Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 4 (2020) 627 - 634 ISSN Media Elektronik: 2580-0760

Implementasi Teknik Kriptografi *CAESAR CIPHER* Untuk Keamanan Data Informasi Berbasis Android

Fina Triana[1], Jon Endri[2] , Irma Salamah[3]
[1,2,3]Teknik Elektro, Politeknik Negeri Sriwijaya
[1]finatriana327@gmail.com, [2]jon_endri@polsri.ac.id, [3]irma.salamah@yahoo.com

Abstract

Information data security is an important aspect of exchanging data and information. Data and information security can be done in various ways, including by using the cesarean cipher method in cryptographic techniques. The cesarean cipher method of cryptographic technique is a substitution coding system which is done by replacing each alphabet character with other characters along the 26 alphabet characters so that the coding only occurs in the alphabet itself without any other punctuation. This study proposes a modification to the cesarean cipher technique by adding to the number of characters used, namely 256 characters in the ASCII code. The caesar cipher application or CaesarApp uses the methodology of library study, consultation, application design and application testing. The implementation of the CaesarApp application was created using the open-source Android Studio 3.5 application. The results of tests conducted on the CaesarApp application note that the modification of the caesar cipher with 256 ASCII characters results in a secure information data security application, this application has a deficiency in reading limitations on ASCII characters, so characters cannot be read properly on android users.

Keywords: Cryptography, Caesar Cipher, Information Data Security, Android

Abstrak

Keamanan data informasi merupakan aspek yang penting dalam pertukaran data dan informasi. Keamanan data dan informasi dapat dilakukan dengan berbagai macam cara, diantaranya adalah dengan menggunakan metode *caesar cipher* pada teknik kriptografi. Metode *caesar cipher* teknik kriptografi adalah sistem persandian substitusi yang dilakukan dengan mengganti setiap karakter alfabet dengan karakter lain sepanjang 26 karakter alfabet sehingga pengkodean hanya terjadi pada alfabet itu sendiri tanpa adanya tanda baca lain. Penelitian ini mengusulkan modifikasi pada teknik *caesar cipher* dengan melakukan penambahan pada jumlah karakter yang digunakan yaitu 256 karakter pada kode ASCII. Aplikasi *caesar cipher* atau *CaesarApp* menggunakan metodologi yaitu studi pustaka, konsultasi, rancangan aplikasi dan pengujian aplikasi. Implemntasi pada aplikasi *CaesarApp* ini dibuat dengan menggunakan aplikasi *open source* android studio 3.5. Hasil pengujian yang dilakukan pada aplikasi *CaesarApp* diketahui bahwa modifikasi *caesar cipher* dengan 256 karakter ASCII menghasilkan aplikasi keamanan data informasi yang aman, aplikasi ini memiliki kekurangan pada keterbatasan pembacaan pada karakter ASCII, sehingga karakter tidak dapat terbaca dengan baik pada android pengguna.

Kata kunci: Kriptografi, *Caesar Cipher*, Keamanan Data Informasi, Android

1. Pendahuluan

Pada era globalisasi sekarang ini, keamanan merupakan salah satu aspek yang sangat penting pada pertukaran data dan informasi. Pertukaran data dan informasi biasa dilakukan secara pribadi maupun suatu kelompok atau suatu organisasi. Suatu data dan informasi tersebut akan memiliki nilai lebih tinggi apabila menyangkut aspek-aspek yang bersifat rahasia. Oleh karena itu, keamanan data dan informasi sangatlah diperlukan agar data dan informasi tersebut tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.

Ada berbagai cara yang dapat digunakan untuk melakukan keamanan data dan informasi, salah satunya adalah dengan menggunakan teknik kriptografi. Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*) [1].

Metode *caesar cipher* merupakan salah satu metode sederhana yang dapat digunakan dalam kriptografi. *Caesar cipher* merupakan sistem persandian berbasis substitusi yang pertama kali digunakan pada tahun 50

Diterima Redaksi : 23-05-2020 | Selesai Revisi : 09-08-2020 | Diterbitkan Online : 20-08-2020

SM oleh Julius Caesar yang merupakan kasiar Roma, ia menggunakan sandi tersebut untuk mengirimkan pesan ke panglima perangnya yaitu Marcuss Cicero [2,3].

Pada metode *caesar cipher*, proses mengubah data informasi menjadi kode disebut enkripsi dan proses mengubah kode menjadi data informasi disebut dekripsi. Proses *caesar cipher* adalah dengan mengganti setiap karakter alfabet dengan karakter lain sepanjang 26 karakter alfabet sehingga pengkodean hanya terjadi pada alfabet itu sendiri tanpa adanya tanda baca lain [4]. Proses enkripsi dan dekripsi *caesar cipher* dengan menggunakan 26 karakter alfabet menggunakan rumus 1 dan 2.

$$C = E(P) = (P + K) mod\ 26 \quad (1)$$

$$P = D(C) = (C - K) mod\ 26 \quad (2)$$

dengan *C* adalah *ciphertext*, *E* adalah enkripsi, *P* adalah *plaintext*, *D* adalah dekripsi, *K* adalah nilai kunci yang digunakan untuk mengganti setiap karakter dan 26 adalah jumlah karakter yang digunakan [5].

Penerapan metode *caesar cipher* telah banyak dilakukan pada penelitian sebelumnya dengan jumlah penggunaan karakter pada enkripsi dan dekrispsi serta tempat pengaplikasianya yang berbeda. Penelitian yang dilakukan oleh [1], melakukan penelitian tentang "Penerapan Kriptografi *Caesar Cipher* pada Fitur *Chatting* Sistem Informasi *Freelance*" yang membahas tentang pembangunan aplikasi *chatting* pada sistem informasi *freelance* menggunakan penerapan kriptografi *caesar cipher*. Kelemahan pada penelitian ini terletak pada penggunaan karakter yang terbatas pada proses enkripsi dan dekripsi pada metode *caesar cipher*, peneliti hanya menggunakan 26 karakter alfabet yaitu huruf A sampai Z.

Penelitian yang dilakukan oleh [3], melakukan penelitian tentang "Implementasi Kriptografi *Caesar Cipher* Menggunakan Matlab R2013a" yang membahas tentang perbaikan atau modifikasi pada jumlah karakter proses enkripsi dan dekripsi teknik kriptografi *caesar cipher*, adapun pengujian dilakukan menggunakan matlab R2013a. Kelemahan pada penelitian ini terletak pada penggunaan karakter yang terbatas pada proses enkripsi dan dekripsi pada metode *caesar cipher*, peneliti hanya menggunakan 40 karakter yaitu 26 karakter alfabet, 10 karakter *number* dan 4 karakter *symbol*.

Penelitian yang dilakukan oleh [4], melakukan penelitian tentang "Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma *caesar cipher* dan *vigenere cipher*" yang membahas tentang pembangunan aplikasi kriptografi berbasis android menggunakan algoritma kombinasi antara *caesar cipher* dan *vigenere cipher*. Kelemahan pada penelitian ini terletak pada penggunaan karakter yang terbatas pada proses enkripsi dan dekripsi pada metode *caesar cipher*, peneliti hanya menggunakan 94 karakter pada tabel ASCII yaitu pada nomor indeks antara 32 sampai 125.

Penelitian yang dilakukan oleh [6], melakukan penelitian tentang "Pembangunan Aplikasi Pembanding Kriptografi dengan *Caesar Cipher* dan *Advance Encryption Standard* (AES) untuk file teks" yang membahas tentang pembangunan aplikasi pembanding antara metode kriptografi *caesar cipher* dan *advance encryption standard* pada file teks. Kelemahan pada penelitian ini terletak pada penggunaan karakter yang terbatas pada proses enkripsi dan dekripsi pada metode *caesar cipher*, peneliti hanya menggunakan 26 karakter alfabet yaitu huruf A sampai Z. Adapun pengaplikasian metode ini dilakukan pada media komputer.

Penelitian yang dilakukan oleh [7], melakukan penelitian tentang "Implementasi Kriptografi Caesar Cipher untuk Keamanan Data" yang membahas tentang pembangunan aplikasi keamanan data dengan menggunakan metode *caesar cipher* yang pengaplikasiannya dilakukan dengan menggunakan media komputer. Kelemahan pada penelitian ini terletak pada keterbatasan penggunaan karakter pada proses enkripsi dan dekripsi *Caesar Cipher*, karakter yang digunakan hanya menggunakan 26 karakter alfabet yaitu a sampai z.

Penelitian yang dilakukan oleh [8], melakukan penelitian tentang "Implementasi Metode Caesar Cipher Alphabet Majemuk Dalam Kriptografi untuk Pengamanan Informasi" yang membahas tentang implementasi metode *caesar cipher* dengan jumlah karakter pada proses enkripsi dan dekripsi sebanyak 256 karakter. Adapun kelemahan pada penelitian ini terletak pada pengaplikasian dilakukan dengan menggunakan media komputer, sehingga tidak praktis untuk dapat dipergunakan dimana saja.

Penelitian yang dilakukan oleh [9], melakukan penelitian tentang "Implementasi Metode Caesar Cipher Dalam Penerapan Sistem E-Voting Berbasis Web Pada Pemilihan Abang None Jakarta" yang membahas tentang implementasi metode *caesar cipher* untuk sistem e-voting yang diaplikasikan dalam bentuk web. Kelemahan pada penelitian ini terletak pada keterbatasan penggunaan karakter pada proses enkripsi dan dekripsi *Caesar Cipher*, karakter yang digunakan hanya menggunakan 26 karakter alfabet yaitu a sampai z.

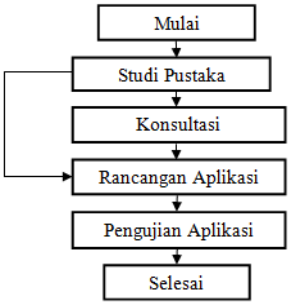
Penelitian yang dilakukan oleh [10], melakukan penelitian tentang "Perancangan Aplikasi Kriptografi Berbasis Web dengan Algoritma Double Caesar Cipher Menggunakan Tabel ASCII" yang membahas tentang merancangan aplikasi *caesar cipher* yang menekankan kombinasi dari 2 algoritma *caesar cipher* atau algoritma *double caesar cipher* yang *ciphertext*nya diterjemahkan menggunakan tabel ASCII yaitu dengan jumlah 256 karakter. Kelemahan pada penelitian ini terletak pada

pada pengaplikasian yang dilakukan pada web, sehingga kurang praktis apabila saat digunakan.

Pada penelitian ini, implementasi teknik kriptografi *caesar cipher* yang akan dibangun adalah *CaesarApp*. Berdasarkan adanya keterbatasan penggunaan karakter pada metode *caesar cipher* yang berjumlah 26 karakter alfabet dengan data karakter A-Z, penulis bermaksud melakukan modifikasi dan perbaikan pada jumlah karakter tersebut dengan menggunakan 256 karakter pada tabel ASCII. *CaesarApp* merupakan aplikasi berbasis andorid yang dibuat dengan menggunakan aplikasi *open source* android studio 3.5 sehingga penggunaan pada aplikasi *CaesarApp* lebih praktis dan dapat langsung digunakan pada *smartphone* android tanpa harus menggunakan web ataupun media komputer.

2. Metodologi Penelitian

Metode penelitian yang dilakukan dalam penelitian ini meliputi studi pustaka, konsultasi, rancangan aplikasi dan pengujian aplikasi. Model kerangka kerja yang akan digunakan dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Kerja Penelitian

Keterangan alur kerangka kerja penelitian Gambar 1, dengan tahapan:

Tahap pertama adalah memulai penelitian dengan studi pustaka yaitu pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

Tahap kedua adalah konsultasi, tahap konsultasi yaitu melakukan konsultasi atau wawancara dengan dosen pembimbing ataupun pihak-pihak yang sebelumnya membuat penelitian yang serupa sehingga mendapatkan suatu informasi yang dapat mendukung penelitian.

Tahap ketiga adalah rancangan aplikasi, yaitu merancang aplikasi dengan metode *caesar cipher* yang dipergunakan pada android. Aplikasi keamanan data ini dirancang untuk meningkatkan keamanan data dan informasi rahasia milik pribadi maupun kelompok atau organisasi dengan media android. Perancangan dan pembuatan aplikasi ini dibagi menjadi dua bagian, antara lain perancangan desain (.xml) dan program (.java). Perancangan aplikasi ini diawali dengan perancangan diagram blok sistem secara keseluruhan. Blok diagram adalah bagian terpenting dalam perancangan suatu aplikasi, karena dari blok diagram inilah dapat dilihat cara kerja aplikasi secara keseluruhan. Dengan begitu, keseluruhan blok diagram aplikasi tersebut dapat menghasilkan suatu sistem yang dapat digunakan atau difungsikan.

Tahap keempat adalah pengujian aplikasi, dalam pengujian aplikasi keamanan data ini akan diujicobakan dengan menggunakan pesan rahasia berupa *plaintext*, yang diharapkan menghasilkan keluaran berupa *ciphertext* yang dapat digunakan dengan jumlah 256 karakter. Uji coba kebenaran metode tersebut juga akan dilakukan menggunakan rumus enkripsi dan dekripsi *Caesar cipher* dengan jumlah 256 karakter.

3. Hasil dan Pembahasan

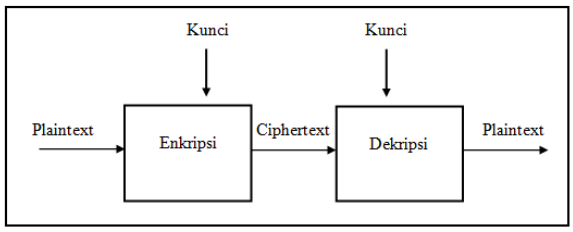
Fitur-fitur yang terdapat dalam aplikasi *caesar cipher* atau *CaesarApp* berbasis android memiliki fungsi dan tujuan yang berbeda. Fitur-fitur aplikasi dengan menggunakan *smartphone* android adalah sebagai berikut.

3.1. Rancangan Aplikasi

Halaman utama aplikasi *caesar cipher* pada Gambar 2 merupakan tampilan aplikasi dengan memiliki logo utama aplikasi *CaesarApp* yang menyediakan berbagai macam fitur. Fitur-fitur yang terdapat pada halaman utama aplikasi ini diantaranya adalah enkripsi dekripsi, *about us* dan *exit*. Fitur enkripsi dekripsi merupakan *point* utama pada penggunaan aplikasi *caesar cipher* ini, dimana fitur ini berfungsi untuk melakukan proses enkripsi dan dekripsi dengan menggunakan metode *caesar cipher*. Fitur *about us* merupakan fitur yang menampilkan informasi data pribadi peneliti. Fitur *exit* adalah fitur yang dapat dipergunakan oleh pengguna apabila ingin mengakhiri penggunaan aplikasi *CaesarApp* ini.

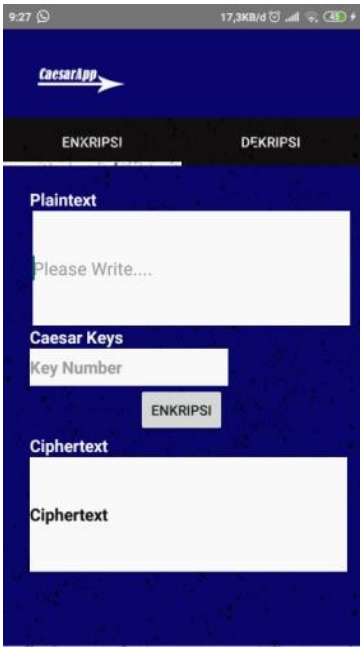
Gambar 2. Tampilan Halaman Utama Aplikasi

Pada Gambar 3 menunjukkan bahwa proses enkripsi dan dekripsi memerlukan kunci dalam mekanismenya dan biasanya berupa *string* atau deretan bilangan.



Gambar 3. Skema Enkripsi dan Dekripsi Menggunakan Kunci

Fitur Enkripsi Dekripsi yang ditampilkan pada Gambar 2 aplikasi *CaesarApp* menampilkan dua fitur dengan fungsi yang berbeda yaitu fitur enkripsi dan fitur dekripsi. Fitur enkripsi pada Gambar 4 berfungsi untuk memberikan kunci keamanan data informasi berupa teks (*plaintext*) sehingga menghasilkan data informasi berupa teks yang terkunci (*ciphertext*). Tahap pertama penggunaan fitur enkripsi ini adalah pengguna menginput data informasi berupa teks pada kolom *Plaintext*. Tahap kedua adalah pengguna menginput kunci *caesar cipher* berupa bilangan bulat pada kolom *caesar keys*, kunci *caesar cipher* inilah yang harus pengguna ingat apabila akan melakukan proses dekripsi. Tahap terakhir adalah pengguna menekan tombol enkripsi, tombol enkripsi ini digunakan untuk melakukan proses enkripsi data informasi, adapun hasil dari fitur ini berupa data informasi berupa *text* yang telah terkunci (*ciphertext*) yang akan ditampilkan secara otomatis pada kolom *ciphertext*.

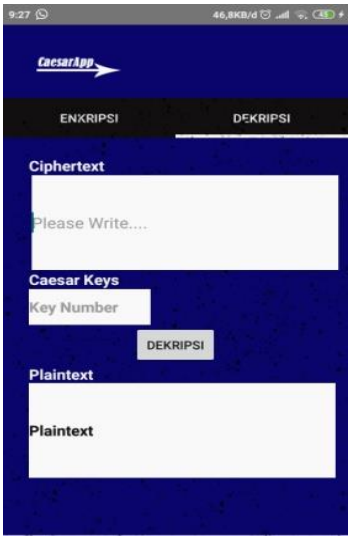


Gambar 4. Tampilan Halaman Fitur Enkripsi

Kode program untuk fitur enkripsi pada aplikasi *CaesarApp* sebagai berikut.

```
Program Enkripsi
 Private String crypt (String newString ,
 int   shift) {
  String hasil_enkrip= “”;
  char[] pecahan = newString.toCharArray();
  for (int i=0;i<pecahan.length;i++){
    hasil_enkrip+=(char)
    ((pecahan[i]+shift)%256);
    }
    Return hasil_enkrip;
 }
```

Fitur Dekripsi pada Gambar 5 berfungsi untuk membuka kunci keamanan pada data informasi berupa teks yang sebelumnya telah dilakukan pada proses enkripsi. Tahap pertama penggunaan fitur ini adalah pengguna menginput data informasi berupa teks yang telah terkunci (*ciphertext*) pada kolom *Ciphertext* adapun data informasi tersebut berupa *text* yang sebelumnya telah diamankan atau telah terkunci pada fitur enkripsi (*ciphertext*). Tahap kedua adalah pengguna menginput kunci *caesar cipher* pada kolom *caesar keys*, dimana kunci tersebut memliki nilai yang sama saat melakukan proses enkripsi. Tahap terakhir adalah pengguna menekan tombol dekripsi, tombol dekripsi digunakan untuk melakukan proses dekripsi data informasi, adapun hasil dari fitur ini berupa data informasi asli (*plaintext*) yang ditampilkan pada kolom *plaintext*.



Gambar 5. Tampilan Halaman Fitur Enkripsi Dekripsi

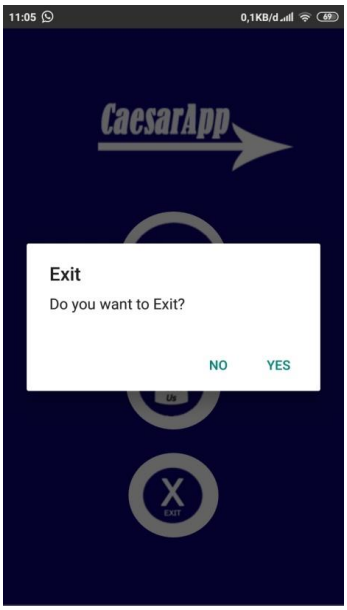
Kode program untuk fitur dekripsi pada aplikasi *CaesarApp* sebagai berikut.

```
Program Dekripsi
 Private String decrypt (String newString ,
 int   shift) {
  String hasil_decrypt= “”;
  char[] pecahan = newString.toCharArray();
  for (int i=0;i<pecahan.length;i++){
    hasil_decrypt+=(char)
    ((pecahan[i]-shift)%256);
    }
    Return hasil_decrypt;
 }
```

Fitur *About Us* pada Gambar 6 menampilkan foto dan informasi data pribadi peneliti. Data pribadi yang diberikan pada fitur ini adalah nama, tempat tanggal lahir (TTL) serta alamat email peneliti.

Gambar 6. Tampilan Halaman Fitur *About Us*

Fitur *exit* pada Gambar 7 aplikasi *CaesarApp* merupakan tampilan halaman fitur *exit*, fitur *exit* ini menampilkan sebuah teks dengan tulisan "*Do you want to exit*?" Serta pilihan *yes* atau *no*. Apabila pengguna memilih *yes*, maka aplikasi *CaesarApp* akan secara otomatis berakhir. Namun apabila pengguna memilih *no*, maka aplikasi *CaesarApp* tetap berjalan atau tidak berakhir.



Gambar 7. Tampilan Halaman *Exit*

Kode program untuk fitur *exit* pada aplikasi *CaesarApp* sebagai berikut.

Program *Exit*

```
Public void onBackPressed(){
  AlertDialog.Builder builder= new AlertDialog
  .Builder(context:MenuUtama.this);
  builder.setCancelable(false);
  builder.setMessage("Do you want to Exit?");
  builder.setPositiveButton(text:"Yes", new
  DialogInterface.OnClickListener(){
    @Override
    Public void onClick(DialogInterface dialog
    ,int which){
      Finish();
    }
  });

  builder.setNegativeButton(text:"No", new
  DialogInterface.OnClickListener(){
    @Override
    Public void onClick(DialogInterface dialog
    ,int which){
      Dialog.cancel();
    }
  });
  AlertDialog alert = builder.cretae();
  Alert.show();
}
```

3.2 Pengujian Aplikasi

Pengujian merupakan tahapan akhir pada kerangka kerja penelitian. Pada fase ini dilakukan dengan dua cara, yaitu menggunakan pengujian pada aplikasi *CaesarApp* dan melakukan pengujian dengan menggunakan rumus enkripsi dan dekripsi *Caesar cipher*. Penerapan metode *caesar cipher* disini menggunakan 256 karakter pada tabel ASCII. Adapun rumus enkripsi dan dekripsi *caesar cipher* yang digunakan pada penelitian ini adalah rumus 3 dan 4 sebagai berikut :

$$C = E(P) = (P + K) mod\ 256 \quad (3)$$

$$P = D(C) = (C - K) mod\ 256 \quad (4)$$

Gambar 8 menunjukkan hasil pengujian aplikasi *CaesarApp* pada tahap enkripsi dengan menggunakan data informasi berupa *plaintext* "(Polsri2020)" dan menggunakan kunci *caesar cipher* atau pergeseran sebesar 9 karakter. Dengan hasil uji enkripsi pada aplikasi *CaesarApp* adalah sebagai berikut.
Plaintext : (Polsri2020)
Caesar Keys : 9
Ciphertext : 1Yxu|{r;9;92

Dari hasil enkripsi di atas, pengujian proses enkripsi pada *plaintext* "(Polsri2020)" dapat dibuktikan menggunakan rumus *caesar cipher* berdasar dengan jumlah karakter yang digunakan, yaitu sebanyak 256 karakter.

Gambar 8. Hasil Pengujian Enkripsi

$$C = E(P) = (P + K) mod\ 256$$
$$= (\ (+9) mod\ 256$$
$$= (40 + 9) mod\ 256$$
$$= 49\ mod\ 256$$
$$= 49$$
$$= 1$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{P} + 9) mod\ 256$$
$$= (80 + 9) mod\ 256$$
$$= 89\ mod\ 256$$
$$= 89$$
$$= \mathrm{Y}$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{o} + 9) mod\ 256$$
$$= (111 + 9) mod\ 256$$
$$= 120\ mod\ 256$$
$$= 120$$
$$= \mathrm{x}$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{l} + 9) mod\ 256$$
$$= (108 + 9) mod\ 256$$
$$= 117\ mod\ 256$$
$$= 117$$
$$= \mathrm{u}$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{s} + 9) mod\ 256$$
$$= (115 + 9) mod\ 256$$
$$= 124\ mod\ 256$$
$$= 124$$
$$= |$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{P} + 9) mod\ 256$$
$$= (80 + 9) mod\ 256$$
$$= 89\ mod\ 256$$
$$= 89$$
$$= \mathrm{Y}$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{r} + 9) mod\ 256$$
$$= (114 + 9) mod\ 256$$
$$= 123\ mod\ 256$$
$$= 123$$
$$= \{$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (\mathrm{i} + 9) mod\ 256$$
$$= (105 + 9) mod\ 256$$
$$= 114\ mod\ 256$$
$$= 114$$
$$= \mathrm{r}$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (2 + 9) mod\ 256$$
$$= (50 + 9) mod\ 256$$
$$= 59\ mod\ 256$$
$$= 59$$
$$= ;$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (0 + 9) mod\ 256$$
$$= (48 + 9) mod\ 256$$
$$= 89\ mod\ 256$$
$$= 57$$
$$= 9$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (2 + 9) mod\ 256$$
$$= (50 + 9) mod\ 256$$
$$= 59\ mod\ 256$$
$$= 59$$
$$= ;$$
$$C = E(P) = (P + K) mod\ 256$$
$$= (0 + 9) mod\ 256$$
$$= (48 + 9) mod\ 256$$
$$= 89\ mod\ 256$$
$$= 57$$
$$= 9$$
$$C = E(P) = (P + K) mod\ 256$$
$$= () + 9) mod\ 256$$
$$= (41 + 9) mod\ 256$$
$$= 50\ mod\ 256$$
$$= 50$$
$$= 2$$

Berdasarkan perhitungan rumus *caesar cipher*, hasil enkripsi dari *plaintext* "(Polsri2020)" dengan kunci bernilai 9 adalah *ciphertext* dengan teks "1Yxu|{r};9;92".

Gambar 9 menunjukkan hasil pengujian aplikasi *CaesarApp* pada tahap dekripsi dengan menggunakan data informasi berupa *ciphertext* "1Yxu|{r};9;92" yang sebelumnya telah dilakukan proses enkripsi dengan menggunakan kunci *caesar cipher* atau pergeseran sebesar 9 karakter. Dengan hasil uji dekripsi pada aplikasi *CaesarApp* adalah sebagai berikut.
Ciphertext : 1Yxu|{r;9;92
Caesar Keys : 9
Plaintext : (Polsri2020)

Gambar 9. Hasil Pengujian Dekripsi

Dari hasil dekripsi di atas, pengujian proses dekripsi pada *ciphertext* "1Yxu|{r};9;92" dapat dibuktikan menggunakan rumus *caesar cipher* berdasar dengan jumlah karakter yang digunakan, yaitu sebanyak 256 karakter.

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ 1-9) mod\ 256 \\ &= (49-9) mod\ 256 \\ &= 40\ mod\ 256 \\ &= 40 \\ &= (\end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ Y-9) mod\ 256 \\ &= (89-9) mod\ 256 \\ &= 80\ mod\ 256 \\ &= 80 \\ &= p \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ x-9) mod\ 256 \\ &= (120-9) mod\ 256 \\ &= 111\ mod\ 256 \\ &= 111 \\ &= o \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ u-9) mod\ 256 \\ &= (117-9) mod\ 256 \\ &= 108\ mod\ 256 \\ &= 108 \\ &= l \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ |-9) mod\ 256 \\ &= (124-9) mod\ 256 \\ &= 115\ mod\ 256 \\ &= 115 \\ &= s \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ \{-9) mod\ 256 \\ &= (114-9) mod\ 256 \\ &= 114\ mod\ 256 \\ &= 114 \\ &= r \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ r-9) mod\ 256 \\ &= (114-9) mod\ 256 \\ &= 105\ mod\ 256 \\ &= 105 \\ &= i \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ ;-9) mod\ 256 \\ &= (59-9) mod\ 256 \\ &= 50\ mod\ 256 \\ &= 50 \\ &= 2 \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ 9-9) mod\ 256 \\ &= (57-9) mod\ 256 \\ &= 48\ mod\ 256 \\ &= 48 \\ &= 0 \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ ;-9) mod\ 256 \\ &= (59-9) mod\ 256 \\ &= 50\ mod\ 256 \\ &= 50 \\ &= 2 \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ 9-9) mod\ 256 \\ &= (57-9) mod\ 256 \\ &= 48\ mod\ 256 \\ &= 48 \\ &= 0 \end{aligned}$$

$$\begin{aligned} P = D(C) &= (C-K) mod\ 256 \\ &= (\ 2-9) mod\ 256 \\ &= (50-9) mod\ 256 \\ &= 41\ mod\ 256 \\ &= 41 \\ &=) \end{aligned}$$

Berdasarkan perhitungan rumus *caesar cipher*, hasil dekripsi dari *ciphertext* "1Yxu|{r};9;92" dengan kunci bernilai 9 adalah *plaintext* dengan teks "(Polsri2020)".

Pada Tabel 1, hasil dari enkripsi dan dekripsi *CaesarApp* menggunakan rumus *caesar cipher* dengan jumlah 256 karakter pada *plaintext* (Polsri2020) dan *ciphertext* "1Yxu|{r};9;92" menggunakan kunci bernilai 9, didapatkan bahwa hasil *CaesarApp* sesuai dengan hasil pengujian pada rumus *caesar cipher*. Sehingga disimpulkan bahwa aplikasi keamanan data informasi *CaesarApp* berbasis android sudah dapat digunakan.

Tabel 1. Hasil Pengujian *CaesarApp* terhadap Rumus *caesar cipher*

Proses	*CaesarApp*	Rumus *Caesar cipher*	Validasi
Enkripsi	1Yxu|{r};9;92	1Yxu|{r};9;92	Sesuai
Dekripsi	(Polsri2020)	(Polsri2020)	Sesuai

Pada Tabel 2 pengujian enkripsi dan dekripsi aplikasi *CaesarApp* yang dilakukan dengan 4 contoh data informasi dan jumlah kunci *caesar cipher* yang berbeda. Sehingga disimpulkan bahwa aplikasi *CaesarApp* telah dapat digunakan dengan berbagai macam karakter dan kunci yang berbeda-beda.

Tabel 2. Pengujian Enkripsi dan Dekripsi Aplikasi *CaesarApp*

Kunci *Caesar*	Enkripsi (*Ciphertext*)	Dekripsi (*Plaintext*)	Status
47	□~{□□x	POLSRI	Sukses
80	¢Å½±□p	Rumah?	Sukses
100	□¤ÆÙÏÙ□	#@buku!	Sukses
190	åøãíèéûëÞñ…	':%/*+=- 3	Sukses

3.3 Kelebihan Aplikasi

Kelebihan dari aplikasi *CaesarApp dengan* modifikasi metode *caesar cipher* yang diajukan ini adalah berupa desain, kemudahan dan hasil dari aplikasi terjamin keamanannya.

Desain pada aplikasi ini sangat menarik, beberapa fitur di desain dengan rapih, sehingga pengguna dapat dengan mudah dalam memahami fitur-fitur yang disediakan.

Kemudahan aplikasi ini terletak pada penggunaan aplikasi yang dapat digunakan pada media *smartphone* berbasis android, sehingga tidak memerlukan komputer untuk melakukan suatu keamanan data informasi.

Hasil dari aplikasi ini terjamin keamanannya karena menggunakan metode yang sebelumnya telah dilakukannya modifikasi dengan menambahkan jumlah karakter sebanyak 256 karakter.

3.4 Kekurangan Aplikasi

Selain kelebihan yang telah disebutkan, aplikasi *CaesarApp dengan* metode *caesar cipher* yang diajukan ini juga masih memiliki kelemahan, yaitu pada hasil karakter *ciphertext* yang tidak terbaca.

Hasil karakter *ciphertext* dengan menggunakan 256 karakter ASCII tidak dapat membaca karakter dengan baik secara keseluruhan karena keterbatasannya pembacaan karakter pada media *smartphone* berbasis android.

4. Kesimpulan

Aplikasi keamanan data informasi dengan menggunakan metode modifikasi *caesar cipher* dengan 256 jumlah karakter ini bernama *CaesarApp*. *Caesar App* dirancang menggunakan aplikasi *open source* android studio 3.5 berbasis andorid. Berdasarkan hasil pengujian aplikasi dengan menggunakan rumus *caesar cipher*, aplikasi *CaesarApp* dapat melakukan proses enkripsi dan dekripsi dengan hasil yang benar. Untuk penelitian dan pengembangan metode modifikasi *caesar cipher* pada aplikasi berbasis andorid ini dapat dilakukan dengan hanya menambahkan karakter yang dapat dibaca pada *smartphone* android. Selain itu juga dapat dilakukannya pengembangan untuk meningkatkan keamanan data informasi dengan menggabungkan atau melakukan modifikasi dengan metode atau teknik keamanan data informasi yang lainnya.

Daftar Rujukan

[1] Yuningrat, Rosihan, Salkin., 2019. *Penerapan Kriptografi Caesar Cipher pada Fitur Chatting Sistem Informasi Freelance*. Jurnal Informatika dan Ilmu Komputer (JIKO), Vol. 2, no. 2, Oktober 2019 hlm. 87-94.

[2] Robbi., 2016. *Penyisipan Pesan dengan Algoritma Pixel Value Differencing dengan Algoritma Caesar Cipher pada Proses Steganografi*. Jurnal TIMES, Vol. V, no.1 : 6-11, 2016

[3] Primaningtyas, Windi., 2017. Seminar Matematika dan Pendidikan Matematika UNY, 2017, *Implementasi Kriptografi Caesar Cipher Menggunakan Matlab R2013a*. Universitas Negeri Yogyakarta.

[4] Imam, Retnani, Rita., 2017. *Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher dan Vigenere Cipher*. Just IT (Jurnal Sistem Informasi, Teknologi dan Komputer), Vol. 9, no. 2, hlm 142-149.

[5] Adnan., 2019. *Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher dan Transposisi Cipher*. JL-TI (Jurnal Teknologi Informasi), Vol. 3, no.1, Juni 2019.

[6] Aji, Anita., 2015. *Pembangunan Aplikasi Pembanding Kriptografi dengan Caesar Cipher dan Advance Encryption Standard (AES) untuk File Teks*. Jurnal Penelitian Komunikasi dan Opini Publik, Vol. 19, no.3, Desember 2015: 213-222.

[7] Rindy, Aliy., 2019. *Implementasi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data*. Jurnal Informasi dan Komputer, Vol. 7, no.2 :81-86, 2019.

[8] Anjar., 2016. *Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi*. Indonesia Journal on Networking and Security, Vol. 5. no. 3 : 16-19, Agustus 2016.

[9] Radithya, Fauziah, Deny., 2020. *Implementasi Metode Caesar Cipher Dalam Penerapan Sistem E-Voting Berbasis Web pada Pemilihan Abang None Jakarta*. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), Vol. 4, no. 3 : 235-246, April 2020.

[10] Endah, Wheny, Achmad, Syaifudin, Bagus., 2017. *Perancangan Aplikasi Kriptografi Berbasis Web Dengan Algoritma Double Caesar Cipher Menggunakan Tabel ASCII.*