IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA *BLOWFISH* UNTUK KEAMANAN ISI *NOTES* BERBASIS ANDROID

Sandi[1)], Ferdiansyah[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : sandi_ku91@yahoo.com[1)], ferdiansyah@budiluhur.ac.id[2)]

Abstrak

Masalah data informasi telah menjadi masalah penting pada era perkembangan teknologi informasi seperti sekarang ini terutama informasi pesan pada smartphone maupun tablet. Terkadang data pesan ini harus bersifat rahasia agar tidak diketahui oleh orang yang tidak berkepentingan. Apabila data tersebut diketahui, maka dapat disalahgunakan demi kepentingan pribadi yang dapat menyebabkan kerugian pada perusahaan maupun pribadi. Di era digital ini, teknologi berbasis android berkembang begitu cepat. Saat ini menyimpan catatan singkat baik bersifat umum dan pribadi tidak membutuhkan buku dan pena lagi. Kita dapat menyimpannya di smartphone karena hampir semua masyarakat memilikinya. Pada laporan tugas akhir ini penulis membuat aplikasi kriptografi notes untuk mengenkripsi teks pesan yang bersifat rahasia pada PT. Nutrindo Grahahusada Utama, yang akan digunakan untuk menyimpan semua catatan kerja diperusahaan yang bersifat rahasia dan catatan penting lainnya. Kerahasiaan informasi catatan tersebut tentunya tidak ingin diketahui dan dicuri oleh orang lain. Maka dari itu dibutuhkannya suatu sistem keamanan yang dapat menjaga informasi tersebut yaitu aplikasi note menggunakan kriptografi. Dengan menggunakan kriptografi ini, informasi yang kita simpan dapat dienkripsi dan dideskripsi dengan suatu kunci yang kita inputkan sehingga hanya kita saja yang tahu isi dari informasi tersebut. Aplikasi yang dihasilkan berbasis android yang dapat mengenkripsi isi pesan yang disimpan didatabase dan dapat mendekripsi kembali seperti pesan semula menggunakan algoritma blowfish dengan kunci tertentu.

Kata Kunci : kriptografi, *blowfish*, *notes*, keamanan, android

1. PENDAHULUAN

Perkembangan teknologi pada saat ini sangat berpengaruh besar terhadap segala aspek kehidupan, salah satunya di bidang informasi dan komunikasi seperti dalam proses penyimpanan data. Teknologi berbasis android berkembang begitu cepat pada saat ini. Ditengah berkembang pesatnya teknologi komunikasi tentunya harus diiringi dengan tingkat keamanan yang baik pula.

Masalah keamanan dan kerahasiaan informasi merupakan suatu hal yang penting. Tidak menutup kemungkinan adanya pihak ketiga yang ingin mengambil atau merubah isi pesan pada database penyimpanan. karena ikut berkembang pula kejahatan teknologi dengan berbagai macam teknik, seperti penyebaran virus, penyadapan, modifikasi, serangan hacker, dan lain-lain.

PT. Nutrindo Grahahusada Utama merupakan perusahaan yang bergerak di bidang farmasi yaitu distributor obat dan suplemen. Informasi perusahaan yang bersifat rahasia tidak boleh diketahui oleh orang yang tidak berhak agar tidak disalahgunakan dan rahasia perusahaan terjaga.

Informasi perusahaan yang bersifat rahasia tersebut harus terjamin keamanannya. Jika informasi tersebut diketahui oleh pihak yang tidak bertanggung jawab dalam skala yang lebih kompleks, kemungkinan akan menyebabkan kerugian yang cukup besar.

Pada dasarnya, setiap perusahaan pasti memiliki standar keamanan untuk data yang bersifat rahasia. Namun dalam riset ini di jelaskan bahwa banyak karyawan PT. Nutrindo Grahahusada Utama ini menyimpan catatan kerja di *smartphone* mereka karena mudah untuk di akses dan tidak perlu repot menulisnya di buku seperti jaman dahulu, namun pesan atau catatan yang disimpan di *smartphone* ini tidak menggunakan pengamanan apapun, sehingga semua pesan yang disimpan terlihat jelas pada aplikasinya padahal pesan ini harusnya bersifat rahasia agar tidak sampai ke pihak yang tidak berhak untuk mengetahuinya. Salah satu cara untuk melindungi isi pesan tersebut adalah mengembangkan aplikasi *notes* dengan menambahkan proses enkripsi, dimana isi pesan yang akan disimpan ke database akan diberikan kunci dan diganti ke huruf lain dahulu kemudian baru di simpan, untuk membuka isi pesan hanya menginput kunci yang sama pada saat proses enkripsi. Kriptografi menggunakan algoritma *blowfish* merupakan salah satu jenis algoritma yang popular dan cocok digunakan sebagai metode penyembunyian pesan, dimana isi *note* atau pesan yang akan disimpan diacak terlebih.

2. METODE PENELITIAN

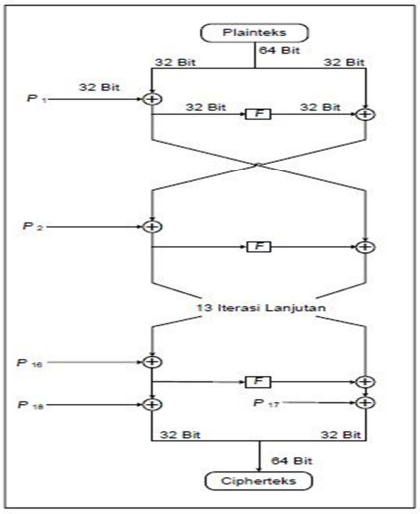
2.1. Kriptografi

Kriptografi berasal dari bahasa yunani yaitu *cryptos* yang artinya *secret* (rahasia) dan *graphein* yang artinya *writing* (tulisan). Prinsip-prinsip yang mendasari kriptografi yakni : *Confidentiality* (kerahasiaan), *Data integrity* (keutuhan data), *Authentication* (otentikasi) dan *Non repudiation* (anti penyangkalan). Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi : Pesan *plaintext* dan *ciphertext,* pengirim dan penerima, enkripsi dan dekripsi, *cipher* dan kunci, dan penyadap [3]. Beberapa algoritma simetris antara lain : DES, AES, RC4, RC6, IDEA, Blowfish, dan lain sebagainya. Algoritma asimetris adalah suatu algoritma kriptografi dimana kunci yang digunakan untuk enkripsi dengan dekripsi berbeda. Kunci enkripsi dinamakan sebagai kunci *public* yaitu kunci yang bebas di ketahui oleh siapapun, sedangkan kunci dekripsi dinamakan kunci *privat* yaitu kunci yang hanya boleh di ketahui oleh penerima pesan. Beberapa algoritma asimetris antara lain : RSA, Difflie Hellman, dan lain sebagainya [2].

2.2. Algoritma *Blowfish*

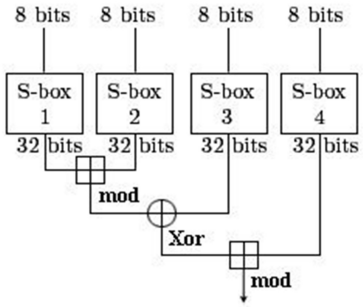
Blowfish adalah algoritma yang menerapkan *Feistel Network* yang terdiri dari 16 putaran. *Blowfish* merupakan *cipher* blok 64 bit dengan panjang kunci variabel. Operasi berbentuk penambahan dan XOR pada variable 32 bit. Tambahan operasi lainnya hanya empat penelusuran tabel *(table look-up) array* berindeks untuk setiap putaran. *Blowfish* menggunakan teknik kunci sembarang, Ukuran kunci yang dapat diterima oleh *blowfish* adalah antara 32 bit hingga 448 bit menjadi beberapa *array* subkunci atau *subkey* dengan total 4168 *byte*, dengan ukuran *default* sebesar 128 bit [4].

Untuk proses enkripsi algoritma *blowfish* dapat dilihat pada Gambar 1 berikut.



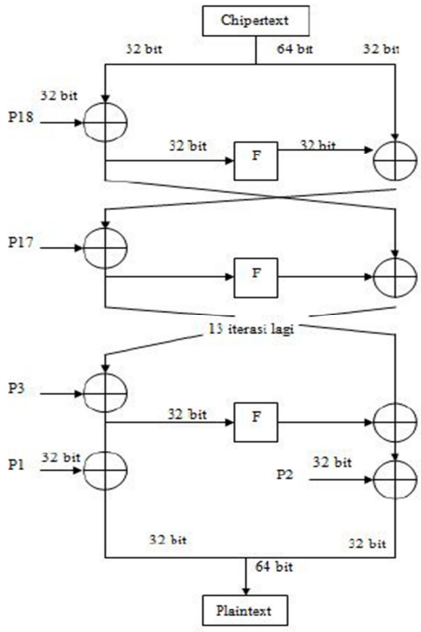
Gambar 1 : Proses Enkripsi Algoritma Blowfish

Berikut Gambar 2 fungsi F yang terdapat pada jaringan *Feistel.*



Gambar 2 : Skema fungsi F pada algoritma blowfish

Untuk proses dekripsi algoritma *bowfish* sama persis dengan proses enkripsi, kecuali P_1, P_2,…, P_{18} digunakan pada urutan yang berbalik *(reverse)*. namun sebagai masukannya adalah *ciphertext* [5]. Berikut Gambar 3 proses dekripsi algoritma *blowfish.*



Gambar 3 : Proses Dekripsi Algoritma Blowfish

2.3. *Notes*

Notes atau buku catatan adalah buku yang ukurannya lebih kecil daripada buku tulis, berfungsi untuk menulis catatan-catatan yang dianggap penting biasanya berisikan berbagai hal seperti kegiatan sehari-hari, rencana untuk kedepan, informasi penting, pesan bersifat rahasia, dan lain sebagainya [1].

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Analisa Masalah

Di zaman yang berkembang ini banyak sekali orang, organisasi, dan perusahaan yang memanfaatkan teknologi untuk memudahkan pekerjaan dalam kehidupan sehari-hari seperti melakukan pencatatan dan penyimpanan pesan informasi. Akan tetapi kemudahan tersebut tidak menjamin keamanan serta keutuhan data yang disimpan. Banyak peluang yang dimanfaatkan pihak-pihak tidak bertanggung jawab untuk mencuri atau mendapatkan data yang bukan haknya untuk kepentingan pribadi maupun organisasi.

PT. Nutrindo Grahahusada Utama merupakan sebuah perusahaan yang mempunyai kualitas untuk memproduksi berbagai macam suplemen dan obat untuk didistribusikan di hampir seluruh wilayah Indonesia. Yang menjadi masalah adalah banyaknya karyawan yang melakukan pencatatan-pencatatan pekerjaan yang bersifat rahasia pada *smartphone* masing-masing terutama pada divisi *finance accounting* yang seharusnya bersifat rahasia. Dimana catatan tersebut tidak ada pengamanan sama sekali besar kemungkinan dapat diketahui pihak-pihak atau divisi lain yang tidak berhak. Karena tingkat kerahasiaan divisi *accounting* yang sangat tinggi maka dibutuhkan sebuah aplikasi untuk mengamankan catatan-catatan rahasia perusahaan yang disimpan dengan cara penyandian atau mengganti isi pesan yang disimpan yang disebut kriptografi.

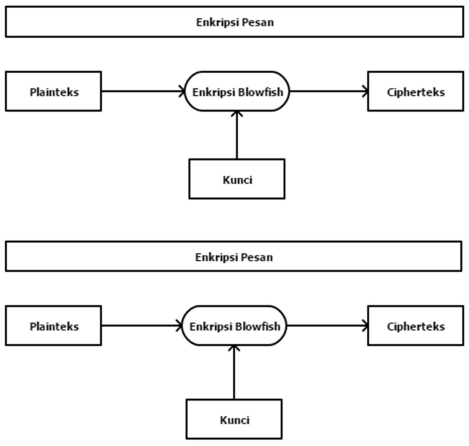
3.2 Penyelesaian Masalah

Penyelesaian masalah dari permasalahan yang diuraikan di atas, maka dibutuhkan aplikasi untuk mengamankan informasi pesan yang disimpan menggunakan *smartphone* android serta dapat diakses dengan menggukan komputer. Dalam proses enkripsi dan dekripsi teks berbasis android ini menggunkan algoritma *blowfish*.

Keamanan teks ini diproses dengan cara mengacak atau mengganti isi pesan menggunakan *secret key*, sehingga isi pesan akan berubah dalam bentuk yang berbeda. Setelah pesan berhasil di enkripsi, kemudian hasil enkripsi tersebut dapat disimpan pada database. Untuk mengembalikan pesan tersebut dilakukan dengan proses dekripsi lawan dari proses enkripsi dimana untuk melakukan prosesnya dibutuhkan *secret key* yang sama pada saat melakukan proses enkripsi, sehingga isi pesan dapat dibuka tanpa mengalami perubahan akan kembali seperti isi pesan semula.

3.3 Penyelesaian Masalah

Teknik kriptografi dalam penggantian isi pesan dan mengembalikan pesan menjadi pesan asli, terdiri dari dua proses, yaitu proses *encrypt* dan *decrypt*. Berikut adalah gambaran sederhana proses penggantian pesan dan mengembalikan pesan menjadi pesan asli kembali, berikut Gambar 4 desain konsep aplikasi.



Gambar 4 : Desain Konsep Aplikasi

Gambar di atas menjelaskan secara sederhana proses yang ada di dalam aplikasi. di mana di dalamnya terdapat proses enkripsi dan proses dekripsi pesan. Di dalam proses enkripsi pesan, terdapat proses enkripsi *blowfish*, di mana dalam proses tersebut membutuhkan dua input yaitu pesan yang masih berupa *plaintext*, dan *key* untuk melakukan proses enkripsi *blowfish*. Output dari proses enkripsi *blowfish* ini adalah *ciphertext*. *Ciphertext* ini nantinya akan digunakan untuk proses dekripsi *blowfish*. Sama dengan proses enkripsi *blowfish*, dalam proses dekripsi *blowfish* membutuhkan dua input, namun dalam proses dekripsi *blowfish*, yang menjadi input adalah *ciphertext* hasil dari enkripsi *blowfish* tadi, dan *key*. Output dari proses ini akan menghasilkan *plaintext* kembali.

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Aplikasi

Pada bagian ini akan diuraikan mengenai tampilan layar aplikasi, mulai dari pertama dijalankan sampai selesai. Berikut ini akan diberikan penjelasan pada setiap Gambar tentang tampilan-tampilan yang ada pada aplikasi ini.

a. Tampilan Layar *Splash Screen*

Ini adalah tampilan yang pertama kali muncul saat membuka aplikasi *notes* sebelum masuk ke dalam aplikasi. Berikut Gambar 5 merupakan layar *splash screen*.

Gambar 5 : Tampilan Splash Screen

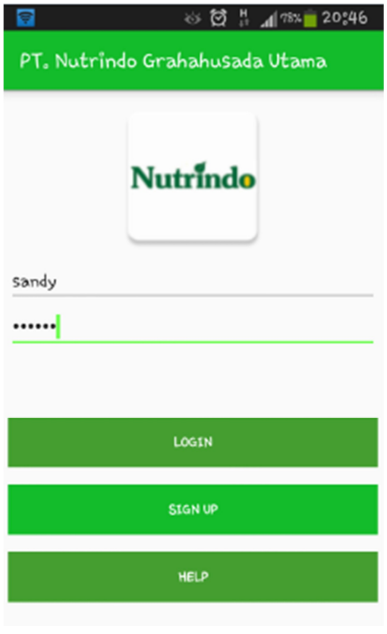
b. Tampilan Layar *Sign Up*

Layar *sign up* ini berfungsi untuk membuat membuat *user* baru, agar mendapatkan *user ID* untuk melakukan *login* pada aplikasi, berikut adalah Gambar 6 merupakan layar *sign up*.

Gambar 6 : Tampilan Layar Sign Up

c. Tampilan Layar *Login*

Pada tampilan ini menu *login* berfungsi untuk masuk ke dalam aplikasi. *User* dapat memasukan *username* dan *password* pada *field* yang sudah disediakan kemudian menekan tombol *login*. Berikut Gambar 7 merupakan layar *login*.

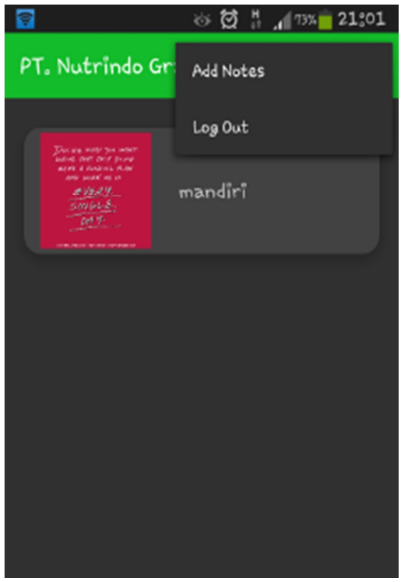


Gambar 7 : Tampilan Layar Login

d. Tampilan *Main Menu*

Pada tampilan layar *main menu* ini, *user* dapat memilih menu yang diinginkan dan dapat melihat isi

notes. Terdapat menu *add notes* dan *log out*. Berikut Gambar 8 merupakan layar *main menu*.



Gambar 8 : Layar Main Menu

e. Tampilan Menu *Add Notes*

Pada tampilan layar a*dd notes* ini, *user* dapat mebuat dan menyimpan *note* ke *server* dengan aman, karena di menu ini pesan asli akan di enkripsi dan disimpan dalam bentuk *ciphertext* dengan mengkombinasikan antara pesan asli dan *key*. Berikut Gambar 9 merupakan layar *add notes*.

Gambar 9 : Tampilan Menu Add Notes

Berikut Gambar 10 tampilan *note* yang berhasil di simpan dan akan otomatis tampil di *main menu*.

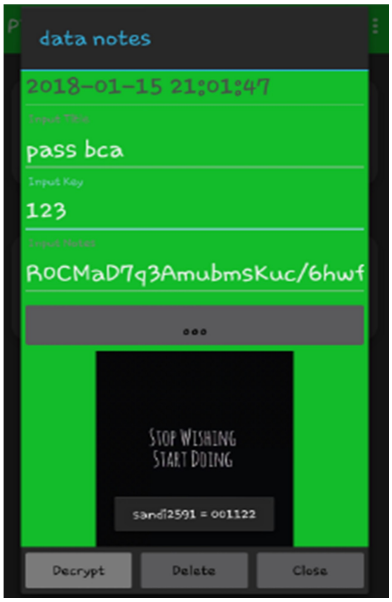
Gambar 10 : Tampilan Note yang berhasil di simpan

f. Tampilan Menu *Decrypt Notes*

Pada tampilan layar *decrypt notes* ini, *user* dapat mengembalikan pesan asli yang disimpan dengan cara *decrypt* kembali *note* yang sudah menjadi *ciphertext*. Caranya input *key* dan pilih tombol *decrypt* maka isi *notes* akan tampil dilayar. Berikut Gambar 11 tampilan layar *decrypt notes*.

Gambar 11 : Tampilan menu Decrypt Notes

Berikut Gambar 12 tampilan note yang berhasil di *decrypt* dan akan langsung tampil di layar.



Gambar 12 : Tampilan Note yang berhasil di decrypt

4.2 Analisa Hasil Implementasi Aplikasi

Berikut merupakan hasil dari percobaan aplikasi *notes*.

a. Tabel *notes* sebelum di enkripsi

Tabel 1 : Isi Notes Sebelum di Enkripsi

Isi Notes Asli		Panjang notes	Key
Title	Isi Notes	(byte)	
pass bca	bca1234	7	bca1
pass bni	bni1234	7	bni1
pass bri	bri1234	7	bri1
pass email	ngusandi101017	14	nutrindo
pass pc	sandi101017	11	nutrindoGU

b. Tabel hasil *notes* setelah di enkripsi

Tabel 2 : Hasil Isi Notes Setelah di Enkripsi

Enkripsi Notes	Panjang enkripsi	Status
Ciphertext Isi Notes	(byte)	
DpgTeBfM01c=	12	Berhasil
wRalR1PDWl4=	12	Berhasil
8bSsZyvSAbg=	12	Berhasil
ynX90gBG/wWNXpHjrRpbaw==	24	Berhasil
bTdRXUTKBLkqiQKJpzDWtw==	24	Berhasil

c. Tabel hasil *notes* setelah di enkripsi

Tabel 3 : Hasil Notes Setelah di Dekripsi

Dekripsi Notes	Key	Status
Plaintext Isi Notes		
bca1234	bca1	Berhasil
bni1234	bni1	Berhasil
bri1234	bri1	Berhasil
ngusandi101017	nutrindo	Berhasil
sandi101017	nutrindoGU	Berhasil

4.3 Evaluasi

Setelah dilakukan analisa dari hasil implementasi aplikasi dapat ditemukan kelebihan dan kekurangan, yaitu sebagai berikut :

a. Aplikasi ini mudah digunakan, karena tampilannya sangat simple dan mudah dimengerti oleh pengguna baru.
b. Aplikasi ini hanya dapat melakukan proses enkripsi dan dekripsi terhadap *text*, belum bisa mengenkrip *type* data yang lain.
c. Aplikasi ini berbasis android yang bisa digunakan melalui *smartphone* kapan saja.
d. Aplikasi ini tidak dapat dijalankan tanpa koneksi internet.
e. Tampilan layar aplikasi masih sederhana.
f. Aplikasi belum bisa melakukan edit isi notes.

5. KESIMPULAN

5.1 Kesimpulan

Dari hasil perancangan dan hasil percobaan aplikasi ini. Dapat diambil kesimpulan sebagai berikut :

a. Implementasi kriptografi menggunakan algoritma *blowfish* untuk keamanan pesan *notes* telah berhasil dilakukan dan bisa di terapkan di PT Nutrindo Grahahusada Utama.
b. Dengan adanya aplikasi ini, pesan yang disimpan pada *smartphone* dapat terjaga kerahasiaanya.
c. Pesan yang sudah disimpan bisa dilihat pada *smartphone* pengguna dimanapun dan kapanpun tanpa harus mengakses komputer.
d. Algoritma *blowfish* cukup aman dan tidak mudah untuk dipecahkan.

5.2 Saran

Selain menarik kesimpulan, adapun saran-saran pengembangan lebih lanjut untuk sistem aplikasi

notes agar berfungsi dengan lebih baik antara lain sebagai berikut :

a. Aplikasi membutuhkan pengembangan lebih lanjut agar lebih sempurna dan terhindar dari berbagai macam *bug* dan *error*.
b. Menambahkan fitur-fitur yang memudahkan pengguna terutama saat membuat dan mendekripsi *notes* yang ditulis.
c. Menambahkan fitur-fitur yang berguna, contoh dibuatkan action untuk *share* isi *notes*.

6. DAFTAR PUSTAKA

[1] D. P. Nasional, 2008, Kamus Besar Bahasa Indonesia Pusat Bahasa, Gramedia Pustaka Utama.
[2] Dony. Ariyus, 2008, *Pengantar Ilmu Kriptografi*, Yogyakarta, Penerbit Andi.
[3] Munir, Rinaldi, 2006, *Kriptografi*, Bandung, Informatika Bandung.
[4] Schneier, Bruce, 1996, *Applied Cryptography*, Second Edition, New Jersey, John Wiley & Sons.
[5] Schneier, Bruce, 1994, *Description of a New Variable-Length Key, 64-Bit Block Cipher*, Cambridge, Springer Verlag.
[6] Syafari, Anjar, 2007, *Sekilas Tentang Enkripsi Blowfish*, http://ilmukomputer.org/2007/07/27/sekilas-tentang-enkripsi-blowfish/, 25 Oktober 2017.