

**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

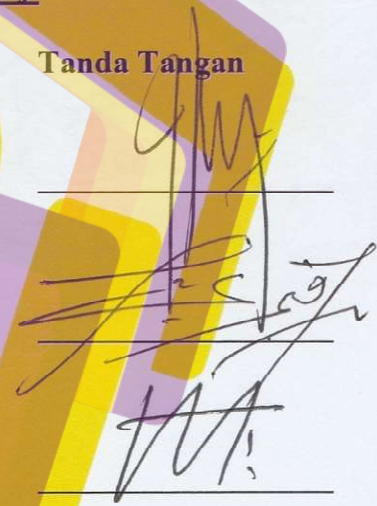
Nama Penguji

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, pemerasa keringat demi kebahagiaan 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 kehadiran 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.

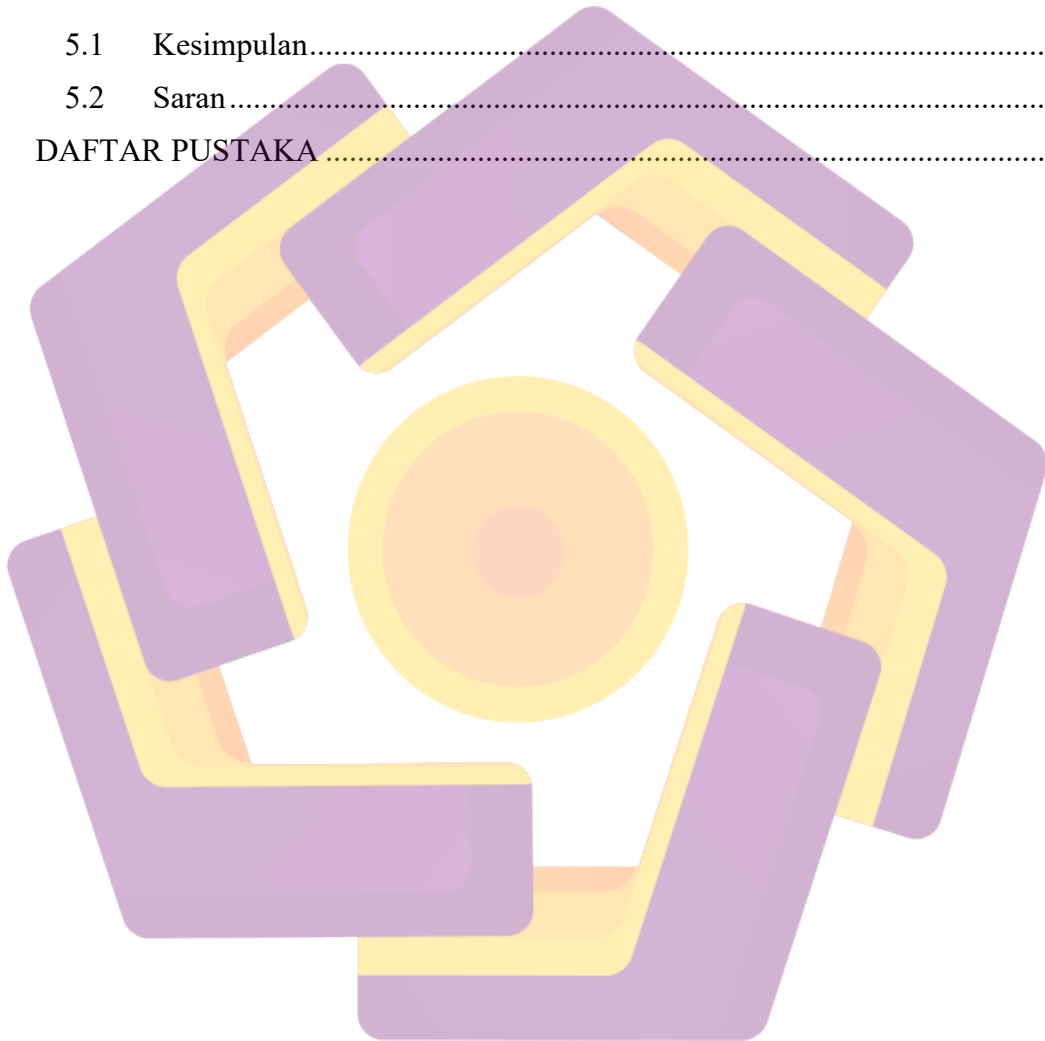
Wassalamu'alaikum Wr.Wb.

DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN KEASLIAN.....	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
INTISARI.....	xiv
<i>ABSTRACT</i>	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Penelitian.....	3
1.7 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	7
2.1 Tinjauan Pustaka	7
2.2 Kriptografi	8
2.2.1 Pengenalan Kriptografi	8
2.2.2 Sejarah Kriptografi.....	11
2.2.3 Algoritma Kriptografi	11
2.2.4 Tujuan Kriptografi	12
2.3 Algoritma Simetri dan Asimetri.....	14
2.3.1 Algoritma Asimetri	14
2.3.2 Algoritma Simetri	14

2.4	AES (<i>Advanced Encryption Standard</i>).....	14
2.4.1	Parameter AES	15
2.4.2	Proses Enkripsi AES	16
2.4.3	Proses Dekripsi AES	17
2.5	Beaufort Cipher	17
2.6	Android.....	20
2.6.1	Pengenalan Android	20
2.6.2	Sejarah Sistem Operasi Android	20
2.6.3	Fitur Android.....	23
2.6.4	Versi Android.....	24
2.6.5	Arsitektur Android	25
2.7	SDLC (<i>Software Development Life Cycle</i>)	28
2.7.1	Model <i>Waterfall</i>	28
2.8	Bahasa Pemrograman JAVA.....	30
2.9	Konsep Pemodelan	31
2.9.1	UML (<i>Unified Modeling Language</i>).....	31
2.9.2	Keunggulan UML	31
2.9.3	<i>Use Case Diagram</i>	32
2.9.4	<i>Activity Diagram</i>	33
2.9.5	<i>Class Diagram</i>	34
2.9.6	<i>Sequence Diagram</i>	37
BAB III ANALISIS DAN PERANCANGAN		38
3.1	Tinjauan Umum.....	38
3.1.1	Gambaran Umum Aplikasi	38
3.1.2	Tujuan Aplikasi.....	38
3.2	Analisis Sistem.....	38
3.2.1	Analisis SWOT	38
3.2.2	Analisis Kebutuhan Sistem	41
3.2.3	Analisis Kelayakan Sistem.....	43
3.2.4	Analisis Penggunaan Sistem	44
3.3	Perancangan Sistem.....	44
3.3.1	Perancangan UML	44
3.3.2	Perancangan Antarmuka Aplikasi.....	54

BAB IV IMPLEMENTASI DAN PEMBAHASAN	59
4.1 Implementasi Aplikasi.....	59
4.2 Pembahasan Kode Program Aplikasi	64
4.3 Instalasi Aplikasi	74
4.4 Hasil Pengujian.....	76
4.4.1 <i>Blackbox Testing</i>	76
BAB V PENUTUP.....	78
5.1 Kesimpulan.....	78
5.2 Saran.....	79
DAFTAR PUSTAKA	80



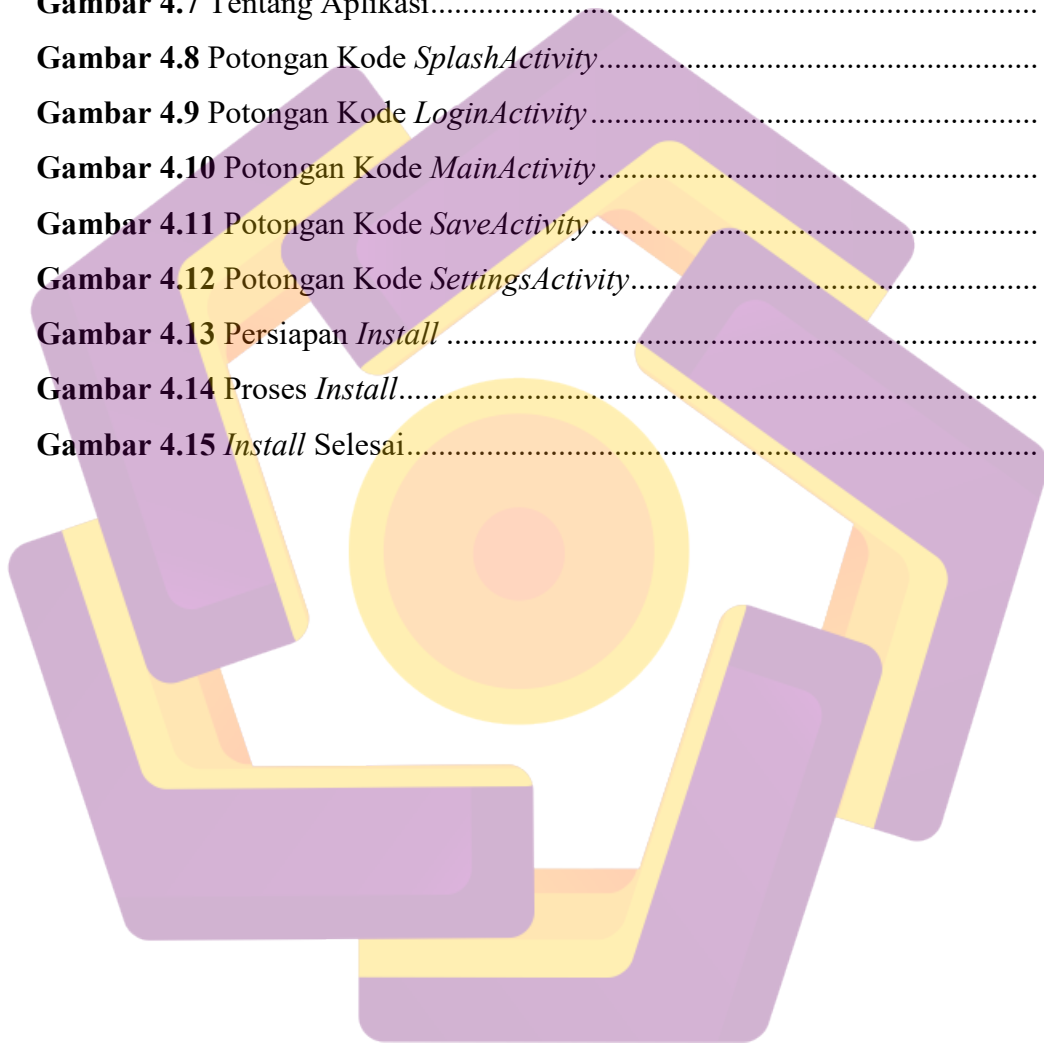
DAFTAR TABEL

Tabel 2.1 Contoh Permutasi Cipher	9
Tabel 2.2 Contoh Deskripsi Permutasi Cipher	10
Tabel 2.3 Contoh Penambahan Huruf Blok	10
Tabel 2.4 Parameter AES	15
Tabel 2.5 Contoh Penggunaan <i>Variant Beauford Cipher</i>	18
Tabel 2.6 Versi Android	24
Tabel 2.7 Simbol <i>Use Case Diagram</i>	32
Tabel 2.8 Simbol <i>Activity Diagram</i>	34
Tabel 2.9 Simbol <i>Class Diagram</i>	36
Tabel 2.10 Simbol <i>Sequence Diagram</i>	37
Tabel 3.1 Analisis SWOT	41
Tabel 4.1 Hasil Uji <i>Blackbox Testing</i> Aplikasi	77

DAFTAR GAMBAR

Gambar 2.1	Gambar diagram AES.....	16
Gambar 2.2	<i>Tabula Recta Variant Beaufort</i>	18
Gambar 2.3	Arsitektur Android.....	25
Gambar 2.4	Model <i>Waterfall</i>	29
Gambar 3.1	<i>Use Case Diagram</i>	45
Gambar 3.2	<i>Activity Splash Screen</i>	46
Gambar 3.3	<i>Activity Tampilan Tentang</i>	46
Gambar 3.4	<i>Activity Input Data</i>	47
Gambar 3.5	<i>Activity Add Simple Note</i>	47
Gambar 3.6	<i>Activity Add Enkripsi Note</i>	48
Gambar 3.7	<i>Activity Enkripsi Note</i>	48
Gambar 3.8	<i>Activity Dekripsi Note</i>	49
Gambar 3.9	<i>Activity Delete Note</i>	49
Gambar 3.10	<i>Activity Edit Note</i>	50
Gambar 3.11	<i>Class Diagram</i>	51
Gambar 3.12	<i>Sequence Diagram Tampilan Enkripsi Note</i>	52
Gambar 3.13	<i>Sequence Diagram Tampilan Dekripsi Note</i>	52
Gambar 3.14	<i>Sequence Diagram Tampilan Edit Note</i>	53
Gambar 3.15	<i>Sequence Diagram Tampilan Tentang</i>	53
Gambar 3.16	Rancangan Tampilan <i>Splash Screen</i>	54
Gambar 3.17	Rancangan Tampilan <i>Form Login</i>	55
Gambar 3.18	Rancangan Tampilan Menu Utama	55
Gambar 3.19	Rancangan Tampilan Tombol Tambahkan.....	56
Gambar 3.20	Rancangan Tampilan Isi Catatan	56
Gambar 3.21	Rancangan Tampilan Catatan Enkripsi	57
Gambar 3.22	Rancangan Tampilan Catatan Biasa	57
Gambar 3.23	Rancangan Tampilan Pengaturan	58
Gambar 3.24	Rancangan Tampilan <i>Edit Data</i>	58

Gambar 4.1 <i>Splash Screen</i> Aplikasi	59
Gambar 4.2 Menu Utama Aplikasi.....	60
Gambar 4.3 Isi Data Aplikasi	61
Gambar 4.4 Tambahkan Catatan Aplikasi.....	61
Gambar 4.5 Isi Catatan Aplikasi	62
Gambar 4.6 Pengaturan Aplikasi.....	63
Gambar 4.7 Tentang Aplikasi.....	63
Gambar 4.8 Potongan Kode <i>SplashActivity</i>	64
Gambar 4.9 Potongan Kode <i>LoginActivity</i>	66
Gambar 4.10 Potongan Kode <i>MainActivity</i>	68
Gambar 4.11 Potongan Kode <i>SaveActivity</i>	71
Gambar 4.12 Potongan Kode <i>SettingsActivity</i>	73
Gambar 4.13 Persiapan <i>Install</i>	74
Gambar 4.14 Proses <i>Install</i>	75
Gambar 4.15 <i>Install</i> Selesai.....	76



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 sebagaimana block cipher pada umumnya. Sedangkan Metode Variant Beaufort sendiri merupakan salah satu algoritma kriptografi klasik dengan teknik substitusi, panjang alphabet/char yang diijinkan dalam aplikasi lebih panjang dari yang bisanya 26 karakter.

Secara garis besar aplikasi ini mampu mengacak informasi dalam catatan cukup baik, sehingga membuat kerahasiaan 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: *Application, cryptography, security, Android, Encryption, Decryption, Note.*