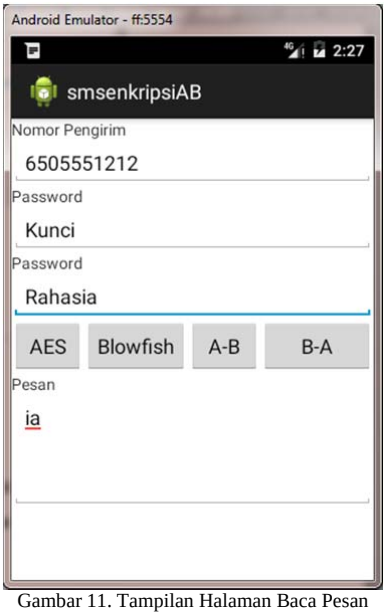
Halaman baca pesan merupakan halaman untuk membaca pesan ciphertext yang telah berhasil dikirimkan. Untuk membaca pesan, user terlebih dahulu harus memilih pesan yang hendak dibaca melalui halaman utama dengan memilih update SMS.



Gambar 10. Proses memilih pesan yang akan dibaca

Proses selanjutnya adalah menentukan kolom yang akan diambil, dalam aplikasi ini hanya memerlukan 2 kolom yaitu kolom pengirim dan isi SMS. Kemudian pilih pesan yang ingin dibaca dan masukkan password untuk membaca pesan. Ketika user menekan tombol buka SMS (password benar), maka ciphertext akan otomatis didekripsikan oleh sistem dan pesan plaintext akan di munculkan.

Terdapat 4 proses dekripsi yaitu dekripsi algoritma AES, Blowfish, AES-Blowfish dan Blowfish AES. dibagi menjadi tahap. Tahap yang pertama adalah melakukan dekripsi dengan metode BLOWFISH. Hasil proses enkripsi tersebut akan ditampilkan seperti pada gambar berikut :

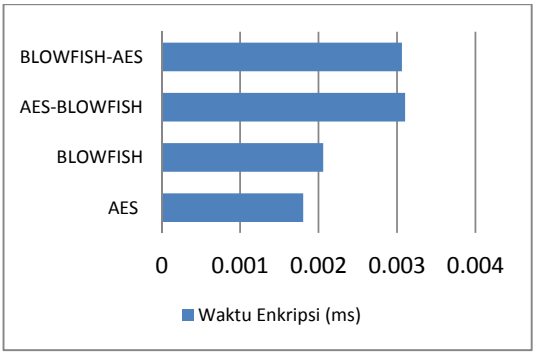


Gambar 11. Tampilan Halaman Baca Pesan

B. Pengujian

1. Waktu Enkripsi

Pengujian ini dilakukan untuk menguji waktu yang diperlukan untuk melakukan enkripsi terhadap pesan yang dikirim. Pengujian dilakukan dengan cara mengenkripsi sms yang akan dikirim sebanyak 50 SMS untuk masing-masing metode. Perbandingan rata-rata waktu yang diperlukan untuk melakukan enkripsi untuk masing –masing metode ditunjukkan pada gambar 12.



Gambar 12. Grafik Waktu Enkripsi

Berikut adalah rata-rata waktu yang diperlukan dalam melakukan enkripsi pesan untuk masing masing metode :

TABEL 3
RATA – RATA WAKTU ENKRIPSI

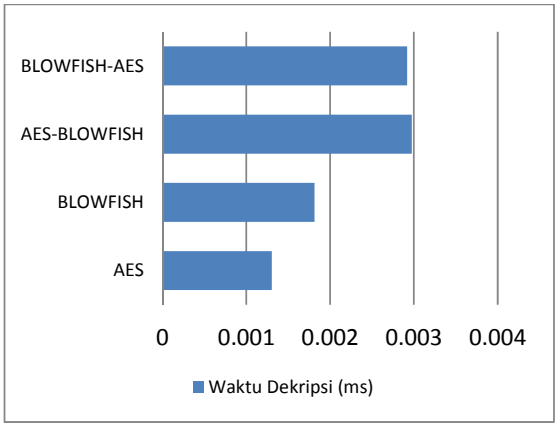
Metode	Waktu Enkripsi(ms)
AES	0.001806421
Blowfish	0.002057949
AES - Blowfish	0.003103601
Blowfish - AES	0.003061534

Berdasarkan tabel 2 dapat di lihat bahwa rata-rata waktu enkripsi AES paling cepat yaitu 0.001806421ms, diikuti oleh Blowfish dengan waktu 0.002057949ms, Blowfish – AES

dengan waktu 0.003061534ms dan AES-Blowfish dengan waktu 0.003103601ms.

2. Waktu Dekripsi

Pengujian ini dilakukan untuk menguji waktu yang diperlukan untuk melakukan dekripsi terhadap pesan yang diterima. Pengujian dilakukan dengan cara mendekripsi sms yang diterima sebanyak 50 SMS untuk masing-masing metode. Perbandingan rata-rata waktu yang diperlukan untuk melakukan dekripsi untuk masing –masing metode ditunjukkan pada Gambar 12.



Gambar 13. Grafik Waktu Dekripsi

Berikut adalah rata-rata waktu yang diperlukan dalam melakukan dekripsi pesan untuk masing masing metode :

:

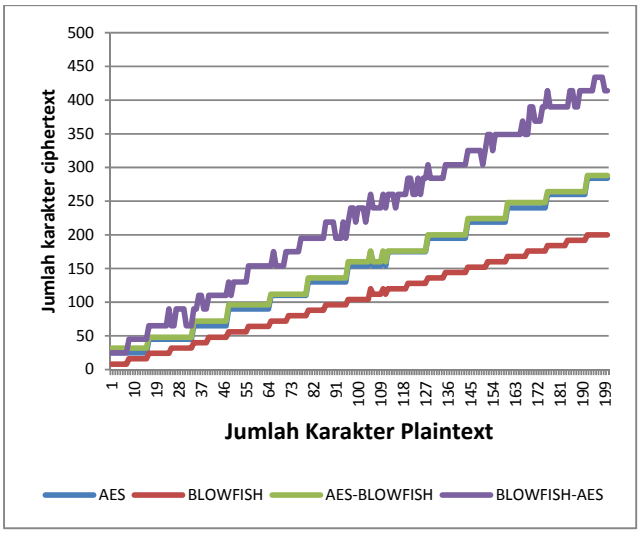
TABEL 4
RATA – RATA WAKTU DEKRIPSI

Metode	Waktu Dekripsi(MS)
AES	0.001302577
Blowfish	0.001813395
AES - Blowfish	0.002974939
Blowfish - AES	0.002918556

Berdasarkan tabel 3 dapat di lihat bahwa rata-rata waktu dekripsi AES paling cepat yaitu 0.001302577ms, diikuti oleh Blowfish dengan waktu 0.001813395ms, Blowfish – AES dengan waktu 0.002974939ms dan AES-Blowfish dengan waktu 0.002918556ms.

3. Jumlah Karakter

Jumlah karakter yang dihitung adalah jumah karakter SMS setelah mengalami proses enkripsi. Pengujian ini menggunakan 800 SMS yang dipilah sesuai dengan algoritma yang digunakan. Grafik panjang karakter dapat dilihat pada gambar 13



Gambar 14. Grafik Panjang Karakter

Berdasarkan grafik di atas terlihat bahwa algoritma Blowfish adalah yang memiliki ukuran panjang SMS yang peling kecil. Antara algoritma AES maupun AES-Blowfish memiliki ukuran panjang SMS yang hampir sama. Sedangkan algoritma Blowfish dan AES memiliki ukuran panjang SMS yang paling besar. Berikut adalah rata-rata panjang karakter hasil proses enkripsi SMS untuk masing masing metode :

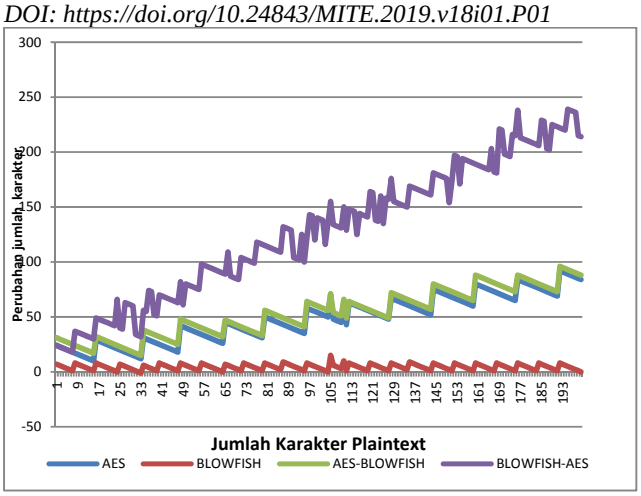
TABEL 5
RATA – RATA PANJANG KARAKTER

Metode	Panjang Karakter
AES	149.205
Blowfish	104.92
AES - Blowfish	154.08
Blowfish - AES	228.51

Berdasarkan tabel 4 dapat di lihat bahwa rata-rata panjang karakter yang paling kecil adalah Blowfish yaitu 104,92 karakter, diikuti oleh AES dengan panjang Karakter 149,25, AES-Blowfish dengan panjang karakter 154,08 dan Blowfish-AES dengan panjang karakter 228.51.

4. Perubahan Jumlah Karakter

Proses enkripsi membuat jumlah karakter SMS berbeda dengan jumlah karakter setelah prosea enkripsi. Pengujian perubahan jumlah karakter ini membandingkan jumlah karakter sebelum di enkripsi dan setelah di enkripsi. berikut adalah grafik yang menggambarkan perubahan panjang karakter tersebut



Gambar 15 Grafik Perubahan Panjang Karakter

Berikut adalah rata-rata panjang karakter hasil proses enkripsi SMS untuk masing masing metode :

TABEL 6
RATA – RATA PERUBAHAN PANJANG KARAKTER

Metode	Panjang Karakter
AES	48,705
Blowfish	4,42
AES - Blowfish	53,58
Blowfish - AES	128,01

Berdasarkan tabel 5 algoritma Blowfish memiliki perubahan panjang data yang sangat kecil apabila dibandingkan dengan algoritma AES, dimana rata-rata perubahan panjang yang terjadi adalah 4,42 karakter dan pada kasus tertentu tidak mengalami perubahan ukuran panjang atau mengalami pengurangan ukuran. Perubahan panjang karakter untuk AES dan AES – Blowfish juga sangat kecil. AES memiliki rata-rata perubahan panjang karakter sebesar 48,705 sedangkan AES-Blowfish sebesar 53,58 karater. Hal ini membuktikan bahwa data yang di enkripsi menggunakan metode blowfish memiliki perubahan yang tidak terlalu besar.

V. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian yang berjudul "Rancang Bangun Sistem Enkripsi Dan Dekripsi SMS Menggunakan AES Dan BLOWFISH Cipher Serta Kombinasinya Pada Telepon Seluler Berbasis Android" ini yaitu :

1. AES memiliki rata-rata waktu enkripsi dan dekripsi paling cepat yaitu 0.0018064211ms untuk enkripsi serta 0.001302577ms untuk dekripsi, diikuti oleh Blowfish dengan waktu enkripsi 0.002057949ms serta 0.001813395ms untuk dekripsi, Blowfish-AES dengan waktu enkripsi 0.003061534ms serta waktu dekripsi 0.002974939ms, dan AES-Blowfish dengan waktu enkripsi 0.003103601ms serta waktu dekripsi 0.00297493958ms.
2. Blowfish memiliki jumlah rata-rata karakter paling kecil yaitu 104,92 karakter, diikuti oleh AES dengan panjang karakter 149,25, AES-Blowfish dengan panjang karakter 154,08 dan Blowfish-AES dengan panjang karakter 228.51.
3. Algoritma Blowfish memiliki rata-rata perubahan panjang karakter paling kecil yaitu sebesar 4,42 karakter per SMS sedangkan algoritma AES yang memiliki rata-rata perubahan panjang karakter sebesar 48,705, algoritma AES-Blowfish memiliki rata-rata perubahan panjang karakter sebesar 53,58 karakter, dan Blowfish-AES memiliki rata-rata perubahan panjang karakter sebesar 128,01 karakter.

REFERENSI

[1]. Dinesh R. Gawade, Amardeep A.Shirolkar, Sagar R. Patil. "E-Voting System Using Mobile SMS". *International Journal of Research in Engineering and Technology*, Volume: 04 Issue: 09, 2015.
[2]. Wadhaval Ashish, Rugved Mehta dan Ashlesha Gawade. "Mobile Commerce and Related Mobile Security Issues". *International Journal of Engineering Trends and Technology (IJETT).* Vol 4. Issue 4. 2013.
[3]. Gudimetla, Sai Dharma Reddy, Buddharaju Shanmukh Varma, Sai Raghukanth Reddy Gudimetla "A Secure Protocol for M-commerce Secure SMS Mobile Payment". *International Journal of Science Engineering and Advance Technology, IJSEAT*, Vol. 4, Issue 4. 2016.
[4]. S.Jyothirmai, J. Lingaiah, M.Raviteta.. "Design and Implementation of an SMS Based Home Security System". *International Journal of Innovative Technologies Volume.*04, Issue No.17. 2016.
[5]. Ruby, Beulah PW, S.Abinashrajasingh, N.Ganeshprasad, "GSM Based Vehicle Theft Control System". *International Journal of Science, Engineering and Technology Research (IJSETR),* Volume 7 Issue 4, 2018.
[6]. Bo Li dan Gyu Im.. "Smartphone Promising Battlefield for Hackers". *Journal of Security Engineering* Vol 8 No.1. 2011
[7]. Sharad Kumar Verma dan Dr. D.B. Ojha.. "An Approach To Enhance The Mobile Sms Security". *Journal of Global Research in Computer Science.* Vol 5, No. 5. 2014.
[8]. Nishika dan Rahul Kumar Yadav. "A Lookup Table Based Secure Cryptographic SMS Communication on Android Environment". *International Journal of Computer Science and Mobile Computing* Vol. 2,Issue 6. 2013.
[9]. Patil Anjali dan Rajeshwari Goudar. "Sensitive Data Storage in Wireless Devices Using AES Algorithm". *International Journal Of Engineering And Computer Science.* Volume 2 Issue 9. 2013.
[10]. Nivedita Bisht dan Sapna Singh.. "A Comparative Study of Some Symmetric and Asymmetric *Key* Cryptography Algorithms". *International Journal of Innovative Research in Science Engineering and Technology* Vol. 4 Issue 3. 2015.
[11]. Ezeofor C. J. dan Ulasi A. G. "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems". *International Journal of Innovative Research in Science, Engineering and Technology.* Vol. 3, Issue 12. 2014.
[12]. Ratna Kumari, U.V, Santosh Pokhrel, dan Hyndavi Anusha Anche. "Blowfish Algorithm-Securing The Future". *Journal of The International Association of Advanced Technology and Science.* Vol. 1. 2015
[13]. Sravana Kumar D, P. Sirisha dan CH Suneetha.. "Cascade Block Cipher Using Braiding/Entanglement Of Spin Matrices And Bit Rotation". *International Journal of Network Security & Its Applications (IJNSA).* Vol.8, No.2. 2016.
[14]. Shital D.Rautkar dan Dr. Prakash S. Prasad. "An Overview of Real Time Secure SMS Transmission". *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 4, Issue 1. 2015.
[15]. Simar Preet Singh, dan Raman Maini.. "Comparison Of Data Encryption Algorithms". *International Journal of Computer Science and Communication.* Vol. 2, No. 1. 2011.
[16]. Safaat. H, Nazruddin *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Bandung: Informatika Bandung. 2011.

[HALAMAN INI SENGAJA DIKOSONGKAN]