APLIKASI ENKRIPSI CATATAN PADA PERANGKAT SMARTPHONE ANDROID DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) DAN METODE VARIANT BEAUFORT CIPHER

SKRIPSI

disusun oleh

Dixon Claudi

12.11.6276

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019

APLIKASI ENKRIPSI CATATAN PADA PERANGKAT SMARTPHONE ANDROID DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) DAN METODE VARIANT BEAUFORT CIPHER

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika

disusun oleh

Dixon Claudi

12.11.6276

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019

PERSETUJUAN

SKRIPSI

APLIKASI ENKRIPSI CATATAN PADA PERANGKAT SMARTPHONE ANDROID DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) DAN METODE VARIANT BEAUFORT CIPHER

yang dipersiapkan dan disusun oleh

Dixon Claudi

12.11.6276

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Oktober 2018

Dosen Pembimbing,

Ferry Wahyu Wibowo, S.Si, M.Cs.
NIK. 190302235

PENGESAHAN

SKRIPSI

APLIKASI ENKRIPSI CATATAN PADA PERANGKAT SMARTPHONE ANDROID DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) DAN METODE VARIANT BEAUFORT CIPHER

yang dipersiapkan dan disusun oleh

Dixon Claudi

12.11.6276

telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Juli 2019

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dony Ariyus, M.Kom. **NIK. 190302128**	
Ferry Wahyu Wibowo, S.Si, M.Cs. **NIK. 190302235**	
Kusnawi, S.Kom, M. Eng. **NIK. 190302112**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Juli 2019

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN KEASLIAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 19 Juli 2019

Dixon Claudi

12.11.6276

MOTTO

“Maka hendaklah kalian berpegang teguh dengan Sunnah-ku dan sunnah para khulafaur rasyidin yang mendapat petunjuk.”

(HR Abu Daud)

“Maka sesungguhnya bersama kesulitan ada kemudahan. Sesungguhnya bersama kesulitan ada kemudahan. Maka apabila engkau telah selesai (dari sesuatu urusan), tetaplah bekerja keras (untuk urusan yang lain). Dan hanya kepada Tuhanmulah engkau berharap.”

(QS. Al-Insyirah,6-8)

“Pendidikan merupakan senjata paling ampuh yang bisa kamu gunakan untuk merubah dunia.”

(Nelson Mandela)

“Banyak kegagalan dalam hidup ini dikarenakan orang-orang tidak menyadari betapa dekatnya mereka dengan keberhasilan saat mereka menyerah.”

(Thomas Alva Edison)

“Ilmu pengetahuan itu bukanlah yang dihafal, melainkan yang memberi manfaat.”

(Imam Syafi’i)

“Bencana akibat kebodohan adalah sebesar-besarnya musibah seorang manusia.”

(Imam Al Ghazali)

“Dunia ini ibarat bayangan. Kalau kau berusaha menangkapnya, ia akan lari. Tapi kalau kau membelakanginya, ia tak punya pilihan selain mengikutimu.”

(Ibnu Qayyim Al Jauziyyah)

PERSEMBAHAN

- *Allah SWT yang telah memberikan kesehatan, kemudahan, dan kelancaran dalam penyusunan dan pembuatan skripsi ini.*
- Untuk sang pemberi pencerahan yang sesungguhnya dimana sebagai junjungan umat muslim diseluruh dunia, sang pembawa kesetaraan, kedamaian, dan sebagai panutan menjadi teladan yang sesungguhnya, Nabi Muhammad SAW.
- Kepada kedua orang tua saya Harun dan Sri Sayuti yang tiada henti berdoa dalam setiap sujudnya, pemeras keringat demi kebahagian keturunannya yang masih sering mengecewakan ini dan juga kepada Adik saya King Chaves terima kasih sudah menjadi motivasi untuk penyelesaian skripsi ini. Sungguh kalian adalah motivasi terbesar saya dalam perantauan yang selalu berusaha memberi penghargaan terbaik buat kalian.
- Kepada bapak Ferry Wahyu Wibowo selaku dosen pembimbing skripsi, saya ucapkan terima kasih atas nasihat serta mengarahkan saya sampai skripsi ini selesai dibuat.
- Untuk Semua Dosen STMIK Amikom Yogyakarta yang pernah mengajar saya dari semester 1 sampai semester akhir. Terima kasih atas semua ilmu yang diberikan yang sangat berguna dalam penyelesaian skripsi ini.
- Untuk teman yang sudah membantu untuk lulus Irfan, Eki, Ardan. Terima kasih atas ilmu yang sangat berharga yang sudah kalian bagikan.
- Untuk rekan-rekan seperjuangan dari kelas 12-S1TI-08 yang selalu memberi dorongan dan motivasi, candaan, dan semua pelajaran tentang arti kebersamaan.
- Untuk Agustin Feriana Utari terima kasih atas motivasi dan dukungan yang selalu merasuk di dalam lubuk hati dan selalu sabar serta setia menunggu.

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Segala puji dan syukur kehadirat Allah SWT yang telah melimpahkan karunia, rahmat dan hidayah-Nya kepada saya sehingga dapat menyelesaikan skripsi dengan judul "Aplikasi Enkripsi Catatan Pada Perangkat *Smartphone* Android Dengan Metode AES (Advanced Encryption Standard) Dan Metode Variant Beaufort Cipher". Shalawat dan salam dijunjung untuk nabi Muhammad SAW, sang teladan yang membawa manusia dari zaman kegelapan kedalam zaman yang penuh ilmu yang terang benderang.

Tujuan dari pembuatan aplikasi ini untuk menerapkan ilmu yang didapat ketika kuliah. Skripsi ini disusun sebagai syarat kelulusan untuk memperoleh gelar sarjana pada Program Pendidikan Strata-1 di Universitas AMIKOM Yogyakarta Program Studi Informatika.

Penulis menyadari sepenuhnya bahwa penulisan penelitian ini masih jauh dari sempurna, itu semua karena keterbatasan penulis dalam hal pengetahuan. Besar harapan dikemudian hari skripsi ini akan bermanfaat dan bisa dikembangkan lagi menjadi yang lebih baik.

Wassalamu'alaikum Wr.Wb.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Pada saat ini sebagian besar dari catatan yang tersimpan adalah catatan yang penting dan sangat rahasia seperti penyimpanan password, akun Email, catatan pemasukan/pengeluaran keuangan, dan catatan pribadi lainnya. Oleh karena itu diperlukan fitur pengamanan untuk mengamankan catatan pengguna dari orang lain. Maka dari itu dibuat aplikasi enkripsi catatan dengan menggunakan 2 metode, yakni metode AES (Advanced Encryption Standard) dan metode Variant Beaufort pada sistem operasi Android.

Metode AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaiman block cipher pada umumnya. Sedangkan Metode Variant Beaufort sendiri merupakan salah satu algoritma kriptografi klasik dengan teknik subtitusi, panjang alphabet/char yang diijinkan dalam aplikasi lebih panjang dari yang bisanya 26karakter.

Secara garis besar aplikasi ini mampu mengacak informasi dalam catatan cukup baik, sehingga membuat kerahasian data catatan pengguna terjamin. Selain itu, dalam penyimpanan pada database juga merupakan hasil enkripsi dan bukan teks asli.

Kata Kunci: Aplikasi, Kriptografi, Keamanan, Android, Enkripsi, Dekripsi, Catatan.

ABSTRACT

At present most of the records stored are important and very confidential records such as password storage, Email accounts, financial entry / expenditure records, and other personal records. Therefore, security features are needed to secure user records from others. Therefore, it is made a record encryption application using 2 methods, namely the AES (Advanced Encryption Standard) method and the Beaufort Variant method on the Android operating system.

This AES method is a block cipher algorithm using permutation and substitution systems (P-Box and S-Box) not with Feistel networks as block ciphers in general. While the Variant Beaufort Method itself is one of the classic cryptographic algorithms with substitution techniques, the length of the alphabet / char allowed in the application is longer than the usual 26 characters.

Broadly speaking, this application is able to scramble the information in the record well enough, so that the confidentiality of user record data is guaranteed. In addition, the storage in the database is also the result of encryption and not the original text.

Keyword: *Aplication, cryptography, security, Android, Encryption, Decryption, Note.*