Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

Perancangan Aplikasi Pengamanan Data Text Menggunakan Kombinasi Algoritma Hill Cipher Dan Algoritma RSA

Yuza Reswan[1], Dedy Agung Prabowo[2]
[1]*Jurusan Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Bengkulu*
[2]*Jurusan Sistem Informasi, Fakultas Teknik, Universitas Muhammadiyah Bengkulu*
[1] *yuzareswan@umb.ac.id,* [2]*dedyagungprabowo@umb.ac.id*

ABSTRACT

It is now commonplace that secrecy must be truly enhanced and tightened as it weighs the emergence of the latest technology that is growing rapidly. Of course an agency, group, or individual have data that is confidential and do not want to be known by other parties hence the need for a system capable of securing the data. For this reason this research aims to create Cryptography application by applying a combination of Hill Cipher and RSA algorithm, Cryptography is also called coding language and I apply Hill Cipher because it is a classical method that uses multiplication for each encoded character while RSA is a modern method that has 2 keys ie key public and secret key where the public key is used for encryption and secret key to retranslate the original form. By applying a combination of classical and modern methods it can be more secure so it is more difficult to be solved by unwanted parties.

Keyword : Data Security, Cryptography, Hill Cipher, RSA

ABSTRAK

Di masa sekarang sudah menjadi hal yang biasa bahwa kerahasiaan harus benar – benar ditingkatkan dan diperketat karena menimbang kemunculan teknologi terbaru yang semakin pesat berkembang. Tentu sebuah Instansi, kelompok, ataupun individu memiliki data yang bersifat rahasia dan tidak ingin diketahui oleh pihak lain maka dari itu diperlukannya system yang mampu mengamankan data tersebut. Untuk itulah penelitian ini bertujuan membuat aplikasi Kriptografi dengan menerapkan kombinasi *Algoritma Hill Cipher* dan *RSA*, Kriptografi juga disebut bahasa persandian dan saya menerapkan *Hill Cipher* karena merupakan metode klasik yang menggunakan perkalian untuk tiap karakter yang disandikan sedangkan *RSA* adalah metode modern yang memiliki 2 kunci yaitu kunci publik dan kunci rahasia dimana kunci publik digunakan untuk penyandian dan kunci rahasia untuk menterjemahkan kembali k bentuk asli. Dengan menerapkan kombinasi metode klasik dan modern ini dapat lebih mengamankan sehingga lebih sulit untuk dapat di pecahkan oleh pihak – pihak yang tidak diinginkan.

Kata Kunci : Pengamanan Data, Kriptografi, Hill Cipher, RSA.

1. PENDAHULUAN

Perkembangan teknologi informasi pada zaman sekarang ini meningkat dengan pesat dan memungkinkan kita mendapatkan informasi secara cepat, tepat dan efisien serta mempunyai manfaat yang sangat besar. Kebutuhan akan informasi semakin meningkat sesuai dengan kebutuhannya[1]. Hal ini membuktikan bahwa teknologi informasi dapat mempermudah dalam menyelesaikan suatu pekerjaan serta dapat mempersingkat waktu suatu pekerjaan khususnya pekerjaan yang berhubungan dengan pengolahan informasi atau data. Dengan semakin banyaknya penggunaan teknologi komputer saat ini, maka permasalahan pun akan bermunculan. Salah satunya yaitu masalah keamanan dan kerahasiaan data yang merupakan aspek penting dari suatu sistem informasi.

Masalah ini dapat berupa pencurian dan pemanipulasian informasi atau data oleh pihak yang tidak berwenang. Misalnya suatu perusahaan memiliki data penting dan bersifat rahasia, namun perusahaan atau organisasi tersebut tidak memiliki aplikasi program yang mengamankan data tersebut sehingga data tersebut dapat diketahui oleh pihak yang tidak berwenang seperti pesaing dari perusahaan lain, yang kemudian memanipulasi dan bahkan menyalin data tersebut. Oleh karena itu suatu cara untuk mengamankan informasi atau data yang sangat penting dan rahasia. Salah satunya yaitu dengan menggunakan kriptografi.

Kriptografi merupakan ilmu yang berguna untuk menyandikan suatu tulisan, data atau informasi yang tidak boleh dilihat, dibaca, dimanip ulasi dan diakui kepemilikan informasi tersebut oleh pihak yang tidak berkepentingan. Algoritma Kriptografi terbagi dua berdasarkan jenis kuncinya yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris atau kunci rahasia, merupakan algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Sedangkan algoritma asimetris atau kunci publik, merupakan algoritma yang menggunakan kunci publik untuk mengenkripsi dan kunci pribadi untuk mendekripsikannya.

Salah satu metode kriptografi yang digunakan untuk menjaga kerahasiaan informasi adalah enkripsi dan dekripsi. Enkripsi dibentuk berdasarkan algoritma yang mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tidak bisa dimengerti. Sedangkan dekripsi merupakan proses dengan algoritma yang sama untuk mengembalikan informasi yang sudah teracak menjadi bentuk aslinya. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih kearah metode-metode yang digunakan[2].

2. LANDASAN TEORI

2.1. Kriptografi

Kriptografi berasal dari dua kata yaitu Crypto dapat diartikan rahasia (secret) dan Graphy dapat diartikan tulisan (writing) jadi Kriptografi dapat diartikan sebagai suatu ilmu atau seni untuk mengamankan pesan agar tidak diketahui oleh pihak yang tidak diinginkan atau kriptografi adalah seni dari penulisan rahasia atau membaca sandi atau tulisan–tulisan rahasia[3].

Kriptografi adalah mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Prinsip-prinsip yang mendasari kriptografi yakni[4] :

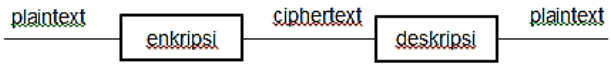
a. Data integrity (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
b. Authentication (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
c. Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah

Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

d. Confidelity (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim.

Plaintext, adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Dengan kata lain plainteks (plaintext) adalah teks-jelas (cleartext). Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (ciphertext). Ciphertext inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan.



Gambar 1 : Alur Enkripsi dan Deskripsi

Dalam sistem komputer, pesan terbuka (plaintext) diberi lambang M, yang merupakan singkatan dari message. Plaintext ini dapat berupa tulisan, foto, atau video yang berbentuk data biner. Plaintext inilah yang nantinya akan dienkripsi menjadi pesan rahasia atau ciphertext yang dilambangkan dengan C (ciphertext). Secara matematis, fungsi enkripsi ini dinotasikan dengan:

E(M) = C.....(1)

Dimana:
M = Pesan Asli
E = Proses Enkripsi
C = Pesan dalam bahasa Sandi

Sedangkan fungsi dekripsi adalah proses pembalikan dari ciphertext menjadi plaintext kembali, secara matematis dinotasikan sebagai berikut:

D(C) = M.....(2)
D(E(M)) = M.....(3)

Dimana:
M = Pesan Asli
D = Proses Deskripsi
C = Pesan dalam bahasa Sandi

2.2. Algoritma Kriptografi

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

a. Enkripsi, merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut

Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

Plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enskripsi bisa diartikan dengan Cipher atau kode.

b. Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (tesk-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma untuk enkripsi.
c. Kunci, yang dimaksud adalah kunci yang dipakai untu melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (private key) dan kunci umum (public key).

2.3. Hill Cipher

Hill cipher dapat digolongkan sebagai kriptografi polyalphabetic yang dapat dikategorikan sebagai block cipher, karena teks yang akan diproses dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter pada satu blok akan mempengaruhi hasil karakter lainnya dalam proses enkripsi maupun dekripsinya, karena karakter yang sama pada blok sebelumnya tidak akan dipetakan menjadi karakter yang sama pada blok sesudahnya. Pada tahun 1929 Lester S. Hill menciptakan algoritma Hill Cipher[5].

Teknik kriptografi ini diciptakan dengan maksud untuk menciptakan cipher yang tidak dapat dipecahkan menggunakan teknik anlisis frekuensi. Terdapat beberapa alasan mengapa algorima kriptografi Hill Cipher sulit untuk dipecahkan. Alasan tersebut adalah sebagai berikut :

a. Hill Cipher menggunakan perkalian untuk dasar enkripsi dan dekripsinya, jadi abjad pada plaintext tidak digantikan oleh abjad yang sama begitu juga dengan ciphertext.
b. Dengan menggunakan perkalian yang lebih besar maka teknik pengamanan frekuensinya menjadi semakin tinggi.

Proses enkripsi pada Hill Cipher dan sekema alur adalah[6] :

$$C = K \cdot P \quad \text{.....(4)}$$

Dimana :
C = Ciphertext
K = Kunci
P = Plaintext

Gambar 2 : Enkripsi Hill

Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

Proses dekripsi pada Hill Cipher dapat diturunkan dari persamaan :

Gambar 3 : Deskripsi Hill

Pengenkripsian pada Hill Cipher yaitu dengan perkalian untuk masing-masing karakter dirubah dari plaintext ke bentuk ciphertext yang nilai terlebih dahulu, Untuk mengembalikan atau menterjemahkan ke bentuk asli atau deskripsi maka dari hasil perkalian tadi dirubah dengan bentuk invers (P = C . K-1), yaitu masing - masing karakter dibagi dengan besaran yang telah ditetapkan.

2.4. RSA

Algoritma RSA diciptakan oleh 3 orang peneliti dari MIT (Masschussets Institute of Technology) pada tahun 1976, yaitu Ron (R)ivest, Adi (S)hamir dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya menfaktorkan bilangan yang besar menjadi faktor-faktor prima. Penfaktoran dilakukan untuk memperoleh kunci private. Selama penfaktoran bilangan besar menjadi bilangan prima belum tentu menemukan algoritma yang benar, maka selama itu pula keamanan algoritma RSA terjamin.

Dalam setiap proses pada algoritma RSA terdapat perhitungan matematis. Pada proses pembangkitan kunci dibutuhkan perhitungan untuk menentukan nilai Totient n dan perhitungan dengan algoritma Euclidean untuk menentukan nilai dua buah bilangan yang relatif prima[7].

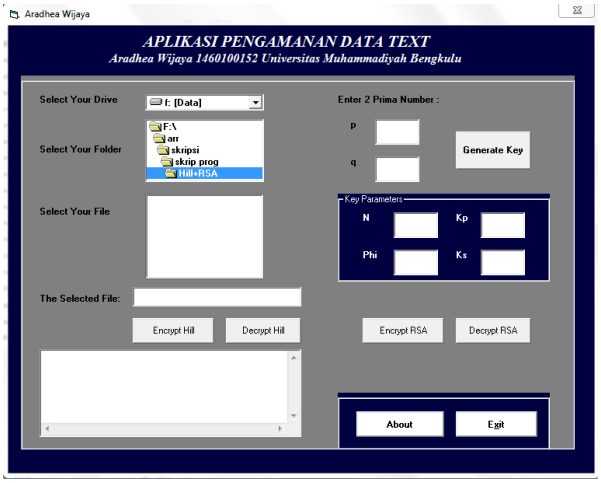
a. Fungsi Totient Euler φ: Fungsi Totient euler φ atau biasa disebut dengan fungsi euler merupakan salah satu fungsi yang dipakai dalam perhitungan matematis pada algoritma RSA. Fungsi euler mendefinisikan φ(n) untuk n ≥ 1 yang menyatakan jumlah bilangan bulat positif < n yang relatif prima dengan n. Dua bilangan bulat a dan b dikatakan relatif prima jika gcd(a,b) = 1(pembagi bersama terbesar dari a dan b adalah 1). Jika n = p . q (p dan q bilangan prima), maka φ(n) = φ(p).φ(q) = (p-1)(q-1).
b. Algoritma Euclidean: Algoritma ini digunakan untuk mencari nilai pembagi persekutuan terbesar (PBB) dari dua bilangan bulat. Algoritma ini didasarkan pada pernyataan bahwa ada dua buah bilangan bulat tak negatif yakni m dan n dimana nilai m ≥ n. Adapun tahap-tahap pada algoritma Euclidean adalah[8] :
    1. Jika n = 0 maka m adalah PBB(m, n); stop. Kalau tidak (yaitu n ≠ 0) lanjutkan ke langkah nomor 2.
    2. Bagilah m dengan n dan misalkan sisanya adalah r.
    3. Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah nomor 1.

Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

4. HASIL PENELITIAN

4.1 Proses Enkripsi Data

Dalam penggunaan Aplikasi Pengamanan Data Teks ini sendiri perlu diperhatikan agar user selalu mencatat ataupun mengingat Kunci Deskripsi Data sehingga dapat mengembalikan data yang telah diamankan menjadi data yang dapat dibaca kembali. Dalam proses enkripsi data yang asli akan dilakukan proses pengacakan dengan algoritma yang sudah ditentukan. Tampilan utama dari aplikasi seperti pada gambar berikut :



Gambar 4 : Tampilan Sistem

Tampilan ini meminta user untuk mengisi field yang ada sebagai proses enkripsi. Adapun langkah-langkah proses enkripsi adalah :

1. User mencari data teks yang akan diamankan pada driver computer.
2. Setelah data dipilih dilanjutkan dengan menekan tombol Encrypt Hill.
3. Maka pada enkripsi tahap 1 karakter pada setiap teks akan dirubah kebentuk decimal dan kemudian akan dilakukan perkalian dengan rumus **C = P . K,** maka akan ditampilkan ciphertext.
4. Setelah ciphertext didapatkan, dilanjutkan kembali enkripsi tahap akhir dengan mengisi field p dan q dengan biangan prima, tekan tombol Generate Key.
5. Kemudian ditampilkan hasil perhitungan RSA pada field Key Parameter.

Penjelasan :

Nilai N didapatkan dengan rumus

N = p x q. .....(5)

Ex : 19 x 41 = 779

Nilai Totient Euler didapatkan dengan rumus

φ(n) = φ(p).φ(q) = (p-1)(q-1). .....(6)

Ex : (19-1) (41-1) = 720

Nilai Kp didapatkan dengan rumus

GCD (φ(n) ,e). .....(7)

Ex : GCD (e,720) = 1

e	GCD (e,720)
2	720 mod 2 = 0 GCD (2,720) = 2
3	720 mod 3 = 0 GCD (3,720) = 3
4	720 mod 4 = 0 GCD (4,720) = 4
5	720 mod 5 = 0 GCD (5,720) = 5
6	720 mod 6 = 0 GCD (6,720) = 6
7	720 mod 7 = 6 7 mod 6 = 1 GCD (7,720) = 1

Jadi didapatkan nilai Kp adalah 7.

Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

Nilai Ks didapatkan dengan rumus

$$d = \frac{1+K^{-1}.\varphi n}{e} \text{ . .....(8)}$$

Ex : K = { 1, 2, 3, 4 …dst}

1. D = $\frac{1+1.720}{7}$ = 103
2. D = $\frac{1+2.720}{7}$ = 205,857142
3. D = $\frac{1+3.720}{7}$ = 308,714286

Jadi didapatkan nilai Ks adalah 103.

6. User kemudian menekan tombol Encrypt RSA dan data akan diamankan menggunakan rumus

   $C = P^{Kp} \bmod N$. .....(9)

7. Maka akan didapatkan kunci untuk deskripsi data, dan datapun telah diamankan.

   Adapun koding Visual Basic pada proses Encrypt saat pengaman data yang isinya meliputi :

a. Enkripsi tahap 1

```
Open fn For Input As #1
        While Not (EOF(1))
            Line Input #1, lin
            dsize = Len(lin)
            If dsize > 0 Then
                ReDim pdata(1 To dsize)
            Else
                ReDim pdata(i)
            End If
            linefeed = ""
            i = 1
            Do Until i = dsize + 1
                 pdata(i) = Mid(lin, i, 1)
                 cenc = Asc(pdata(i)) * 2
                 splain = splain & Chr(cenc)
                i = i + 1
            Loop
        Wend

         Close #1

        Text9.Text = splain
```

b. Enkripsi tahap 2

```
PRIME1 = Text3.Text
PRIME2 = Text4.Text
PROD = PRIME1 * PRIME2
PHIE = (PRIME1 - 1) * (PRIME2 - 1)

cont = False
For i1 = 2 To (PHIE - 1)
   If cont = False Then
       a1 = PHIE Mod i1
       If a1 = 0 Then
       Else
           PUBLICKEY = i1
           cont = True
       End If
   End If
Next i1

cont = False
For q = 1 To 100000
    If cont = False Then
        If ((PUBLICKEY * q) Mod PHIE) = 1 Then
            SECRETKEY = q
            cont = True
        End If
    End If
Next q
```

4.2 Proses Deskripsi Data

Proses deskripsi merupakan proses yang dilakukan untuk menterjemahkan file yang telah diamankan sehingga dapat dibaca kembali, untuk langkahnya sendiri berkebalikan dengan proses enkripsi. Adapun langkah-langkah proses deskripsi adalah :

1. User mencari data yang akan diterjemahkan pada driver computer.
2. Saat data dipilih dan menekan tombol Decrypt RSA. Maka akan diminta untuk memasukan kunci deskripsi data.
3. Setelah kunci dimasukan maka data akan dideskripsi tahap 1 dengan rumus
   $P = C^{Ks} \bmod N$. .....(10)
4. Kemudian dilanjutkan dengan menekan tombol Decrypt Hill maka deskripsi tahap akhir akan proses dengan rumus
   $P = C \cdot K^{-1}$. .....(11)
5. Maka data yang sebelumnya diamankan telah diterjemahkan dan dapat dibaca kembali.

Pada proses Decrypt untuk menerjemahkan kembali data teks meliputi :

a. Deskripsi tahap 1

Jurnal Sistem Informasi (JSI), VOL.10, NO.2, Oktober 2018
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal2.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

```
txtTemp.Text = txtFileName.Text
If (UCase(Right(txtFileName.Text, 3)) <> "TXT") Then
    MsgBox "Cannot Encrypt This Type Of File!", vbExclamation, "Type Mismatch!!!"
    Exit Sub
End If
SECRETKEY = InputBox("Masukan Kunci Deskripsi", "Crypto System")
PROD = InputBox("Masukan Kode Phi", "Crypto System")
Open fn For Input As #1
    While Not EOF(1)
        Line Input #1, lin
        dsize = Len(lin)
        If dsize > 0 Then
            ReDim pdata(1 To dsize)
        Else
            ReDim pdata(1)
        End If
        rlinefeed = ""
        j = ""
        i = 1
        Do Until i = dsize + 1
            j = Mid(lin, i, 1)
            rlinefeed = rlinefeed & j
            i = i + 1
        Loop
        X = rlinefeed
        Y = SECRETKEY
        N = PROD
```

b. Deskripsi tahap 2

```
        pcnt = 1
        jc = 1
        For ic = 1 To chlen
            If ch(ic) <> 0 Then
                suma(jc) = (disp(ic))
                pcnt = pcnt + 1
                jc = jc + 1
            End If
        Next ic

        res = 1
        Dim q1 As Integer
        res = (suma(1) * suma(2)) Mod N
        For q1 = 2 To (pcnt - 2)
            res = (res * suma(q1 + 1)) Mod N
        Next q1
        pout = Chr(res / 2)

        Dim loc As Integer
        filepout = filepout & pout
        X = Y = N = res = 0
    Wend
    Open fnt For Append As #2
            Print #2, filepout
    Close #2
Close #1
FileCopy fnt, fn
Kill (fnt)
MsgBox ("Decryption Is Completed Successfully")
```

5. KESIMPULAN

Berdasarkan hasil dari pembuatan aplikasi pengamanan data teks menggunakan kombinasi algoritma Hill Cipher dan RSA, maka didapatkan kesimpulan yaitu :

1. Rancangan kombinasi aplikasi dibuat dengan melipatgandakan atau dua kali proses pengamanan.
2. Persandian dan penterjemahan pada aplikasi ini menggunakan 2 tahap yaitu pengamanan pertama diamankan menggunakan algoritma Hill Cipher kemudian diamankan kembali pada tahap akhir menggunakan algoritma RSA.
3. Dengan aplikasi ini, file data teks yang bersifat penting dan rahasia yang tidak ingin diakses ataupun diketahui oleh pihak yang tidak diinginkan dapat lebih diamankan.
4. Aplikasi ini mudah untuk digunakan oleh siapapun dengan kapasitas ukuran memory sangat kecil, hanya 104 kb saja.

5. Lama waktu yang diperlukan untuk proses enkripsi berkaitan dengan berapa banyak karakter yang akan dienkripsi, sedangkan hasil dari proses enkripsi juga akan menambah ukuran dari file yang cukup besar sehingga mempengaruhi kapasitas memory.

DAFTAR PUSTAKA

[1] Prabowo, D. A. (2016). Sistem Informasi Pendataan Mahasiswa Menggunakan Fitur Binary Large Object (Blob) Untuk Menyimpan Data Gambar (Studi Kasus: Program Studi Sistem Informasi Universitas Muhammadiyah Bengkulu). *Jurnal Pseudocode*, *3*(1), 10-14

[2] Basuki, A., Paranita, U., & Hidayat, R. (2016). Perancangan aplikasi kriptografi berlapis menggunakan algoritma caesar, transposisi, vigenere, dan blok chiper berbasis mobile. *Semnasteknomedia online*, *4*(1), 1-2

[3] Munir, Rinaldi. (2004). Kriptografi. Bandung. Informatika.

[4] Kori Carda Puspita. Implementasi Kriptografi Dengan Metode Rsa Menggunakan Java. Diakses pada 20 may 2016.

[5] Hill, L. S. (1929). Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, *36*(6), 306-312.

[6] Arif, M. H., & Fanani, A. Z. (2016). Kriptografi Hill Cipher dan Least Significant Bit untuk Keamanan Pesan pada Citra. *CSRID (Computer Science Research and Its Development Journal)*, *8*(1), 60-72.

[7] Lubis, M. S., Budiman, M. A., & Manik, K. L. (2013). Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)* (Vol. 1, No. 1).

[8] Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to algorithms*. MIT press.