Terbit *online* pada laman: https://journal.fkpt.org/index.php/BIT
BULLETIN OF INFORMATION TECHNOLOGY (BIT)
ISSN (Media Online) 2722-0524

PERANCANGAN APLIKASI PENGAMANAN PESAN CHATTING MENGGUNAKAN SOLITAIRE CHIPER BERBASIS ANDROID

Tiara Andini
Program Studi Teknik Informatika, Universitas Budi Darma, Sumatera Utara, Indonesia
Email: tiara@gmail.com

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi : 10 Oktober 2021
Revisi Akhir : 1 November 2021
Diterima : 20 November 2021
Diterbitkan *Online* : 28 November 2021

KATA KUNCI

Kata Kunci: *Security Chat Messages, Solitaire Cipher, Android, Classical Cryptography Progress*

KORESPONDENSI

E-mail: andinitiara8@gmail.com

A B S T R A C T

Progress on the delivery of android-based information has many advantages, especially because it can reduce many things that are not necessary or can be said to have an impact on efficiency in many ways. However, along with negative aspects also occur, such as crime, which includes theft, fraud and extortion.
By using the Solitaire Cipher Algorithm which is a classic cryptographic algorithm, which uses playing cards as intermediaries. This type of algorithm uses the order of playing cards as keys that will be securely given to the recipient of the ciphertext. Whereas to do the encryption and decryption process of this solitaire algorithm, the order of cards is changed in certain order and rules.
The design of this application also facilitates the process of securing text so that it is not easily read by others so that the authenticity of the data is maintained. It is an effort to safeguard information from those who are not entitled to access or in other words a confidential information that may not be accessed by others and may only be accessed by those who are granted access..

1. PENDAHULUAN

Saat ini, teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Contoh dari perkembangan ini adalah jaringan internet, yang pada saat ini telah memungkinkan banyak orang untuk saling bertukar data secara bebas melalui jaringan tersebut. Karena kemudahan yang dimilikinya, internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Namun, kemudahan ini juga dimanfaatkan oleh sebagian pihak yang mencoba untuk melakukan kejahatan. Dengan berbagai teknik, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu, sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan sisi keamanan.

Chatting sudah menjadi hal yang umum digunakan oleh masyarakat luas. Kemampuan pengiriman pesan secara cepat membuat user dapat berkomunikasi satu sama lain secara real-time. Selama ini aplikasi tersebut belum bisa menjamin keamanan privasi diantara pengirim dan penerima ketika melakukan obrolan. Untuk menjamin keamanan privasi tersebut dengan melakukan enkripsi pada aplikasi chatting dapat membantu user dalam merahasiakan pesan yang akan dikirimkannya agar terjaga dari orang-orang yang ingin mengetahui isi percakapan si user

2. METODOLOGI PENELITIAN

2.1 Aplikasi

Aplikasi dapat diartikan sebagai suatu program berbentuk perangkat lunak yang berjalan pada suatu sistem tertentu yang berguna untuk membantu berbagai kegiatan yang dilakukan oleh manusia. Selain pengertian di atas, ada banyak pengertian dari kata ‘Aplikasi’ yang dikemukakan oleh para ahli[2].

2.1.1 Pengertian Aplikasi Menurut Para Ahli

Beberapa pengertian aplikasi menurut para ahli adalah sebagai berikut :
1. Ali Zaki dan Smitdev Community

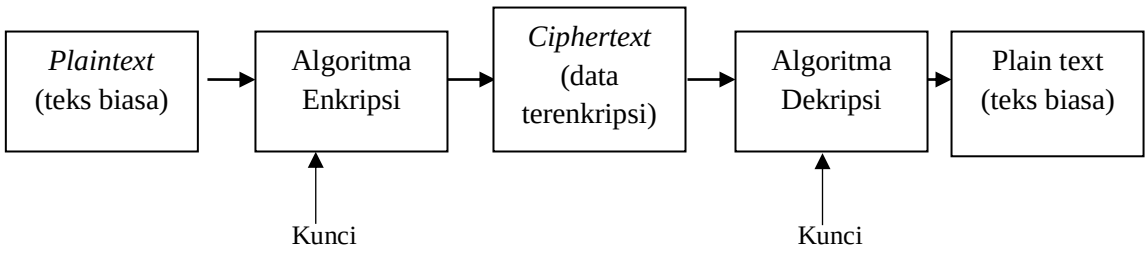
Menurut Ali Zaki dan Smitdev Community, Aplikasi merupakan komponen yang bermanfaat sebagai media untuk menjalankan pengolahan data ataupun berbagai kegiatan lainnya seperti pembuatan ataupun pengolahan dokumen dan file.

2. Sri Widianti
   Menurut Sri Widianti, Aplikasi merupakan sebuah software (perangkat lunak) yang bertugas sebagai front end pada sebuah sistem yang dipakai untuk mengelolah berbagai macam data sehingga menjadi sebuah informasi yang bermanfaat untuk penggunanya dan juga sistem yang berkaitan.
3. Harip Santoso
   Menurut Harip Santoso, Aplikasi merupakan sebuah kelompok file (class, form, report) yang ditujukan sebagai pengeksekusi aktivitas tertentu yang saling berkaitan seperti contohnya aplikasi payroll dan aplikasi fixed asset.
4. Yuhefizar
   Menurut Yuhefizar, Aplikasi adalah program yang sengaja dibuat dan dikembangkan sebagai pemenuh kebutuhan penggunanya dalam menjalankan suatu pekerjaan tertentu.
5. Hengky W. Pramana
   Menurut Hengky W. Pramana, pengertian aplikasi adalah satu unit perangkat lunak yang sengaja dibuat untuk memenuhi kebutuhan akan berbagai aktivitas ataupun pekerjaan, seperti aktivitas perniagaan, periklanan, pelayanan masyarakat, game, dan berbagai aktivitas lainnya yang dilakukan oleh manusia.

2.1.2 Sistem Kriptografi

Sistem Kriptografi memiliki 5 bagian antara lain [6] :

1. Plainteks
   Pesan atau data dalam bentuk aslinya yang dapat terbaca. Plainteks adalah masukan bagi algoritma enkripsi. Untuk selanjutnya digunakan istilah teks asli sebagai padanan kata plainteks.
2. Secret Key
   Secret Key juga yang merupakan masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi. Untuk selanjutnya digunakan istilah kunci rahasia sebagai padanan kata secret key
3. Cipherteks
   Cipherteks adalah keluaran algoritma enkripsi. Cipherteks dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan cipherteks yang terlihat acak.
4. Enkripsi
   Algoritma enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.
5. Dekripsi
   Algoritma dekripsi memiliki 2 masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai algoritma dekripsi sama dengan kunci rahasia yang dipakai algoritma enkripsi.



Gambar 1 Proses Enkripsi dan Dekripsi data: Dony Ariyus, 2005 [3]

Prosesnya adalah sebagai berikut:

Proses Enkripsi

$C = E_k(M)$

Proses Dekripsi

$M = D_k(C)$ keterangan:

C = Chipertext
Enkripsi dengan menggunakan kunci K
M = Pesan (Message)
Dekripsi dengan menggunakan kunci K

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Volume 2, No. 3, Nopember 2021, pp 95- 106
ISSN 2722-0524 (media online)

3. ANALISA DAN PEMBAHASAN

3.1 Analisa

Sub bab ini berisikan tentang analisa sistem yang akan dibangun. Sub bab ini membahas teknik pemecahan masalah yang menguraikan sebuah sistem menjadi bagian-bagian komponen dengan tujuan mempelajari seberapa baik bagian-bagian komponen tersebut bekerja dan berinteraksi. Pada proses pengamanan pesan chating memastikan bahwa user (pengguna) dan orang yang berkomunikasi dengan user (pengguna) saja yang dapat membaca apa yang dikirimkan. Pesan-pesan yang akan diamankan (enkripsi) dengan kunci dan hanya penerima dan user (pengguna) saja yang memiliki kunci special yang diperlukan untuk membuka dan membaca pesan yang dikirimkan. Untuk membuka pesan yang telah dikirim si penerima pesan harus melakukan proses dekripsi dan penggunaan kunci yang telah ditentukan oleh user (pengguna) sehingga pesan tersebut dapat dibaca oleh si penerima pesan. Adapun sekenario dari proses pengamanan pesan chatting dapat dilihar pada tabel dibawah ini.

3.2 Penerapan Algoritma Solitaire Cipher

Algoritma untuk menghasilkan kunci untuk proses enkripsi dan dekripsi terdiri dari enam langkah. Enam tahap ini akan menghasilkan sebuah angka yang merupakan salah satu bagian aliran kunci. Enam tahap ini kemudian dilakukan kembali untuk mendapatkan kunci kedua dan terus diulang sampai panjang kunci yang diinginkan atau disepakati. Adapun langkah-langkah algoritma soltaire cipher antara lain :

1. Urutkan tumpukan kartu berdasarkan kunci tertentu.
   Bagian ini adalah bagian paling penting, karena pihak yang mengetahui sebuah nilai awal dari deck dapat dengan mudah mendapatkannilai yang sama darinya. Bagaimana sebuah tumpukan diinisialisasi terserah oleh penerima. Mengocok kartu dengan benar-benar acak akan lebih baik, walaupun masih ada beberapa metode lain.
   Urutan awal seperti ini:
   1 47 10 13 16 19 22 25 **28** 3 6 9 12 1518 21 24
   27 2 5 8 11 14 17 20 23 26
2. Temukan joker A (yang bernilai 27).
   Pindahkan satu kartu ke bawah (dengan kata lain, menukar dengan satu kartu dibawahnya). Jika joker tersebut berada di tumpukan paling bawah, pindahkan ke tepat di bawah tumpukan teratas.
   Urutan kartu tersebut akan menjadi seperti ini:
   1 47 10 13 16 19 22 25 **28** 3 6 9 12 1518 21 24
   2 **27** 5 8 11 14 17 20 23 26
3. Temukan joker B (yang bernilai 28).
   Pindahkan dua kartu ke bawah. Jika joker tersebut berada pada tumpukan terbawah, pindahkan ke bawah kartu kedua dari atas (jadi kartu ketiga). Jika joker tersebut berada pada posisi kedua dari bawah, pindahkan ke bawah kartu teratas (menjadi kartu kedua).
   Setelah langkah ketiga ini, urutan kartu akan menjadi:
   1 47 10 13 16 19 22 25 3 6 **28** 9 12 15 18 21 24
   2 **27** 5 8 11 14 17 20 23 26
4. Lakukan *triple cut*.
   Yaitu ganti kartu-kartu yang berada di bagian kiri kartu joker pertama dengan kartu-kartu di bagian kanan dari kartu joker kedua. Perlu diperhatikan bahwa joker pertama adalah joker yang berada di posisi lebih tinggi dari kartu joker lain, tidak penting apakah itu joker A atau B.
   Susunan kartu sebelum triple cut dilakukan:
   1 4 7 10 13 16 19 22 25 3 6 **28** 9 12 15 18 21 24
   2 **27** 5 8 11 14 17 20 23 26
   Susunankartu setelah triple cut dilakukan:
   5 8 11 14 17 2023 26 **28** 9 12 15 18 21 24 2 **27**
   1 4 7 10 13 16 19 22 25 3 6
5. Lakukan count cut.
   Lihat nilai kartu terbawah, anggap nilai tersebut adalah n. Ambil n kartu pertama dan pindahkan ke posisi kedua dari bawah.
   Susunan kartu sebelum count cut dilakukan:
   5 8 11 14 17 20 23 26 **28** 9 12 15 18 21 24 2 **27**
   1 4 7 10 13 16 19 22 25 3 6
   Susunan kartu setelah count cut dilakukan:
   23 26 **28** 9 12 15 18 21 24 2 **27** 1 4 7 10 13 16
   19 22 25 3 5 8 11 14 17 206
6. Temukan kartu keluaran.
   Untuk melakukan ini, lihat kartu paling atas. Hitung sebanyak nilai kartu tersebut mulai dari kartu setelah kartu paling atas. Nilai kartu pada urutan tersebut adalah nilai berikutnya dalam kunci aliran.

Pada contoh yang digunakan, nilai kartu paling atas adalah 23. Nilai kartu ke 23 dari kartu setelah kartu paling atas adalah 11. Nilai 11 inilah yang dimasukkan ke dalam kunci aliran. Setelah itu ulangi lagi dari langkah kedua sampai ke enam. Lakukan terus sampai sebanyak panjang kunci yang digunakan. Sebelum mengulang langkah-langkah tersebut, urutan kartu dari proses sebelumnya tidak perlu diubah.

3.2.1 Proses Enkripsi Dengan Algoritma Solitaire Cipher

Untuk contoh Implementasi ini, pesan dan kunci yang digunakan harus ditentukan terlebih dahulu. Adapun pesan yang akan diamankan adalah "TIARAANDINI" dengan kunci "BUDIDARMA". Sesuai dengan langkah-langkah enkripsi yang diberikan pada bagian sebelumnya, maka hal yang boertama harus dilakukan adalah pengurutan sesuai dengan kunci yang diberikan. Untuk pengurutan kartu awal ini, langkah yang harus dilakukan adalah

1. Ambil sebuah karakter dari kata kunci untuk contoh implementasi pertama (huruf B) maka
   Cut size = 2
2. Lakukan enam langkah untuk mendapatkan huruf aliran kunci yang telah dijelaskan dari contoh sebelumnya, maka pengurutan kartu dimulai. Urutan kartu awal dari huruf terkecil ke nilai terbesar. Perlu di ingat kembali bahwa nilai 1-13 diberikan untuk kartu As-kartu king keriting (*clubs*) secara berurutan. Nilai 14-26 untuk kartu berjenis wajik (*diamonds*), nilai 27-39 untuk kartu hati (*heart*) dan nilai 40-52 untuk kartu pohon (*spades*).
   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A B
   Langkah pertama adalah pemindahan joker A maka susunan kartu akan menjadi
   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 B A
   Langkah kedua adalah Pemindahan joker B. Susunan kartu akan berubah menjadi
   1 B 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
   18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
   36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A
   Langkah selanjutnya adalah triple cut yang akan menjadi susunan kartu seperti berikut
   B 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A 1
   Langkah keempat adalah count cut yang akan memindahkan 1 kartu Pertama. Posisi kartu selanjutnya.
   2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
   20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37
   38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A B 1
   Setelah count cut ini, proses pembangkitan aliran kunci untuk penyusunan kartu sesuai kunci telah selesai.
3. Lakukan triple cut. Sejumlah cut_size kartu awal diganti dengan kartu terakhir. Dari hasil di nomor dua, maka posisi urutan kartu berikutnya didapatkan dengan mengganti 2 kartu pertama dengan kartu terakhir.
   1 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
   21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
   39 40 41 42 43 44 45 46 47 48 49 50 51 52 A B 2 3
4. Lakukan pemindahan kartu berikutnya, dengan meletakan kartu pertama sebagai kartu paling bawah. Posisi kartu lain tidak diubah.
   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48 49 50 51 52 A B 2 3 1
   Dengan demikian proses untuk mendapatkan susunan kartu menurut karakter pertama dari kunci telah dilakukan. Langkah-langkah diatas diulangi untuk semua karakter lain dari kata kunci. Selanjutnya akan dicontohkan pengaturan kunci untuk karakter kedua, yaitu U. susunan kartu awal untuk karakter U ini diambil dari susunan yang dihasilkan untuk pengaturan kartu berdasarkan karakter B. maka sususnan awal pengaturan kunci untuk karakter U ini adalah
   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48 49 50 51 52 A B 2 3 1

Langkah-langkahnya adalah :

1. Penentuan cut_size
   Cut_size = 21
2. Enam langkah mendapatkan aliran kunci, hasil dari pergeseran joker A
   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48 49 50 51 52 B A 2 3 1
   Hasil dari penggeseran joker B :
   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39

40 41 42 43 44 45 46 47 48 49 50 51 52 A 2 B 3 1
Hasil dari triple cut :
3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 30 41 42 43 44 45 46 47 48 49 50 51 52
Hasil dari count cat :
51 3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
34 35 36 37 38 39 30 41 42 43 44 45 46 47 48 49 50 52

3. Triple cut
Hasil dari triple cut :
52 3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
34 35 36 37 38 39 30 41 42 43 44 45 46 47 48 49 50 51

4. Pemindahan kartu pertama
Hasilnya ;
3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Penyusunan kartu untuk karakter (D) :
Susunan kartu awal
3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52

Langkah yang dilakukan :

1. Penentuan cut_size
cut_size = 3
2. Enam langkah mendapatkan aliran kunci.
Hasil dari penggeseran joker A :
3 1 2 A B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Hasil dari penggeseran joker B :
3 1 2 A 4 5 B 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Hasil dari triple cut :
6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41
42 43 44 45 46 47 48 49 50 51 52 A 4 5 B 3 1 2
Hasil count cat
8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51 52 A 4 5 B 3 1 6 7 2
3. Triple cut
Hasil dari triple cut :
2 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45
46 7 48 49 50 51 A 4 5 B 3 1 6 7 52 8 9 10
4. Pemindahan kartu pertama, hasil nya :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 A 4 5 B 3 1 6 7 52 8 9 1 0 2
Penyusunan berikutnya adalah penyusunan karakter keempat. Yaitu I. susunan kartu awal untuk karakter I :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 A 4 5 B 3 1 6 7 52 8 9 1 0 2

Langkah untuk menyusun kartu :

1. Penentuan cut _size = 9
2. Enam langkah mendapatkan aliran kunci.
Hasil dari penggeseran joker A :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 4 A 5 B 3 1 6 7 52 8 9 1 0 2

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Volume 2, No. 3, Nopember 2021, pp 95- 106
ISSN 2722-0524 (media online)

Hasil dari penggeseran joker B :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 4 A 5 3 1 B 6 7 52 8 9 1 0 2
Hasil dari triple cut :
6 7 52 8 9 1 0 2 A 5 3 1 B 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4
Hasil dari count cut :
A 5 3 1 B 11 12 13 14 15 16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 6 7 52 8 9 1 0 2

3. Triple cut :
2 4 6 7 52 8 9 10 A 5 3 1 B 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
34 35 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4

4. Pemindahan kartu pertama
Hasilnya :
4 6 7 52 8 9 10 A 5 3 1 B 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2
Penyusunan kartu untuk karakter kelima (D)
Dimulai dengan sususnan kartu :
4 6 7 52 8 9 10 A 5 3 1 B 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2

Langkah untuk penyusunan kartu :

1. Penentuan cut_size = 4
2. Enam langkah mendapatkan aliran kunci.
Hasil dari penggeseran joker A :
4 6 7 52 8 9 10 5 3 A 1 B 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2
Hasil dari penggeseran joker B :
4 6 7 52 8 9 10 5 3 A 1 11 12 B 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 2
Hasil dari triple cut :
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 35 36 37 38 39 40 41 42 43 44 45 46 47
48 49 50 51 4 2 A 1 11 12 B 4 6 7 52 8 9 10 5 3
Hasil dari count cut ;
B 4 6 7 52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 23 24 25 26 27 28 29 30 31 32 33 34 35 35 36 37 38
38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 11 12
3. Triple cut
Hasil dari triple cut sususnan kartu :
12 52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 23
24 25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 B 11
4. Pemindahan kartu pertama, hasilnya :
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 B 11 12
Selanjutnya adalah penyusunan kartu berdasarkan karakter A susunan awal kartunya:
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 B 11 12
1. Penentuan cut_size
Cut_size = 1
2. Penggerakan joker A. hasilnya :
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 1 A B 11 12

Penggeseran joker B. hasilnya :
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 1 A 11 12 B
Triple cut :
52 A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21
22 23 2 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48 49 50 51 4 2 1
Count cut ;
B 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41
42 43 44 45 46 47 48 49 50 51 52 A 11 12 1

3. Triple cut :
1 A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21
22 23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
4. Hasil dari pemindahan kartu pertama
A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1

Penyusunan berikutnya dimulai dengan sususnan :
A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1

1. Penentuan cut size = 18
2. Hasil dari penggeseran joker A ;
11 A 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1
Penggeseran joker B ;
11 A 12 9 10 B 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1
Triple cut :
B 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26
27 A 12 9 10 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48 49 50 51 52 1 11
Count cut :
5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
A 12 9 10 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
3. Triple cut
11 12 A 9 10 28 29 30 31 32 33 34 35 36 37 38 39 40
5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B
4. Pemindahan kartu pertama
12 9 A 10 28 29 30 31 32 33 34 35 36 37 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
Selanjutnya penyusunan kartu berdasarkan karakter R. susunan awal kartunya :
12 9 A 10 28 29 30 31 32 33 34 35 36 37 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
Langkah-langkah penyusunan kartu ;

1. Penentuan nilai cut_size
Cut_size = 9
2. Empat langkah pembangkitan aliran kunci.
Pertama, penggesran joker A :
12 9 10 A 28 29 30 31 32 33 34 35 36 37 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
Kedua, penggeseran joker B :
12 B 9 10 A 28 29 30 31 32 33 34 35 36 37 38 39
40 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25

26 27 41 42 43 44 45 46 47 48 49 50 51 52 1 11
Ketiga, triple cut :
9 10 A 28 29 30 31 32 33 34 35 36 37 38 39 40 5 3
13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27 41
42 43 44 45 46 47 48 49 50 51 52 1 11 12 B
Keempat, count cut :
38 39 40 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4
2 A 28 29 30 31 32 33 34 35 36 37 25 26 27 41 42
43 44 45 46 47 48 49 50 51 9 10 52 1 11 12 B

3. Triple cut
B 29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 A 28
4. Pemindahan kartu pertama
29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 A 28 B

Selanjutnya adalah proses penyusunan kartu terakhir dengan dengan karakter M. susunan kartu awlnya sama dengan susunan terakhir yang dihasilkan oleh penyusunan kartu dengan karakter A yaitu ;

29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 A 28 B

Langkah-langkah penyusunan kartu :

1. Penentuan nilai cut size
Cut_size = 1
2. Empat langkah pembangkitan aliran kunci.
Pertama, penggeseran joker A :
0 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A B
Kedua, penggeseran joker B:
30 B 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29
Ketiga , triple cut :
B 31 32 33 34 35 36 37 25 26 27 41 42 43 44 45 46
47 48 49 50 51 9 10 52 1 11 12 38 39 40 5 3 13
14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29 30
Keempat, count cut :
37 25 26 27 41 42 43 44 45 46 47 48 49 50 51 9
10 52 B 31 32 33 34 35 36 1 11 12 38 39 40 5 3 13
14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29 30
3. Triple cut
30 49 50 51 9 10 52 B 31 32 33 34 35 36 37 25 26
27 41 42 43 44 45 46 47 48 49 50 51 1 11 12 38 39
40 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29
Pemindahan kartu pertama
49 50 51 9 10 52 B 31 32 33 34 35 36 37 25 26 27
41 42 43 44 45 46 47 48 49 50 51 1 11 12 38 39 40
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 30

Dengan demikian proses pengurutana

Kartu awal telah selesai.susunan kartu yang terakhir dihasilkan sudah bisa digunakan untuk melakukan enkripsi pesan

Proses selanjutnya adalah penjumlahan *keystream* dengan *plainteks* antara lain :

1. Penentuan nilai dari kartu keluaran untuk kunci **B**
Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (4+1)=5.
Maka kartu keluaran adalah pada posisi 5. Nilai kartu pada posisi 5 tersebut adalah 9. Kartu dengan nilai 9 adalah Sembilan As. Sehingga hasilnya adalah
Nilai keluaran = 9
Kartu keluaran = Sembilan As.
2. Penentuan nilai dari kartu keluaran untuk kunci **U**
Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (3+1)=4.

Maka kartu keluaran adalah pada posisi 4. Nilai kartu pada posisi 4 tersebut adalah joker B atau sama dengan nilai 54. Kartu dengan nilai 54 adalah joker B. Sehingga hasilnya adalah
Nilai keluaran = 54
Kartu keluaran = joker B

3. Penentuan nilai dari kartu keluaran untuk kunci **D**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (11+1)=12.
   Maka kartu keluaran adalah pada posisi 12. Nilai kartu pada posisi 12 tersebut adalah 23. Kartu dengan nilai 23 adalah Sepuluh Wajik. Sehingga hasilnya adalah
   Nilai keluaran = 10
   Kartu keluaran = Sepuluh wajik
4. Penentuan nilai dari kartu keluaran untuk kunci **I**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (4+1)=5.
   Maka kartu keluaran adalah pada posisi 5. Nilai kartu pada posisi 5 tersebut adalah 9. Kartu dengan nilai 9 adalah Sembilan As. Sehingga hasilnya adalah
   Nilai keluaran = 9
   Kartu keluaran = Sembilan As
5. Penentuan nilai dari kartu keluaran untuk kunci **D**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (52+1)=53.
   Maka kartu keluaran adalah pada posisi 53. Nilai kartu pada posisi 53 tersebut adalah 12. Kartu dengan nilai 12 adalah pro As. Sehingga hasilnya adalah
   Nilai keluaran = 12
   Kartu keluaran = pro As
6. Penentuan nilai dari kartu keluaran untuk kunci **A**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (joker A atau 53 +1)=54.
   Maka kartu keluaran adalah pada posisi 54. Nilai kartu pada posisi 54 tersebut adalah joker B atau bernilai 54. Kartu dengan nilai 54 adalah pro As.karena melebihi 26, maka nilainya dikurangi 26 menjadi 28.Sehingga hasilnya adalah
   Nilai keluaran = 28
   Kartu keluaran = dua hati
7. Penentuan nilai dari kartu keluaran untuk kunci **R**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (12 +1)=13.
   Maka kartu keluaran adalah pada posisi 13. Nilai kartu pada posisi 13 tersebut adalah 37. Kartu dengan nilai 37 adalah jack hati. .karena melebihi 26, maka nilainya dikurangi 26 menjadi 11. Sehingga hasilnya adalah
   Nilai keluaran = 11
   Kartu keluaran = jack As
8. Penentuan nilai dari kartu keluaran untuk kunci **M**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (29 +1)=30.
   Maka kartu keluaran adalah pada posisi 30. Nilai kartu pada posisi 30 tersebut adalah 39. Kartu dengan nilai 39 adalah king hati. .karena melebihi 26, maka nilainya dikurangi 26 menjadi 13. Sehingga hasilnya adalah
   Nilai keluaran = 13
   Kartu keluaran = king As
9. Penentuan nilai dari kartu keluaran untuk kunci **A**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (49 +1)=50.
   Maka kartu keluaran adalah pada posisi 50. Nilai kartu pada posisi 50 tersebut adalah 28. Kartu dengan nilai 28 adalah dua hati. karena melebihi 26, maka nilainya dikurangi 26 menjadi 2. Sehingga hasilnya adalah
   Nilai keluaran = 2
   Kartu keluaran = dua As
   Setelah Sembilan kali pembangkitan keystream yang dilakukan di atas, maka keystream yang didapatkan adalah :

   B U D I D A R M A
   9 54 10 9 12 28 11 13 2
   Dengan *plainteks*
   T I A R A A N D I N I
   20 9 1 18 1 1 14 4 9 14 9
   Maka penjumlahannya adalah
   9 54 10 9 12 28 11 13 2
   20 9 1 18 1 1 14 4 9 14 9 + (mod 26)

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Volume 2, No. 3, Nopember 2021, pp 95- 106
ISSN 2722-0524 (media online)

3 11 11 1 13 3 25 17 11 14 9
C K K A M C Y Q K N I

Maka *ciphertеksnya* adalah

C K K A M C Y Q K N I

i. Proses Deskripsi Dengan Algoritma Soltaire Cipher

Untuk proses deskripsi, dua langkah yang harus dilakukan sama dengan dua langkah pertama enkripsi. Jika pada enkripsi *keystream* dijumlahkan dengan *plainteks*, maka pada deskripsi chiperteks dikurangi dengan *keystream*. Untuk contoh di atas, setelah mendapatkan *keystream*.

B U D I D A R M A
9 54 10 9 12 28 11 13 2

Maka chiperteknya adalah

C K K A M C Y Q K N I
3 11 11 1 13 3 25 17 11 14 9

Dikurangi dengan keystream tersebut. Hasilnya

C K K A M C Y Q K N I
9 54 10 9 12 28 11 13 2
3 11 11 1 13 3 25 17 11 14 9 - (mod 26)

Adalah :

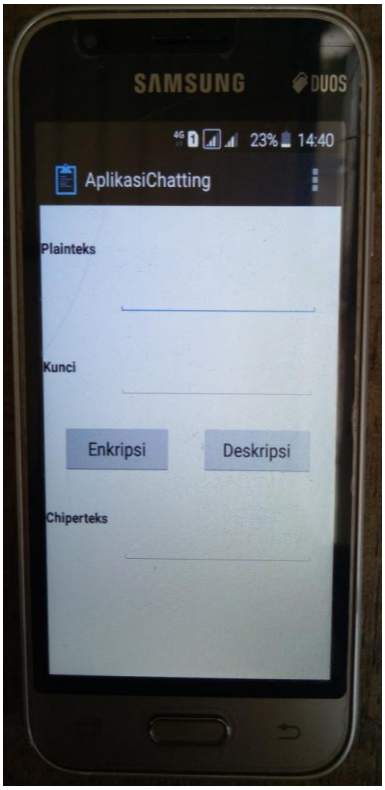
20 9 1 18 1 1 14 4 9 14 9
T I A R A A N D I N I

Dari hasil deskripsi, penerima bisa menebak apakah karakter terakhir adalah karakter *padding* atau tidak.

4. IMPLEMENTASI

4.1. Hasil

1. Tampilan Aplikasi Chatting



Gambar 2 Tampilan Aplikasi Chatting

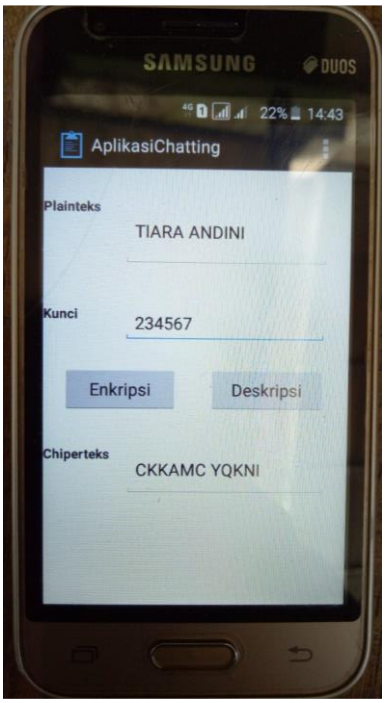
Keterangan :

1. Textbox pada plainteks berfungsi untuk memasukan pesan yang akan digunakan untuk enkripsi.
2. Textbox kunci berfungsi untuk kunci pesan pada plainteks
3. Button enkripsi digunakan untuk proses enkripsi pesan pada plainteks.
4. Button deskripsi digunakan untuk mengembalikan hasil enkripsi
5. Textbox chiperteks berfungsi untuk menampung hasil dari enkripsi dan deskripsi.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Volume 2, No. 3, Nopember 2021, pp 95- 106
ISSN 2722-0524 (media online)

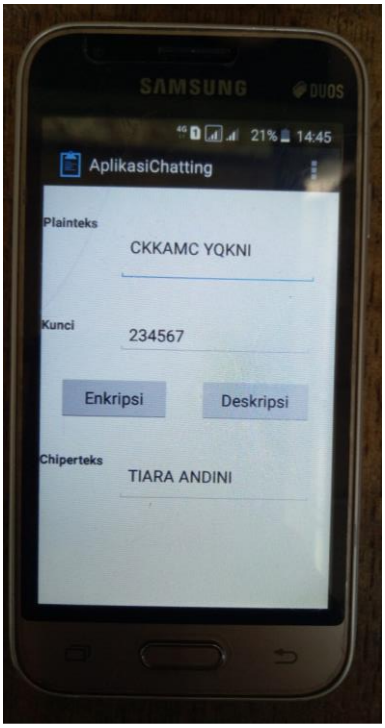
4.2 Tampilan Output

1. Tampilan Proses Enkripsi



Gambar 3 Tampilan Proses Enkripsi

2. Tampilan Proses Deskripsi



Gambar 4 Tampilan Proses Deskripsi

5. KESIMPULAN

Setelah menyelesaikan skripsi yang berjudul perancangan aplikasi pengamanan pesan chatting menggunakan solitaire cipher berbasis android, dapat ditarik beberapa kesimpulan sebagai berikut :

1. Dalam pengujian Aplikasi ini berhasil mengamankan pesan pengguna yang dikirim melalui pesan chating.
2. Aplikasi dapat memproses Pesan teks minimal 12 karakter dengan kunci 128 bit
3. Penerapan metode pengamanan data pada plainteks dilakukan untuk menyembunyikan rahasia pada saat pendistribusian pesan rahasia, yaitu dengan cara simetris yang dilakukan melalui proses dekripsi. Dimana data

pada plainteks awalnya diproses melalui kunci enkripsi, lalu data dialirkan menjadi kunci dekripsi sehingga akhirnya menjadi teks/data asli yang aman.

REFERENCES

[1] Baez, Jeffrey, 2009, "Math In The Solitaire Cipher",Journal IEEE Trans. On Computer, Vol. 58, No. 6, pp.721-727.
2] http://www.e-jurnal.com/2014/02/pengertian-pesan.html, diakses tanggal 24 Mei 2018.
[3] https://www.maxmanroe.com/vid/teknologi/pengertian-chatting.html,diakses tanggal 24 April 2018.
[4] Ariyus, Dony, 2005, "Kriptografi Keamanan Data Dan Komunikasi". Edisi Pertama. Yogyakarta. Graha Ilmu.
[5] Sadikin, Rifki, 2012, "Kriptografi Untuk Keamanan Jaringan", Penerbit Andi, Yogyakarta.
[6] Ariyus, Dony, 2008, "Computer Security, Andi, Yogyakarta.
[7] https://www.maxmanroe.com/vid/teknologi/pengertian chatting.html,diakses tanggal 24 April 2018.
[8] A.S. Rosa dan Shalahuddin. M, 2013, "Rekayasa Perangkat Lunak Terstruktur", Andi, Yogyakarta.