JURNAL
TEKNOLOGI INFORMASI
DAN KOMUNIKASI

Vol.7 No. 1, Juni 2018 : 11 - 26

KRIPTOGRAFI HYBRIDA AGLORITMA HILL CIPHER DAN RIVEST SHAMIR ADLEMAN (RSA) SEBAGAI PENGEMBANGAN KRIPTOGRAFI KUNCI SIMETRIS (STUDI KASUS : NILAI MAHASISWA AMIK MBP)

HYBRID CRYPTOSYSTEM HILL CIPHER ALGORITHM AND RIVEST SHAMIR ADLEMAN *(RSA) ALGORITHM AS DEVELOPMENT OF CRYPTOGRAPHY WITH SYMMETRIC KEY (CASE STUDY : STUDENT GRADES AMIK MBP)*

Lisda Juliana Pangaribuan
Akademi Manajemen dan Informatika Komputer Medan Business Polytechnic
Jl. Djamin Ginting no.285-287, Medan
lisdajuliana@gmail.com

ABSTRAK

Risiko mengirim informasi melalui internet adalah tingkat keamanan yang rendah, sebab itu informasi harus dijaga supaya informasi tersebut dikirim dan diterima oleh orang yang berhak. Nilai mahasiswa yang dikirim ke Sistem Informasi Akademik AMIK MBP dapat di bajak oleh kriptanalis, sehingga perlu adanya metode untuk mengamankan nilai tersebut. Untuk meningkatkan keamanan informasi digunakan kriptografi. Penelitian ini bertujuan untuk menganalisis kinerja algoritma kriptografi terhadap peningkatan keamanan nilai sehingga nilai tidak dapat dibajak oleh kriptanalis. Algoritma yang digunakan adalah modifikasi algoritma hill cipher dengan menggunakan hybrid cryptosystem untuk menyembunyikan kunci. Kunci yang digunakan karakter ASCII yang diubah menjadi numerik kemudian disusun dengan matriks 3x3 yang memiliki determinan dan invertible. Penelitian ini menggunakan metode kuantitatif yang bersifat pengembangan dengan membangun sebuah sistem untuk melakukan uji coba dan analisis. Hasil penelitian menunjukkan dengan kriptografi hybrida pada kunci Hill dan algoritma RSA, pengiriman nilai lebih aman daripada kriptografi menggunakan kunci hill cipher. Untuk mengetahui kunci hill harus mencoba 256^9 kombinasi angka, dan untuk mengetahui kunci hill setelah di hybrid dengan Rivest Shamir Adleman (RSA) 12 bit mencapai $256^9 \times 10^{36}$ kemungkinan, RSA 16 bit mencapai $256^9 x 10^{45}$ kemungkinan, RSA 32 bit mencapai $256^9 x 10^{81}$ kemungkinan. Jumlah karakter setelah di enkripsi dan di dekripsi tetap sama demikian juga besar file setelah di dekripsi menggunakan kriptografi hybrid karena penggunaan modulo 256, sedangkan waktu yang digunakan untuk dekripsi kriptografi hybrid ternyata lebih lama daripada hill cipher.

Kata Kunci*: Kriptografi_Hybrida, HillCipher, RSA, Keamanan_Informasi.*

ABSTRACT

Risk of sending information through internet is a low level of security so information must received by rightful persns. Student's grade of AMIK which is sent to website can be plowed by cryptanalyst, so it needs a method for secure the information. To improve security of information uses cryptography. This study aims to analyze the performance of cryptographic algorithm to improve message security so it can't be replaced by others. The algorithm which is used is modification of hill cipher algorithm by using hybrid cryptosystem to hide the key. The key used is ASCII arranged with 3x3 matrics that have a determinant and an invertible. This research used quantitative d*evelopmental method by building a system to analyze. The result showed that using hybrid cryptosystem on the hill key and RSA algorithm delivery of students's grade is more secure than using hill key. To find out hill key should try* 256^9

combinations, to guess hill key after hybrid process through RSA 12bit reach 256^9x10^{36} possibility, 16bit reach 256^9x10^{45} possibility, 32bit reach 256^9x10^{81} times. Size of files after encryption and decryption remains the same due to the use of modulo 256, while the time used for decryption of hybrid cryptography was longer than hill cipher.

***Keywords**: Hybrid_Cryptosystem, HillCipher, RSA, Information_security.*

PENDAHULUAN

AMIK MBP (Akademi Manajemen Informatika Komputer Medan Busines Politeknik) Medan mengirim daftar nilai mahasiswa melalui jaringan internet yang dapat disadap dan dimodifikasi oleh *cryptanalys.* Pengiriman informasi melalui internet mempunyai risiko di bidang keamanan, sebab itu informasi memerlukan pengamanan yang baik saat didistribusikan ataupun saat disimpan.

Selain steganografi, metode yang dapat digunakan untuk pengamanan data adalah kriptografi. Hal yang perlu dipertimbangkan untuk menentukan algoritma kriptografi yang akan digunakan dalam sistem keamanan data adalah kekuatan kunci terhadap serangan *Cryptanalis* dan pertimbangan kecepatan dalam proses enkripsi serta dekripsi. Jika kunci sudah diketahui kriptanalis maka seluruh informasi yang dikirim dapat diketahui. Namun dalam pengiriman informasi, pengguna harus memilih suatu pilihan yang sulit antara keamanan dan kenyamanan. Masalah inilah yang membuat para peneliti mempelajari dan mengembangkan algoritma yang dapat meningkatkan keamanan dan kenyamanan Informasi.

Kriptografi algoritma *Rivest Shamir Adleman* (RSA) dan algoritma *Hill Cipher* masih menjadi perhatian dalam penelitian terkait dengan keamanan informasi. Torani dan Falahati [1] mengatakan *Hill Cipher* merupakan algoritma enkripsi simetris yang rentan terhadap serangan *known-plaintext*. Bila kriptanalisis dapat mengumpulkan *plaintext* dan *ciphertext* dengan kunci yang sama maka kriptanalisis dapat mengetahui kunci *Hill*. Oleh sebab itu kunci harus dibuat sekuat dan seaman mungkin karena keamanan pengiriman informasi terletak pada distribusi kunci, jika kunci sudah diketahui kriptanalis maka seluruh informasi yang dikirim dapat diketahui.

Wowor [2] mengatakan *plaintext* yang dienkripsi menggunakan algoritma *hill cipher* akan menghasilkan jumlah karakter (besar file) yang sama dengan *plaintext* aslinya sehingga tidak ada perubahan dalam jumlah memori yang dipakai. Hal ini membuat waktu proses enkripsi cepat. Namun, jika dimodifikasi menggunakan *Convert Between Base*, jumlah *file* lebih besar sehingga memori yang digunakan juga lebih besar dan waktu proses enkripsi dan dekripsi lebih lambat.

Menurut penelitian Shahram dan Siavash [3] *Hill Cipher* kuat dalam menghadapi *Ciphertext-Only Attack* (COA) namun COA telah mampu dipecahkan dengan *Chinese Remainder Theorem*. Untuk itu, algoritma *Hill cipher* sebaiknya dikembangkan lagi. Salah satunya adalah dengan melakukan kombinasi terhadap algoritma asimetris, misalnya dengan algoritma RSA.

Mahajan dan Sigh [4] mengatakan algoritma RSA aman karena untuk memfaktorkan bilangan prima yang besar membutuhkan waktu yang lama, namun algotitma RSA tidak nyaman karena proses menghitung bilangan prima membutuhkan waktu yang lebih lambat sehingga akan mengakibatkan lambatnya proses enkripsi dan dekripsi. Penelitian serupa juga dikemukakan oleh Meng and Zheng [5] yang mengatakan algoritma RSA aman untuk bilangan prima yang besar, sedangkan untuk bilangan prima 512 bit sudah dapat dipecahkan oleh *cryptanalyst* , dan untuk bilangan prima besar membutuhkan waktu dan kompleksitas ruang. Menurut Chmielowiec [6] panjang kunci yang aman untuk algoritma RSA adalah 1024 bit. Tao [7] dalam

penelitiannya juga mengatakan keamanan algoritma RSA dapat dilakukan dengan meningkatkan jumlah digit atau panjang kunci menggunakan faktorisasi bilangan prima 7 x 107.

Oleh sebab itu, menurut Lyer [8] salah satu solusi untuk keamanan distribusi kunci, dibuatlah Kriptografi hibrida (*Hybrid Cryptosystem).* Kriptografi hibrida merupakan algoritma yng memanfaatkan dua tingkatan kunci yaitu kunci rahasia simetris dengan satu kunci (*session key*) dan enkripsi asimetris dengan sepasang kunci (*public/private key)* kriptografi hibrida diharapkan akan memberi keamanan yang lebih baik terhadap pengiriman informasi dengan rasio ukuran dan waktu proses enkripsi yang lebih baik sehingga *bandwith* jaringan yang digunakan relatif kecil.

Berdasarkan latar belakang di atas, maka dibuat penelitian dengan judul " Kriptografi Hybrida Agloritma Hill Cipher Dan RSA Sebagai Pengembangan Kriptografi Kunci Symetris (Studi Kasus : Nilai Mahasiswa Amik MBP)".

Penelitian ini diharapkan dapat mengatasi kelemahan kriptografi algoritma hill cipher dalam mengamankan kunci dengan melakukan *hybrid cryptosystem* terhadap algoritma RSA sehingga keamanan nilai mahasiswa meningkat. Dari hasil penelitian nantinya akan diketahui ukuran file (jumlah karakter) setelah proses enkripsi dan dekripsi. Selain itu juga diketahui waktu proses enkripsi dan dekripsi pesan berdasarkan waktu CPU. Untuk membuktikan keamanan pesan juga akan dilakukan cara mengenkripsi dan mendekripsi pesan (nilai mahasiswa) menggunakan *hybrid cryptosystem* algoritma *hill cipher* dan algoritma RSA .

Penelitian ini bertujuan menganalisis kinerja algoritma *hybrid cyptosystem* algoritma Hill Cipher dan algoritma RSA terhadap keamanan pengiriman nilai mahasiswa.

Kriptografi

Konheim [9] mengatakan bahwa kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari sebuah sumber informasi ke suatu tujuan pengiriman informasi. Adapun kunci yang digunakan dalam algoritma kriptografi menurut jenisnya ada dua macam, yaitu: algoritma simetris dan algoritma asimetris. Hoffstein [10] mengatakan algoritma kriptografi simetris atau disebut juga algoritma kriptografi konvensional. Algoritma Simetris adalah algoritma dimana kunci untuk proses enkripsi sama dengan dan proses dekripsi, misalnya permutasi, subtitusi, *Hill Cipher*. Sedangkan algoritma kriptografi asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Untuk mendekripsi pesan, penerima menggunakan kunci rahasia *(secret key)* Paar [11], contohnya RSA dan ElGamal.

Kriptografi Hibrida (*Hybrid Cryptosystem*)

Tyagi N. *et al* [12] mengatakan *Hybrid Cryptosystem* merupakan gabungan dari *asymmetric cryptosystem* dan *symmetric cryptosystem* dengan memanfaatkan kelebihan masing-masing *cipher*, sementara menurut Gupta and Singh [13] Sebuah *Hybrid Cryptosystem* dapat dibangun dengan menggunakan dua kriptografi yang terpisah yaitu kunci yang memiliki skema enkapsulasi kunci publik dan kunci yang memiliki skema enkapsulasi kunci simetris.

Manajemen Kunci

Selain algoritma kriptografi, manajemen kunci yang baik juga faktor pendukung dalam meningkatkan keamanan pesan. Hal ini didukung oleh Schneier [14] yang mengatakan *cryptanalyst* sering menyerang kriptografi kunci simetris dan kunci public melalui manajemen kunci. Menurut Munir [15], bagian dari manajemen kunci adalah pembangkit kunci, pendistribusian kunci dan protokol pertukaran kunci. Pendistribusian kunci dapat dilakukan dengan mengunduh atau diberikan langsung. Untuk mencegah pemalsuan kunci oleh pihak ketiga maka diperlukan adanya sertifikat.

Manajemen kunci lainnya yaitu protokol pertukaran kunci. Protokol pertukaran kunci merupakan suatu sistem dimana dua pihak bernegosiasi untuk menentukan *secret value*. Contohnya adalah SSL (*secure socket layer*).

Algoritma *Hill Cipher*

Hill Cipher merupakan penerapan arithmetic modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Algoritma enkripsi *hill cipher* menurut Dooley [16] diawali dengan menentukan *plaintext* terlebih dahulu kemudian korespondensikan abjad pada *plaintext* dengan numerik. Setelah itu tentukan kunci dimana kunci adalah matriks bujursangkar yang memiliki determinan dan invertible yaitu memiliki *multiplicative inverse* atau K^{-1}. Matriks kunci harus memiliki determinan yang relative prima dengan 256 atau gcd (d,256) = 1. Setelah itu. masukkan *plaintext* kemudian *plaintext* ditranspose sesuai panjang *plaintext* dan ukuran kolom matriks kunci. *Plaintext* memiliki ukuran kolom yang sama dengan ukuran baris matriks kunci. Kemudian hitung *Ciphertext* dengan ketentuan C=K.P mod 256 …….. (1)

dimana : C= *Ciphertext*
P= *Plaintext*
K=Matriks kunci

Setelah proses enkripsi dilakukan proses deskripsi. Algoritma dekripsi *hill cipher* dilakukan dengan mengorespondenkan abjad dengan numerik. Langkah kedua cari invers dari matriks kunci dengan rumus :

$K = \frac{1}{Det\ A}$; dimana A adalah matriks kunci;

Det A = nilai determinan matriks kunci

$K^{-1} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ * Adj K ……(2) ;

dimana : Adj K = Adjoint matriks kunci
K^{-1} = Invers Matriks.

Bila invers matriks kunci pecahan, konversikan matriks kunci menjadi integer. Langkah ketiga masukkan *ciphertext* kemudian *ciphertext* ditranspose sesuai panjang pesan dan ukuran kolom invers matriks kunci. Langkah terakhir hitting *plain text* dengan rumus:

$P = K^{-1}.C \bmod 256$ …….. (3)

dimana: P= *Plaintext*
K^{-1} = invers matrix kunci
C=*Ciphertext*

Algoritma RSA

Palanisamy [17] mengatakan RSA melibatkan kunci publik dan sebuah kunci pribadi. Kunci publik dapat diketahui semua orang dan digunakan untuk mengenkripsi pesan. Kemudian pesan yang dienkripsi dengan kunci publik hanya dapat dideskripsi kembali menggunakan kunci pribadi.

Langkah-langkah yang digunakan untuk membangkitkan pasangan kunci di RSA dirumuskan oleh Paar [11] yaitu pilih dua buah bilangan prima sembarang p dan q. (rahasiakan p&q). Kedua hitung:

n = p * q …… (4)., dengan p ≠ q dan n tidak rahasia. Ketiga hitung

$\varphi(n) = (p-1)*(q-1)$ …….. (5) ; dimana n= hasil perkalian 2 buah bilangan prima; dan $\varphi(n)$=(bilangan prima pertama-1) dikali (bilangan prima kedua-1); Keempat pilih kunci public e, yang relativ prima terhadap $\varphi(n)$ atau

$GCD(e, \varphi(n)) = 1$;dimana e ≠ (p-1), e ≠ (q-1)……. (6).

Kelima bangkitkan kunci privat d dengan kekongruenan $e.d \equiv 1 \pmod{\varphi(n)}$. Maka

$d = e^{-1} (1 + k.\varphi(n))$

atau $d = \frac{1 + k.\varphi(n)}{e}$ …….. (7)

dimana d adalah bilangan bulat murni. Hasil dari algoritma diatas adalah kunci publik (n, e) dan kunci privat (d,e).

Algoritma enkripsi dan dekripsi RSA

Algoritma enkripsi RSA yang dirumuskan oleh Paar[11] diawali dengan mengambil kunci publik milik penerima pesan (n dan e). Lalu pecah *plainteks* menjadi blok-blok m_1, m_2,…,

sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, n-1]. Setiap blok m dienkripsi menjadi blok c_i dengan rumus

$$\mathbf{c_i = p_i^e \bmod n} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

dimana $\mathbf{c_i}$ = chiperteks (pesan yang telah didekripsi) dan p_i = plainteks (pesan); e dan n adalah kunci public.

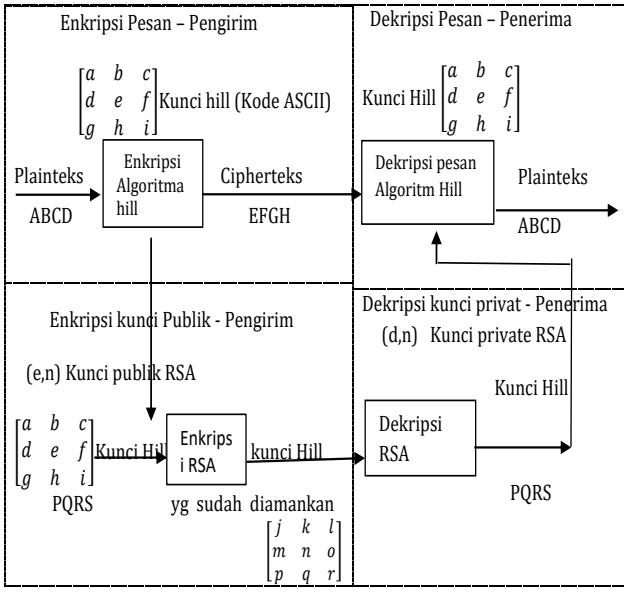
Untuk mendapatkan *plainteks* kembali, blok *cipherteks* ci didekripsi menjadi blok m_i dengan rumus

$$\mathbf{p_i = c_i^d \bmod n} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9)$$

dimana $\mathbf{p_i}$= plainteks (pesan yang telah dienkripsi) ; d dan n adalah kunci privat.

METODE PENELITIAN

Metode penelitian menggunakan metode kuantitatif yang bersifat pengembangan dengan penerapan metode *hybrid cryptosystem* terhadap algoritma *hill cipher* dan algoritma RSA melalui studi literatur dan perhitungan matematis yang dilengkapi dengan sebuah sistem sebagai *tools* untuk melakukan pengujian terhadap hasil penelitian.



Gambar1. Alur kerja *Hybrid Criptosystem Hill Cipher* dan RSA

Sesuai dengan Gambar1, penelitian ini dilakukan dengan beberapa tahapan. Pada tahap pertama ditentukan *Plaintext. Plaintext* adalah file daftar nilai mahasiswa dengan *field* NamaDosen, KodeMatakuliah, NilaiAngka, NilaiHuruf. Kemudian masukkan kunci karakter ASCII yang diubah menjadi numerik dalam bentuk matriks ber-ordo 3x3. Matriks kunci memiliki determinan dan invertible yaitu memiliki *multiplicative inverse* atau K^{-1}. Bila determinan matriks kunci *hill* = 0 atau bilangan genap, maka matriks tidak boleh dijadikan kunci *hill*. Tahap kedua, sesuaikan *plaintext* dengan ukuran kunci lalu enkripsikan p*laintext* menggunakan kunci yang diberikan dengan algoritma *Hill Cipher*. Dan tahap ketiga adalah mengamankan kunci *hill* dengan mengenkripsi menggunakan algoritma RSA. Dari proses ini akan diperoleh kunci public dan kunci privat untuk membuka kunci yang telah dienkripsi. Tahap terakhir mendekripsikan kembali *ciphertext* yang diterima dengan algoritma *Hill Cipher* sehingga kembali ke pesan yang sebenarnya. Dari tahapan ini nantinya akan diketahui besar *file* (jumlah karakter) setelah dienkripsi dan didekripsi. Waktu proses juga akan diketahui sesuai dengan waktu CPU.

HASIL DAN PEMBAHASAN

Untuk mengetahui hasil penelitian, maka dilakukan pengujian dan analisa. Input data adalah sebuah file.txt.

Pengujian Keamanan *Hybrid* RSA dan *Hill Cipher*.

Algoritma *hill* dengan matriks kunci 3x3 sudah dianggap aman. Namun masih dapat dipecahkan oleh kriptanalis karena kunci enkripsi (pengirim) sama dengan kunci dekripsi (penerima), demikian menurut Wowor [2]. Bila kunci penerima diketahui maka pesan asli dapat dibuka.

Pada penelitian ini digunakan pesan asli : **LISDAMKK4121431000886A**

Konversi ke angka desimal pada kode ASCII menjadi **76 73 83 68 65 77 75 75 52 49 50 49 52 51 49 48 48 48 56 56 54 65.** Ubah plaintext ke dalam matriks dengan jumlah kolom

3 menjadi :

$$\begin{bmatrix} 76 & 68 & 75 & 49 & 52 & 48 & 56 & 65 \\ 73 & 65 & 75 & 50 & 51 & 48 & 56 & 88 \\ 83 & 77 & 52 & 49 & 49 & 48 & 54 & 88 \end{bmatrix}$$

Kunci yang diberikan kepada penerima adalah : **KOMINFOKU** diubah kedalam angka menjadi

$$\begin{bmatrix} 75 & 79 & 77 \\ 73 & 78 & 70 \\ 79 & 75 & 85 \end{bmatrix}$$

Setelah dihitung determinannya 2724. Karena deteminan angka genap dan GCD (2724, 256) ≠ 1 maka matriks tidak dapat dijadikan sebagai kunci.

Lalu ubah kunci menjadi : $\begin{bmatrix} 24 & 18 & 13 \\ 237 & 60 & 36 \\ 229 & 147 & 0 \end{bmatrix}$

Sesuai dengan rumus persamaan (1) ,maka diperoleh nilai *Ciphertext* =

$$\begin{bmatrix} 121 & 219 & 242 & 153 & 243 & 80 & 238 & 192 \\ 36 & 4 & 83 & 249 & 252 & 112 & 144 & 45 \\ 231 & 39 & 40 & 139 & 205 & 128 & 64 & 173 \end{bmatrix}$$

Diubah menjadi ASCII menjadi

y$çÛ_'òS(™ù‹óüÍPp□î□@À-

Sesuai dengan rumus (2) diperoleh kunci

invers = $\begin{bmatrix} 76 & 129 & 100 \\ 108 & 217 & 95 \\ 45 & 190 & 58 \end{bmatrix}$

Untuk mengetahui pesan asli digunakan rumus

$Pi = K^{-1} * Ci \bmod 256$…… (3)

Sesuai dengan rumus persamaan (3) diperoleh

nilai Pi = $\begin{bmatrix} 76 & 68 & 75 & 49 & 52 & 48 & 56 & 65 \\ 73 & 65 & 75 & 50 & 51 & 48 & 56 & 88 \\ 83 & 77 & 52 & 49 & 49 & 48 & 54 & 88 \end{bmatrix}$

Jika dikonversi kedalam kode ASCII maka Pi = LISDAMKK4121431000886AXX dimana XX adalah *Dummy.* Sehingga Plainteks menjadi **LISDAMKK4121431000886A**. Dengan demikian maka dapat dibuktikan bahwa jika kunci pengirim diketahui maka *cryptanalyst* dapat mengetahui pesan asli . Untuk mengetahui kunci *hill* dengan cara *bruto forse* maka harus mencoba 256^9 kombinasi angka.

Untuk meningkatkan keamanan maka kunci pengirim akan dienkripsikan terlebih dahulu dengan algoritma RSA dengan cara :

Kunci = $\begin{bmatrix} 24 & 18 & 13 \\ 237 & 60 & 36 \\ 229 & 147 & 0 \end{bmatrix}$

Kunci dienkripsi dengan algoritma RSA dengan nilai : p = 11 dan q = 43 . Dengan menggunakan persamaan (4) diperoleh nilai n = 472 , kemudian dengan persamaan (6) diperoleh nilai e = 31, sedangkan dari persamaan(5) diperoleh nilai φ = 420 dan dengan menggunakan persamaan (7) didapat nilai d = 271.

Untuk kunci 12 bit akan dienkripsi menjadi

255 370 101 457 181 36 185 26 0

Plaintext yang dikirim =

y$çÛ_'òS(™ù‹óüÍPp□î□@À-

Kunci diubah ke matriks 3 x 3 menjadi

$$\begin{bmatrix} 255 & 457 & 185 \\ 370 & 181 & 26 \\ 101 & 36 & 0 \end{bmatrix}$$

Determinan = 43617. Dengan menggunakan rumus (2), maka diperoleh hasil :

$K^{-1} = \begin{bmatrix} 41 & 247 & 167 \\ 90 & 68 & 93 \\ 143 & 30 & 231 \end{bmatrix}$

Jika kunci dipakai untuk medekripsikan *ciphertext* maka sesuai dengan rumus (3) hasilnya menjadi :

$$Pi = \begin{bmatrix} 206 & 96 & 239 & 109 & 202 & 96 & 206 & 6 \\ 5 & 57 & 168 & 109 & 215 & 96 & 44 & 77 \\ 64 & 254 & 0 & 18 & 64 & 80 & 146 & 161 \end{bmatrix}$$

Plainteks = **206 5 64 96 57 254 239 168 0 109 109 18 202 215 64 96 96 80 206 44 146 6 77 161** dikonversikan ke dalam kode ASCII menjadi **:Î @`9þï¨ mm Ê×@``PÎ,' M¡**Sedangkan plaintext asli = LISDAMKK4121431000886A. Dari proses tersebut dapat dilihat bahwa pesan yang didekripsi tidak sama dengan pesan asli. Ini membuktikan bahwa dengan melakukan kriptografi hibrida pesan yang dikirim lebih aman. Dengan demikian kunci penerima pesan kuat.

Proses Enkripsi Pesan Dengan Algoritma Hill cipher

Plaintext=LISDAMKK4121431000886A

Konversi ke angka desimal pada kode ASCII menjadi **76 73 83 68 65 77 75 75 52 49 50 49 52 51 49 48 48 48 56 56 54 65.** Ubah plaintext ke dalam matriks dengan jumlah kolom 3

menjadi :

$$\begin{bmatrix} 76 & 68 & 75 & 49 & 52 & 48 & 56 & 65 \\ 73 & 65 & 75 & 50 & 51 & 48 & 56 & 88 \\ 83 & 77 & 52 & 49 & 49 & 48 & 54 & 88 \end{bmatrix}$$

Huruf X ditambah dibelakang untuk mengisi kekosongan karakter. Dengan menggunakan persamaan (1), maka diperoleh angka desimal hasil enkripsi dari *plaintext* adalah **121 36 231 219 4 39 242 83 40 153 249 139 243 252 205 80 112 128 238 144 64 192 45 173**. Dengan kode ASCII hasil enkripsi adalah :
y$çÛ_'òS(™ù‹óüÍPp□î□@À-.

Proses Enkripsi Dan Dekripsi Kunci Dengan Algoritma RSA.

Selanjutnya kunci harus diamankan. Proses enkripsi kunci dengan algoritma RSA diawali dengan memilih nilai p dan q. Angka yang dipilih untuk nilai p = 71 dan nilai q = 59. Dengan menggunakan persamaan (4) diperoleh n= 4189, dengan persamaan (5) diperoleh nilai ϕ(n)=4060, kemudian dengan persamaan (6) didapati nilai e= 1767, dan dengan menggukan persamaan (7) diperoleh nilai d= 1783. Sehingga kunci public dan kunci privat yang diperoleh adalah kunci publik = 4189, 1767 sedangkan kunci privat = 1783, 1767.

Kunci Hill = $\begin{bmatrix} 24 & 18 & 13 \\ 237 & 60 & 36 \\ 229 & 147 & 0 \end{bmatrix}$

di enkrispi dengan persamaan (8). Dengan demikian didapatkan kunci hill yang telah dienkripsi adalah : **2457 2 2456 1889 3954 1858 4136 948 0.**

Untuk mengetahui kunci asli maka kunci yang diterima harus didekripsi terlebih dahulu. Kunci yang akan didekripsi adalah :
2457 2 2456 1889 3954 1858 4136 948 0
Kunci didekripsi dengan persamaan (9) sehingga kunci menjadi: $\begin{bmatrix} 24 & 18 & 13 \\ 237 & 60 & 36 \\ 229 & 147 & 0 \end{bmatrix}$

Proses dekripsi pesan dengan algoritma *Hill Cipher* adalah dimulai dengan *chipertext* **y$çÛ_'òS(™ù‹óüÍPp□î□@À-** diubah kembali menjadi angka desimal pada kode ASCII sehingga menjadi **121 36 231 219 4 39 242 83 40 153 249 139 243 252 205 80 112 128 238 144 64 192 45 173** . Setelah dihitung dengan persamaan (2) maka kunci invers = $\begin{bmatrix} 76 & 129 & 100 \\ 108 & 217 & 95 \\ 45 & 190 & 58 \end{bmatrix}$

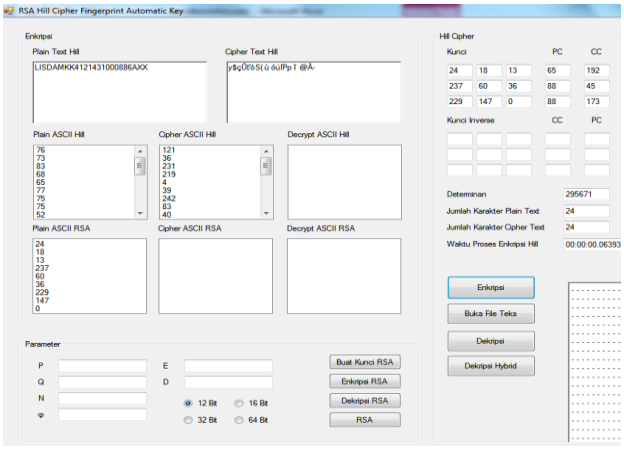
Untuk mengembalikan pesan ke semula digunakan dengan rumus persamaan (3) maka diperoleh *plaintext* : 76 73 83 68 65 77 49 50 49 52 52 49 48 48 48 56 56 54 65 88 88. Bila di konversi kedalam kode ASCII menjadi **LISDAMKK4121431000886AXX**. Huruf X adalah dummy sehingga plainteks menjadi **LISDAMKK4121431000886A.**

Hasil Simulasi Proses Enkripsi dan Dekripsi

Berdasarkan sistem yang telah dibangun, hasil simulasi dari **hybrid cryptosystem algoritma hill cipher dan RSA** dilihat pada proses berikut ini :

Proses Enkripsi dan Dekripsi Pesan Dengan Algoritma Hill Cipher.

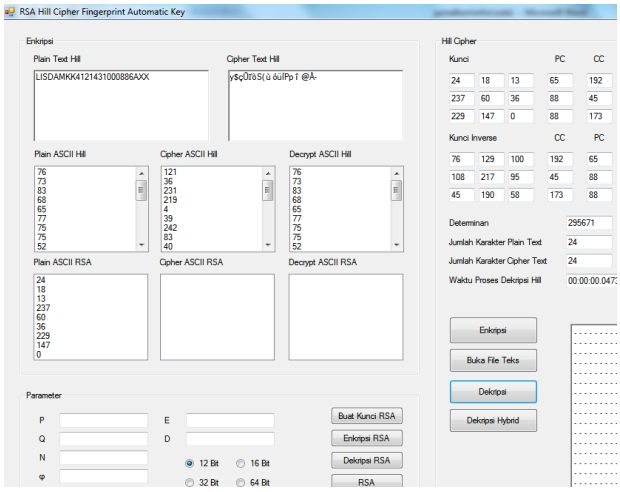
Proses enkripsi pesan dengan menggunakan algoritma *hill cipher* dapat dilhat pada Gambar 2.



Gambar 2. Proses enkripsi pesan dengan algoritma hill cipher

Pada Gambar 2 dapat dilihat proses enkripsi dengan menggunakan kunci hill

$\begin{bmatrix} 24 & 18 & 13 \\ 237 & 60 & 36 \\ 229 & 147 & 0 \end{bmatrix}$. Setelah diinput *plaintext* **LISDAMKK4121431000886A** yang diambil dari sebuah file nilai.txt , diketahui besar file atau jumlah karakter adalah 24 karakter, 2 karakter adalah *dummy*. Dari sistem dapat dilihat hasil enkripsi menjadi : $\begin{bmatrix} 121 & 219 & 242 & 153 & 243 & 80 & 238 & 192 \\ 36 & 4 & 83 & 249 & 252 & 112 & 144 & 45 \\ 231 & 39 & 40 & 139 & 205 & 128 & 64 & 173 \end{bmatrix}$. Angka pada matriks diubah dalam bentuk ASCII menjadi **y$çÛ_'òS(™ù‹óüÍPp□î□@À-**. *Ciphertext* **y$çÛ_'òS(™ù‹óüÍPp□î□@À-** berjumlah 24 karakter (24 byte) walaupun tidak semua kelihatan karena ada beberapa kode ASCII yang tidak dapat ditampilkan misalnya *space, tab* dan tombol yang lain. *Ciphertext* **y$çÛ_'òS(™ù‹óüÍPp□î□@À-** inilah yang akan dikirim ke penerima. Waktu yang dibutuhkan untuk mengenkripsi pesan adalah 00:00:00.0639371 detik. Dekripsi *ciphertext* dengan algoritma *Hill Cipher* menggunakan kunci yang sama dengan kunci enkripsi. Proses dekripsi dengan *hill cipher* dapat dilihat pada Gambar 3. Proses dekripsi membutuhkan waktu : 00:00:00.0473737 detik.



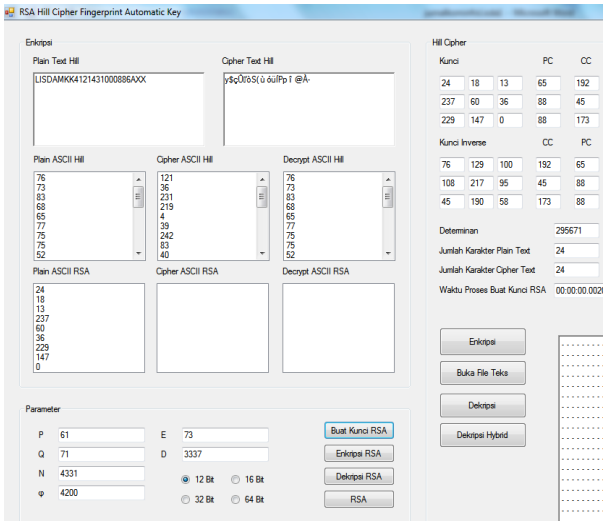
Gambar 3. Proses Dekripsi Dengan Hill Cipher

Matrik hasil dekripsi sesuai Gambar 3 adalah: $\begin{bmatrix} 76 & 68 & 75 & 49 & 52 & 48 & 56 & 65 \\ 73 & 65 & 75 & 50 & 51 & 48 & 56 & 88 \\ 83 & 77 & 52 & 49 & 49 & 48 & 54 & 88 \end{bmatrix}$ = **LISDAMKK4121431000886AXX**

Hasil dekripsi kembali menjadi *plain text* sebesar 24 characters (24 byte). Dari hasil implementasi dapat diketahui bahwa waktu dekripsi *ciphertext* dengan algoritma *Hill Cipher* lebih lambat dibandingkan dengan waktu enkripsi *plaintext*. Hal ini disebabkan oleh karena menghitung enkripsi hanya menggunakan determinan dan kunci, sedangkan menghitung dekripsi menggunakan invers matriks dan waktu untuk menghitung invers matriks lebih lama dari pada menghitung determinan. Waktu yang dibutuhkan akan lebih lama kalau diperoleh nilai yang tidak interger (bulat) harus terlebih dahulu di konversi ke bilangan bulat.

Proses Enkripsi dan Dekrpsi Dengan Algoritma Hybrid RSA dan Hill Cipher

Kunci harus di amankan terlebih dahulu dengan menggunakan algoritma RSA. Untuk itu diperlukan pembuatan kunci RSA dengan melakukan percobaan untuk kunci 12 bit. Proses membuat kunci 12 bit dapat dilihat pada Gambar 4.

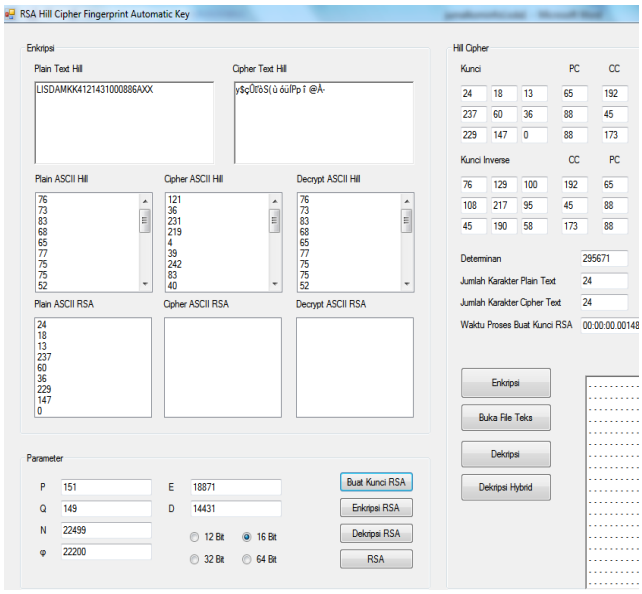


Gambar 4. Pembuatan kunci 12 bit

Dari Gambar dapat dilihat nilai p dan q yang dipilih secara acak adalah p = 61 q = 71. Kemudian dengan rumus persamaan (4) diperoleh n = 4331. Dari rumus persamaan (5) didapati nilai ϕ(n)= 4200. Dari Gambar juga dapat dilihat nilai e = 73 dan nilai d= 3337. Dari

proses pembentukan kunci 12 bit tersebut diperoleh kunci publik = 4331,73. dan kunci privat = 3337,73. Waktu yang dibutuhkan untuk membuat kunci RSA 12 bit adalah 00:00:00.0007053 detik.

Proses pembuatan kunci RSA 16 bit dapat dilihat pada Gambar 5.

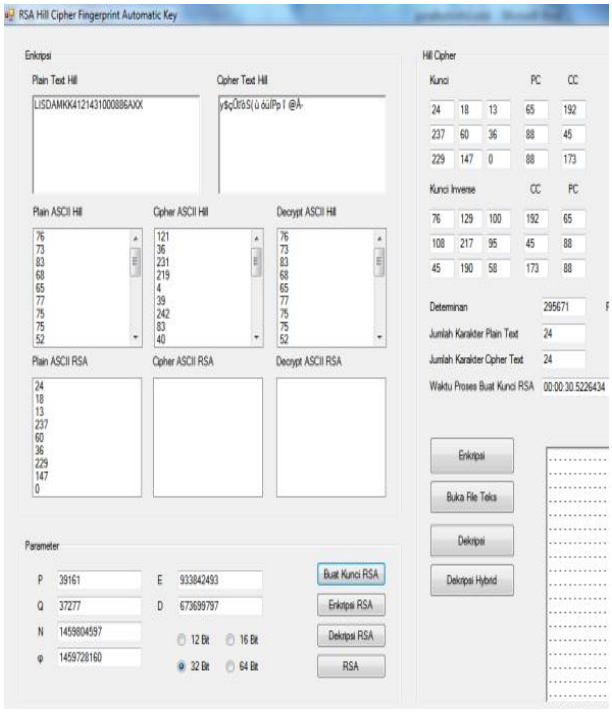


Gambar 5. Pembuatan kunci 16 bit

Dari sistem dilihat waktu pembuatan kunci 16 bit 00:00:00.0007342 detik. Secara acak diberikan nilai p = 113 q = 41, dengan menggunakan persamaan (4) diperoleh nilai n= 4633 kemudian dengan persamaan (5) didapati nilai ϕ(n) = 4480. Lalu dengan persamaan (6) dan (7) diperoleh nilai e= 569 dan nilai d= 1929. Dari proses tersebut diperoleh kunci publik = 4633, 569 dan kunci privat = 1929, 569.

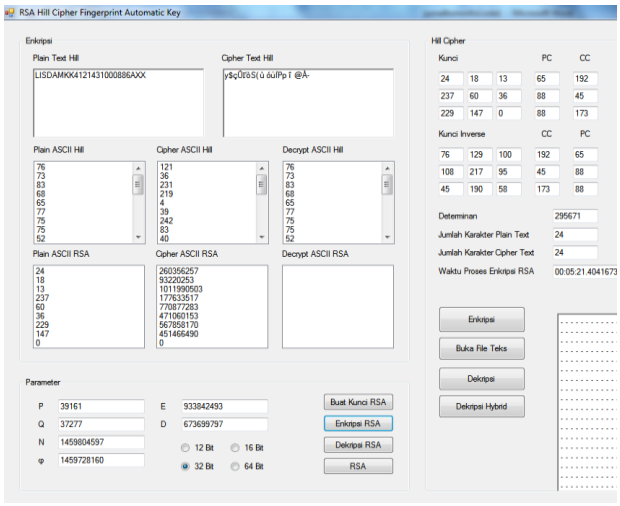
Sedangkan proses pembuatan kunci 32 bit dapat dilihat pada Gambar 6. Waktu yang dibutuhkan untuk membuat kunci 32 bit adalah 00:00:19.4184832 detik dengan nilai p = 39161 dan nilai q = 37277. Dengan menggunakan persamaan (4) dapat diketahui nilai n = 1459804597 dan sesuai persamaan (5) diperoleh nilai ϕ = 1459728160. Kemuadian dengan persamaan (6) dan persamaan (7) diperoleh nilai e = 933842493 dan d = 673699797. Dari proses tersebut didapatkan kunci public = 1459804597 , 933842493 dan kunci privat = 6736997971, 933842493.

Waktu untuk membuat kunci RSA tergantung pada jumlah bit kunci, jika jumlah bit kunci makin panjang maka nilai bilangan prima p dan q juga makin besar sehingga waktu pembuatan kunci makin lama.



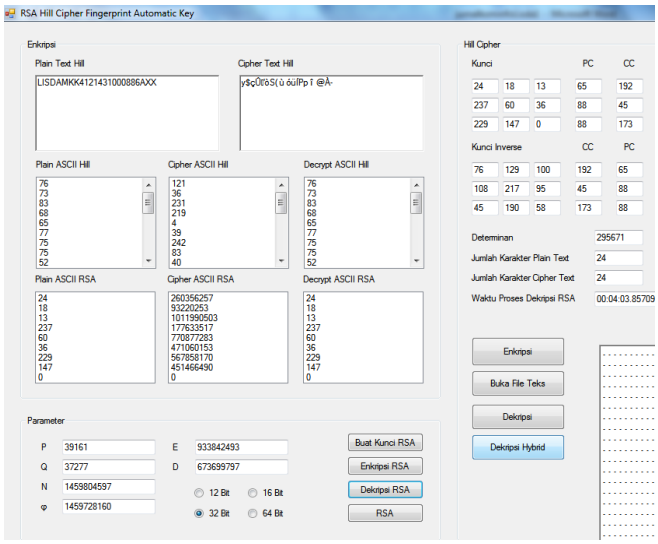
Gambar 6. Proses pembuatan kunci 32 bit

Setelah proses pembentukan kunci public dan kunci privat, *kunci Hill* akan diamankan terlebih dahulu sebelum diberikan kepada penerima pesan dengan mengenkripsi menggunakan algoritma RSA. Proses enkripsi yang digunakan adalah dengan kunci 32 bit. Proses enkripsi kunci *Hill* dapat dilihat pada Gambar 7. Kunci *hill* yang dienkripsi adalah **24 18 3 237 60 36 229 147 0.** Hasil enkripsi adalah **332527821 498382408 163832222 111996410 29391187 172626334 73397591 371326128 0 .** Kunci inilah yang akan diberikan kepada penerima pesan, sehingga keamanan kunci meningkat. Waktu yang dibutuhkan untuk melakukan proses enkripsi adalah 00:01:05.8522038 detik.



Gambar 7. Enkripsi kunci 32 bit

Setelah melakukan proses enkripsi kunci dengan algoritma RSA, selanjutnya untuk mengetahui kunci yang sebenarnya maka kunci yang diberikan kepada penerima harus didekripsi terlebih dahulu. Proses dekripsi kunci dapat dilihat pada Gambar 8.



Gambar 8. Dekripsi kunci RSA 32 bit

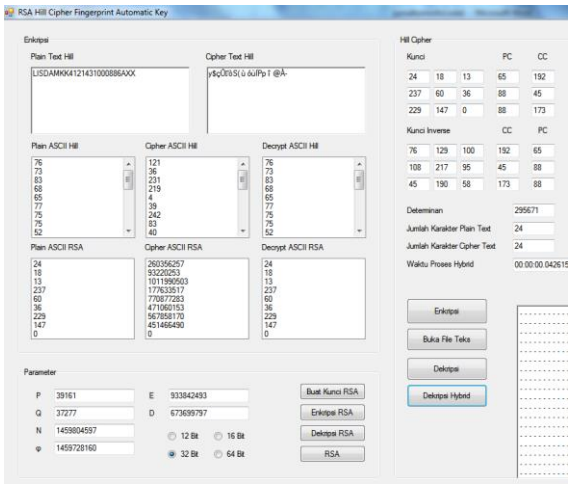
Waktu untuk mendekripsi kunci 00:02:36.6650126 detik. Waktu dekripsi lebih lama dari waktu enkripsi. Hal ini terjadi karena bilangan pangkat (nilai d) yang diproses untuk dekripsi jauh lebih besar daripada bilangan pangkat untuk enkripsi.

Dari Gambar 8 dapat dilihat bahwa kunci yang akan di enkripsi adalah **332527821 498382408 163832222 111996410 29391187 172626334 73397591 371326128 0.** Setelah di dekripsi akan kembali ke kunci Hill semula yaitu **24 18 3 237 60 36 229 147 0.**

Dari hasil enkripsi beberapa kunci dapat dilihat pada lampiran 5 bahwa tingkat kesulitan untuk menebak kunci 32 bit adalah $256^{9}x10^{9x9}$ atau $\mathbf{256^{9}x10^{81}}$.

Waktu untuk mengenkripsi kunci RSA lebih cepat dari pada waktu untuk dekripsi kunci RSA karena nilai d jauh lebih besar dari nilai e sehingga untuk mengitung nilai pangkat dekripsi lebih lama dari pada enkripsi.

Setelah mengetahui kunci aslinya maka untuk mengetahui pesan sebenarnya, *ciphertext* yang diterima akan di dekripsikan kembali dengan algoritma *hill cipher*. Proses dekripsi *Hybrid* algoritma RSA dan *Hill cipher* dapat dilihat pada Gambar 9.



Gambar 9. Dekripsi Hybrid Algoritma RSA dan Algoritma Hill Cipher

Sesuai dengan waktu CPU, waktu yang dibutuhkan untuk mendekripsikan *ciphertext* adalah 00:00:00.0426159. Setelah dilakukan proses dekripsi dengan algoritma *hill cipher*, *ciphertext* yang dikirim akan kembali ke pesan aslinya yaitu : **LISDAMKK4121431000886AXX**.

Jumlah karakter setelah dienkripsi adalah 24 karakter dan jumlah karakter setelah didekripsi juga 24 karakter. Sesuai dengan waktu CPU, waktu yang digunakan untuk

melakukan dekripsi *ciphertext* dengan algoritma *Hybrid* RSA dan *Hill Cipher* ternyata lebih cepat daripada waktu yang digunakan untuk melakukan dekripsi *ciphertext* dengan algoritma *Hill Cipher*, sedangkan jumlah karakter (besar file) setelah dienkripsi dan di dekripsi sama. Hal ini disebabkan karena penggunaan modulo 256 dalam perhitungan enkripsi jadi batas karakter setelah dienkripsi dan setelah didekripsi adalah 0 sampai 255. Jadi masing-masing karakter setelah dienkripsi akan menjadi 1 karakter ASCII juga.

Pengujian dan simulasi menunjukkan bahwa metode *hybrid cyptosystem* RSA dan *Hill Cipher* dibandingkan *Hill Cipher* terbukti dapat mengembalikan pesan yang telah di enkripsi ke pesan semula setelah proses dekripsi.Hasil percobaan terhadap beberapa kunci dapat dilihat pada lampiran 3.

SIMPULAN

Hasil penelitian menunjukkan bahwa dengan melakukan *hybrid cryptosystem* pada kunci *Hill Cipher* pada matriks 3x3 dengan algoritma RSA keamanan pengiriman nilai mahasiswa lebih baik karena kunci enkripsi tidak sama dengan kunci dekripsi. Selain itu sangat sulit menebak angka kunci karena jumlah karakter kunci yang dikirim kepada penerima tidak sama dengan jumlah karakter kunci yang sebenarnya. Jika dilakukan dengan *bruto force* menebak kunci *hill* ada 256^9 kemungkinan, dan untuk menebak kunci *hill* setelah di *hybrid* dengan RSA 12 bit mencapai 256^9x10^{36} kemungkinan, sementara untuk RSA 16 bit mencapai 256^9x10^{45} kemungkinan, dan untuk RSA 32 bit mencapai 256^9x10^{81} kemungkinan. Selain itu *plaintext* yang sama akan menghasilkan *ciphertext* yang berbeda jika kunci yang diberikan berbeda, sedangkan untuk besar file(jumlah karakter) yang sama waktu yang digunakan untuk melakukan dekripsi *ciphertext* dengan *Hybrid Cryptosystem* menggunakan algoritma *Hill Cipher* dan algoritma RSA ternyata lebih lama daripada waktu yang digunakan untuk melakukan dekripsi *ciphertext* dengan algoritma *Hill Cipher*. Waktu untuk membuat kunci RSA tergantung pada jumlah bit kunci dan tergantung pada nilai p dan q yang diacak. Makin besar nilai p dan q, maka waktu pembuatan kunci makin lama, sementara waktu proses enkrispi dan dekripsi kunci dengan RSA tergantung pada panjang kunci.

Jumlah karakter (besar file) setelah dienkripsi dan di dekripsi sama. Hal ini disebabkan karena penggunaan modulo 256 dalam perhitungan enkripsi jadi batas karakter setelah dienkripsi dan setelah didekripsi adalah 0 sampai 255 sehingga masing-masing karater setelah dienkripsi akan menjadi 1 karakter ASCII juga.

DAFTAR PUSTAKA

[1] Toorani, M. and Falahati, A., A Secure Variant of the Hill Cipher, *Proceedings of the 14th IEEE Symposium on Computers and Communications (ISCC'09).* DOI 10.1109/ISCC.2009.5202241, 2009.

[2] Wowor, Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base, Open Acsess Journal of Information System (OAJIS), 2013.

[3] Shahram, K. and Siavash, A., Ciphertext-only attack on *d*×*d* Hill in *O*(*d*13*d*), *Information Processing Letters 118,* 2016, pp. 25–29. (online) http://www.elsevier.com/locate/ipl.

[4] Mahajan, S. and Singh, M., Performance Analysis of Efficient RSA Text Encryption Using NVIDIA CUDA-C and OpenCL. *Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing - ICONIAAC '14* ISBN: 978-1-4503-2908-8, 2014, pp.1-6.

[5] Meng, X. and Zheng, X., Cryptanalysis Of RSA With A Small Parameter Revisited. *Information Processing Letters* 115: 858–862, 2015.

[6] Chmielowiec, A., Fixed Points Of The RSA Encryption Algorithm. *Elsevier Theoretical Computer Science* 411, 2010, pp.288-292.

[7] Thao, J., RSA Visual: A Visualization Tool for the RSA Cipher, *Proceedings of the ACM National Science Foundation under grants DUE-1140512, DUE-1245310 and IIS-1319363.* Department of Computer Science Michigan Technological University Houghton, MI. USA. 2014.

[8] Iyer, S.C., Sedamkar, R.R., Gupta, S., A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach. *7th International Conference on Communication, Computing and Virtualization,* 2016, pp. 293-298.

[9] Konheim, A.G., *Computer Security and Cryptography.* Wiley-Interscience, A John Wiley and Sons Inc, 2007.

[10] Hoffstein,J., Pipher,J. and Silverman.J.H., *An Introduction Of Mathematical Cryptography*. Springer Science + Business Media .e-ISBN: 978-0-387-77994-2, 2008.

[11] Paar, J., Pelzl, J., Preenel, B. (Editors), *Understanding Cryptography.* Springer : New York, 2010.

[12] Tyagi, N. et al, Hybrid Key Cryptography: A Tool for Security. *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 6, Issue 3, 2017. ISSN: 2347-6710.

[13] Gupta,R.K. and Singh, P., A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network. *International Journal of Emerging Technology and Advanced Engineering* ISSN 2250-2459, 2013.

[14] Schneier, B., *Applied Cryptography 2nd edition, Protocols,Algorithms,and Source Code in C*. ISBN-13: 978-1-119-09672-6, Amazon,1996.

[15] Munir, R., *Kriptografi*. Informatika, Bandung. 2006.

[16] Dooley, J.F., *A Brief History of Cryptology and Cryptographic Algorithms*. *Springer Brief in Computer Science.* ISBN 978-3-319-01628-3, 2013.

[17] Palanisamy, V. & Jeneba, M. A., Hybrid Cryptography By The Implementation Of RSA And AES, *International Journal of Current Research* Vol. 33, Issue, 4, 2011, pp.241-244. ISSN: 0975-833X.

LAMPIRAN

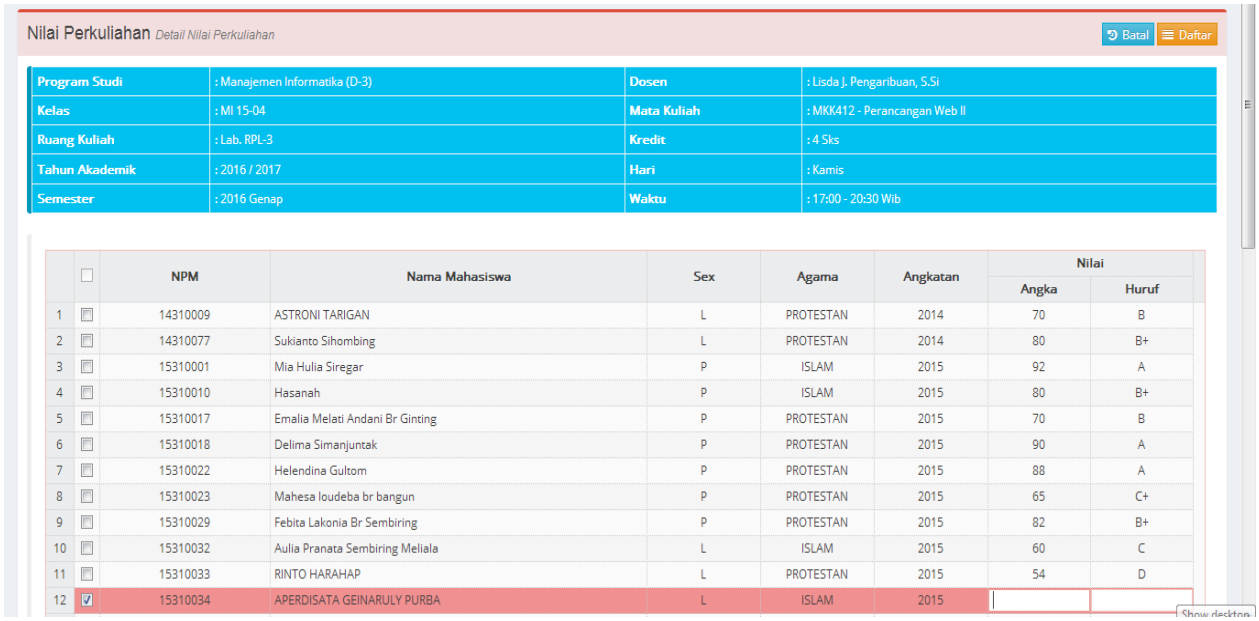
Lampiran 1. Daftar Nilai Mahasiswa

DAFTAR NILAI UJIAN AKHIR SEMESTER
JURUSAN MANAJEMEN INFORMATIKA
AMIK MBP MEDAN

Kelas	:MI	Dosen	: Lisda J Pangaribuan,M.Kom
Hari	: Jum'at	Matakuliah	: PERANCANGAN WEB I
Tanggal UAS	:	Bobot SKS	: 4 SKS
TAHUN AKADEMIK	: 2015/2016	Ruangan	: Lab. Ecomerce
SEMESTER	: 2015 Ganjil	Jam	: 17:00 - 20:30 WIB

No	NPM	NAMA MAHASISWA	Nilai						
			0,1	0,15	0,2	0,25	0,3	Akhir	
			Kh	Qs	Ts	UTS	UAS	Angka	Huruf
1	13310166	RIZKA NOVIDA	75	85	55	52	35	55	C
2	13310259	ARIADY BOY PUTRA SITUMEANG	93,75	75	70	55	55	65	C+
3	14310006	Arnas Julius Tarigan	87,5	65	60	50	30	52	D
4	14310008	Asrawati Pakpahan	93,75	95	95	83	75	86	A
5	14310013	Dame Yohana	100	75	85	50	70	72	B
6	14310023	Erika Febryani Br Sembiring	100	70	90	73	75	79	B+
7	14310027	Ester	100	95	90	100	60	85	A
8	14310029	Evelia Louise Girsang	87,5	100	90	100	80	91	A
9	14310032	Heri Aribowo	100	0	75	65	60	59	C
10	14310038	Jisman Samosir	100	70	90	70	65	76	B
11	14310039	Jojor Delima Br Hotang	100	95	90	100	60	85	A
12	14310041	Jonson Fernando Silaen	100	100	100	92	85	94	A
13	14310044	Lici Jayanti Sitorus	100	95	95	77	90	90	A
14	14310048	Martayessa Silitonga	100	95	95	100	65	88	A
15	14310051	Monica Putri Br Ginting	93,75	85	90	70	60	76	B
16	14310053	Murni Verawati Sinaga	100	90	90	75	55	77	B+
17	14310081	Wanri Siburian	100	80	70	77	60	73	B
18	14310098	Vonsius De Martin Sigiro	100	80	85	95	65	82	B+
19	14310100	Johannes C. Sinaga	100	70	80	65	45	66	C+
20	14310120	Leonardo Pinem	93,75	50	85	65	65	70	B
21	14310131	Siti Fatimah Tampubolon	100	70	75	57	70	71	B
22	14310134	Rendiyanta Surbakti	93,75	60	90	80	45	70	B

Lampiran 2. Tampilan Daftar Nilai Mahasiswa Pada Sistem



Lampiran 3. Hasil Percobaan enkripsi dan dekripsi untuk kunci RSA 12 bit

Kunci Hill	Determinan	Plainteks	Jumlah karakter	Teks yang dikirim (Enkripsi Hill)	ASCII ENKRIPSI	Waktu Enkripsi Hill	Kunci Yang dikirim: Kunci Pubic	Kunci private	enkripsi Rsa	Waktu enkripsi	Dekripsi kunci Hil (RSA)	Waktu Dekripsi (RSA)	Dekripsi	Waktu Dekripsi Hybrid
75 79 77 73 78 70 79 75 85	2724	LISDAMKK4121431 000886AXX	24	GCD (Det,256) ≠ 1										
24 18 13 237 60 36 229 147 0	295671	LISDAMKK4121431 000886AXX	24	y$çÛ 'òS(□□üÍPp□□À--	121 36 231 219 4 39 242 83 40 153 249 139 243 252 205 80 112	00:00:00.0528006	2263 ; 1837	2053 ;1837	1119 164 425 18 1546 36 1450 804 0	00:00:00.00180 27	24 18 13 237 60 36 229 147 0	00:00:00.0018 292	LISDAMKK4121 431000886AXX	00:00:00.0374674
48 33 35 37 39 90 167 24 4	198039	LISDAMKK4121431 000886AXX	24	I¸¨Í¨×ÅUík □xÀ □□½	2 73 184 168 205 168 215 140 197 85 237 107 6 131 120 192 32 144 26 156 160 144 189 7	00:00:00.0285942	3233 ; 1607	2423 ; 1607	2942 1258 1824 541 1651 223 2245 69 1509	00:00:00.00221 82	48 33 35 37 39 90 167 24 4	00:00:00.0025 365	LISDAMKK4121 431000886AXX	00:00:00.0407051
91 93 92 91 77 95 83 92 95	73	LISDAMKK4121431 000886AXX	24	ú□«"!Ü¢n□ □q.®õCå- Öæái9	11 250 153 99 171 34 33 220 162 110 127 106 18 149 28 158 42 113 46 174 245 67 229 45 16 214 230 225 105 57	00:00:00.0300074	3763 ; 2313	1377 ; 2313	2604 1276 1238 2604 784 2038 1302 1238 2038	00:00:00.00238 40	91 93 92 91 77 95 83 92 95	00:00:00.0021 659	LISDAMKK4121 431000886AXX	00:00:00.0409319
77 253 224 191 214 85 9 87 91	17019	LISDAMKK4121431 000886AXX	24	¡Iü £Ú.ë□ "ë³åà p□Gy	161 73 252 17 163 218 46 235 156 7 160 34 235 179 148 224 224 16 112 134 50 133 71 121	00:00:00.0307677	3599 ; 1187	2363 ; 1187	3306 2704 2040 3501 1116 2631 2765 1836 958	00:00:00.00134 72	77 253 224 191 214 85 9 87 91	00:00:00.0025 340	LISDAMKK4121 431000886AXX	00:00:00.0391770
0 166 89 110 79 71 73 217 207	141	LISDAMKK4121431 000886AXX	24	14ªë¢À¶Ë u ú ¬®ÐÀ0 R ¨~I	49 52 170 235 162 192 182 203 2 117 19 250 27 172 174 208 192 48 22 82 26 168 126 73	00:00:00.0546201	3713 ; 1169	1949;1169	0 1716 895 544 637 1931 693 1953 827	00:00:00.00213 22	0 166 89 110 79 71 73 217 207	00:00:00.0019 465	LISDAMKK4121 431000886AXX	00:00:00.0451993
0 125 66 193 122 95 9 37 0	505713	LISDAMKK4121431 000886AXX	24	ã9ÑÉ □z ôó□3Ðà Dò ¨□	11 227 57 151 209 201 7 149 122 12 244 243 137 177 51 208 224 160 68 242 16 168 153 1	00:00:00.0365427	5293;2869	445 ;2869	0 3249 1588 3606 948 3071 724 391 3605	00:00:00.00195 33	0 125 66 193 122 95 9 37 0	00:00:00.0012 308	LISDAMKK4121 431000886AXX	00:00:00.0470215
24 18 13 237 60 36 229 147 0	295671	FAUZIHARISMKK11 31431010680B+XX	30	sþñ:□□®; ov÷Ï:Þ ÂªsÂ¶5 eú`¨ºÏÿ	115 254 241 58 142 109 145 169 59	00:00:00.0023322	5767;3747	3131 ; 3747	4085 5252 5649 3792 3914 5962 5745 3140 0	00:00:00.00119 27	24 18 13 237 60 36 229 147 0	00:00:00.0012 083	FAUZIHARISMK K11314310106 80B+XX	00:00:00.0364966
48 33 35 37 39 90 167 24 4	198039	FAUZIHARISMKK11 31431010680B+XX	30	ç !q®½□¼ □ˆÌý-q¶□a0¶	32 231 22 33 113 174 189 141 59 190 24 137 20 136 73 253 30 173 113 182 157 194 97 79 182 156 16 112 143 173	00:00:00.0367459	5183 ; 3293	2357 ; 3293	2885 4200 3967 1024 2661 1321 3839 4310 2975	00:00:00.00285 96	48 33 35 37 39 90 167 24 4	00:00:00.0016 771	FAUZIHARISMK K11314310106 80B+XX	00:00:00.0467705
91 93 92 91 77 95 83 92 95	73	FAUZIHARISMKK11 31431010680B+XX	30	ú□«"!Ü¢n□ □q.®õCå- Öæái9	11 250 153 99 171 34 33 220 162 110 127 106 18 149 28 158 42 113 46 174 245 67 229 45 16 214 230 225 105 57	00:00:00.0367019	1343 ; 973	1189 ; 973	333 264 431 333 59 657 716 431 657	00:00:00.00201 15	91 93 92 91 77 95 83 92 95	00:00:00.0019 704	FAUZIHARISMK K11314310106 80B+XX	00:00:00.0470506
77 253 224 191 214 85 9 87 91	17019	FAUZIHARISMKK11 31431010680B+XX	30	«ÉÄ7 □H °2¿Ü0µDGîÄó□ m□Ò¾çÝ³	171 201 196 55 20 145 119 72 26 176 50 191 220 48 181 68 71 238 196 143 130 109 157 59 8 210 190 231 221 179	00:00:00.0384389	3599 ; 2173	1957 ; 2173	2008 1583 3102 3453 2945 389 1644 2308 2728	00:00:00.00265 48	77 253 224 191 214 85 9 87 91	00:00:00.0013 775	FAUZIHARISMK K11314310106 80B+XX	00:00:00.0483992
0 166 89 110 79 71 73 217 207	141	FAUZIHARISMKK11 31431010680B+XX	30	³¶Ê^+Ã□ :□□ú vYäæØS . ¨	179 182 202 94 43 195 141 123 18 1 58 149 207 240 139 218 117 32 118 89 228 230 216 83 18 46 6 168 10 3	00:00:00.0399833	2449;1067	443 ;1067	0 561 1906 1819 1106 1414 2390 2139 799	00:00:00.047043	0 166 89 110 79 71 73 217 207	00:00:00.0013 726	FAUZIHARISMK K11314310106 80B+XX	00:00:00.0533938
0 125 66 193 122 95 9 37 0	505713	FAUZIHARISMKK11 31431010680B+XX	30	§KÛ5\·Ü,#ï □,U àM□\Û ©tè¨ ;	167 75 219 53 92 183 220 44 35 239 26 12 143 20 184 85 25 224 77 157 224 92 219 169 116 150 232 168 3 59	00:00:00.0460690	4453 ; 4151	391 ; 4151	0 796 4213 750 1098 156 2693 2464 0	00:00:00.003263	0 125 66 193 122 95 9 37 0	00:00:00.0031 856	FAUZIHARISMK K11314310106 80B+XX	00:00:00.0505819

Lampiran 4. Hasil Percobaan enkripsi dan dekripsi untuk kunci RSA 16 bit

Kunci Hill	Determinan	Plainteks	Jumlah karakter	Teks yang dikirim (Enkripsi Hill)	ASCII ENKRIPSI	Waktu Enkripsi Hill	Kunci Yang dikirim				Dekripsi kunci Hil (RSA)	Waktu Dekripsi (RSA)	Dekripsi Hybrid	Waktu Dekripsi Hybrid
							Kunci Pubic	Kunci private	enkripsi Rsa	Waktu enkripsi				
75 79 77 73 78 70 79 75 85	2724	LISDAMKK41 21431000886A XX	24	GCD (Det,256) ≠ 1										
24 18 13 237 60 36 229 147 0	295671	LISDAMKK41 21431000886A XX	24	y$çÛ 'òS(ÐßúÍPpÐÀ--	121 36 231 219 4 39 242 83 40 153 249 139 243 252 205 80 112	00:00:00.0640007	20003 ; 19289	19529 ; 19289	12281 1155 14847 11508 486 12445 3931 2069 0	00:00:00.0548293	24 18 13 237 60 36 229 147 0	00:00:00.0073646	LISDAMKK41 21431000886 AXX	00:00:00.0428061
48 33 35 37 39 90 167 24 4	198039	LISDAMKK41 21431000886A XX	24	Ì¸Í×åÛîk ßÀ ÐÐ	2 73 184 168 205 168 215 140 197 85 237 107 6 131 120 192 32 144 26 156 160 144 189 7	00:00:00.0285942	15397 ; 8859	3699 ; 8859	9294 9375 12145 902 2556 90 10547 1927 523	00:00:00.0041408	48 33 35 37 39 90 167 24 4	00:00:00.0414393	LISDAMKK41 21431000886 AXX	00:00:00.0419130
91 93 92 91 77 95 83 92 95	73	LISDAMKK41 21431000886A XX	24	úÐ"!Ûœnß Ðq.®õCâ- Öæái9	11 250 153 99 171 34 33 220 162 110 127 106 18 149 28 158 42 113 46 174 245 67 229 45 16 214 230 225 105 57	00:00:00.0297353	25787 ; 5477	6893 ; 5477	7799 15047 568 7799 24594 21035 3267 568 21035	00:00:00.0029104	91 93 92 91 77 95 83 92 95	00:00:00.0035860	LISDAMKK41 21431000886 AXX	00:00:00.0337378
77 253 224 191 214 85 9 87 91	17019	LISDAMKK41 21431000886A XX	24	¡Iü £Ú.ê "ë³àà pÐGy	161 73 252 17 163 218 46 235 156 7 160 34 235 179 148 224 224 16 112 134 50 133 71 121	00:00:00.0371360	7663 ; 3473	6065 ; 3473	2445 572 2201 5152 1920 2413 6717 3066 2700	00:00:00.0016698	77 253 224 191 214 85 9 87 91	00:00:00.0039365	LISDAMKK41 21431000886 AXX	00:00:00.0341273
0 125 66 193 122 95 9 37 0	505713	LISDAMKK41 21431000886A XX	24	ä9ÑÉ ß ôóëÐà Dò ¨	11 227 57 151 209 201 7 149 122 12 244 243 137 177 51 208 224 160 68 242 16 168 153 1	00:00:00.0365427	18281 ; 6617	6953 ; 6617	0 3136 14976 13250 13352 12964 4425 5147 0	00:00:00.0178931	0 125 66 193 122 95 9 37 0	00:00:00.0033093	LISDAMKK41 21431000886 AXX	00:00:00.0405376
24 18 13 237 60 36 229 147 0	295671	FAUZIHARISM KK113143101 0680B+XX	30	sþñ·ÐØ; ov÷Ï·Þ Å°sÅ¶5eú¨°îÿ	115 254 241 58 142 109 145 169 59	00:00:00.0023322	15023 ; 2507	4763 ; 2507	955 6239 3044 14964 3907 13546 11897 2975 0	00:00:00.0019484	24 18 13 237 60 36 229 147 0	00:00:00.0027643	FAUZIHARISM KK113143101 0680B+XX	00:00:00.5124619
48 33 35 37 39 90 167 24 4	198039	FAUZIHARISM KK113143101 0680B+XX	30	ç !q®½¾ Ð'Íý·q¶Åa0¶Ðp	32 231 22 33 113 174 189 141 59 190 24 137 20 136 73 253 30 173 113 182 157 194 97 79 182 156 16 112 143 173	00:00:00.0365985	51529 ; 43773	7945 ; 43773	8588 9065 14712 14455 17685 19782 33416 48024 12908	00:00:00.0152005	48 33 35 37 39 90 167 24 4	00:00:00.0325422	FAUZIHARISM KK113143101 0680B+XX	
91 93 92 91 77 95 83 92 95	73	FAUZIHARISM KK113143101 0680B+XX	30	úÐ"!Ûœnß Ðq.®õCâ- Öæái9	11 250 153 99 171 34 33 220 162 110 127 106 18 149 28 158 42 113 46 174 245 67 229 45 16 214 230 225 105 57	00:00:00.0297881	54253 ; 47381	38769 ; 47381	27620 5695 10932 27620 6913 2375 31973 10932 2375	00:00:00.0163820	91 93 92 91 77 95 83 92 95	00:00:00.0137947	FAUZIHARISM KK113143101 0680B+XX	00:00:00.0364552
77 253 224 191 214 85 9 87 91	17019	FAUZIHARISM KK113143101 0680B+XX	30	«ÉÂ7 ØH °2¿Ü0µDGiÅóÐØÒ¾ ¿Ý²	171 201 196 55 20 145 119 72 26 176 50 191 220 48 181 68 71 238 196 143 130 109 157 59 8 210 190 231 221 179	00:00:00.0384389	6169 ; 2801	2021 ; 2801	511 2288 5290 211 1878 1728 5687 5647 4555	00:00:00.0026978	77 253 224 191 214 85 9 87 91	00:00:00.0024182	FAUZIHARISM KK113143101 0680B+XX	00:00:00.0399277
0 125 66 193 122 95 9 37 0	505713	FAUZIHARISM KK113143101 0680B+XX	30	ŠKÛ5\·Ü,#ï Ð¸U àMÐÛ©tè˜ ;	167 75 219 53 92 183 220 44 35 239 26 12 143 20 184 85 25 224 77 157 224 92 219 169 116 150 232 168 3 59	00:00:00.0370175	11327 ; 7187	9083 ; 7187	0 1210 7643 2457 2227 8132 7348 7780 0	00:00:00.0023654	0 125 66 193 122 95 9 37 0	00:00:00.0016204	FAUZIHARISM KK113143101 0680B+XX	00:00:00.0430634

Lampiran 5. Hasil Percobaan enkripsi dan dekripsi untuk kunci RSA 32 bit

Kunci Hill	Determinan	Plainteks	Jumlah karakter	Teks yang dikirim		Waktu Enkripsi Hill	Kunci Yang dikirim					Waktu Dekripsi (RSA)	Dekripsi	Waktu Dekripsi Hybrid
				(Enkripsi Hill)	ASCII ENKRIPSI		Kunci Pubic	Kunci private	enkripsi Rsa	Waktu enkripsi	Dekripsi kunci Hil			
75 79 77 73 78 70 79 75 85	2724	LISDAMKK41 21431000886 AXX	24	GCD (Det,256) ≠ 1										
24 18 13 237 60 36 229 147 0	295671	LISDAMKK41 21431000886 AXX	24	y$çÛ 'òS(▯▯üÍPp▯▯À--	121 36 231 219 4 39 242 83 40 153 249 139 243 252 205 80 112	00:00:00.0 672828	394920133 ; 391349243	264231087 ; 391349243	269197131 310657928 205780391 28789525 246271100 275299892 141304570 314983085 0	00:01:45.77 63870	24 18 13 237 60 36 229 147 0	00:01:35. 1531395	LISDAMKK4 1214310008 86AXX	00:00:00.1458 331
48 33 35 37 39 90 167 24 4	198039	LISDAMKK41 21431000886 AXX	24	I¸¨Í¨×ÅUík ▯xÀ ▯▯½	2 73 184 168 205 168 215 140 197 85 237 107 6 131 120 192 32 144 26 156 160 144 189 7	00:00:00.0 285942	1819724899 ; 1375800895	583543567 ; 1375800895	307775538 1725945820 538682066 599510520 909790610 741198884 1627768971 998042269 612289839	00:06:36.07 01410	48 33 35 37 39 90 167 24 4	00:02:57. 4921491	LISDAMKK4 1214310008 86AXX	00:00:00.0912 424
91 93 92 91 77 95 83 92 95	73	LISDAMKK41 21431000886 AXX	24	ú▯«"!Ü¢n▯ ▯q.®õCå- Ö	11 250 153 99 171 34 33 220 162 110 127 106 18 149 28 158 42 113 46 174 245 67 229 45 16 214 230 225 105 57	00:00:00.0 300074	316611833 ;24703013	145487477 ; 24703013	265282877 149722290 264407139 265282877 39412827 307841592 225254090 264407139 307841592	00:00:07.19 31433	91 93 92 91 77 95 83 92 95	00:00:43. 6713803	LISDAMKK4 1214310008 86AXX	00:00:00.1009 858
77 253 224 191 214 85 9 87 91	17019	LISDAMKK41 21431000886 AXX	24	¡Iü £Ú.ë▯ "ë³åà p▯Gy	161 73 252 17 163 218 46 235 156 7 160 34 235 179 148 224 224 16 112 134 50 133 71 121	00:00:00.0 336164	886721167 ; 562138487	110103911 ; 562138487	149116999 860555786 30494408 56489980 865947890 767080040 92703869 753007448 244683092	00:03:24.93 68228	77 253 224 191 214 85 9 87 91	00:00:42. 3765393	LISDAMKK4 1214310008 86AXX	00:00:00.1313 481
0 166 89 110 79 71 73 217 207	141	LISDAMKK41 21431000886 AXX	24	14ªë¢À¶Ë u ú ¬®ÐÀ 0 R ¨~I	49 52 170 235 162 192 182 203 2 117 19 250 27 172 174 208 192 48 22 82 26 168 126 73	00:00:00.0 802481	1348081457 ; 176555507	642028643 ; 176555507	0 1232120955 1173680545 963356787 305449982 492832743 174000796 1245045005 487873317	00:00:48.546	0 166 89 110 79 71 73 217 207	00:03:02. 8481868	LISDAMKK4 1214310008 86AXX	00:00:00.0967 295
0 125 66 193 122 95 9 37 0	505713	LISDAMKK41 21431000886 AXX	24	ã9ÑÉ ▯z ôó▯3Ðà Dò ¨▯	11 227 57 151 209 201 7 149 122 12 244 243 137 177 51 208 224 160 68 242 16 168 153 1	00:00:00.0 303735	2053980853; 193538023	1521968087 ; 193538023	0 1758651304 622103580 1402977577 546540074 1237140351 115335966 1789674879 0	00:00:13.25 90750	0 125 66 193 122 95 9 37 0	00:00:00. 2453017	LISDAMKK4 1214310008 86AXX	00:00:00.0266 789
24 18 13 237 60 36 229 147 0	295671	FAUZIHARIS MKK1131431 010680B+XX	30	sþñ:▯▯; ov÷Ï:Þ ÂªsÂ ¶5eú`¨°Ïÿ	115 254 241 58 142 109 145 169 59	00:00:00.0 299810	132691547 ; 71071613	4991957 ; 71071613	46313165 18305436 120048064 75421923 9548843 26215525 54382380 119052557 0	00:00:17.30 78228	24 18 13 237 60 36 229 147 0	00:00:01. 4325389	FAUZIHARIS MKK113143 1010680B+ XX	00:00:00.0972 242
0 166 89 110 79 71 73 217 207	141	FAUZIHARIS MKK1131431 010680B+XX	30	³¶Ê^+Ã▯ :▯▯u vYäæØS . ¨	179 182 202 94 43 195 141 123 18 1 58 149 207 240 139 218 117 32 118 89 228 230 216 83 18 46 6 168 10 3	00:00:00.0 350732	363714493 ; 278474489	31388489 ; 278474489	0 315899543 217504765 168138687 228241358 303170169 737987 115346707 291041879	00:01:16.03 54984	0 166 89 110 79 71 73 217 207	00:00:08. 9241587	FAUZIHARIS MKK113143 1010680B+ XX	00:00:00.0981 589
0 125 66 193 122 95 9 37 0	505713	FAUZIHARIS MKK1131431 010680B+XX	30	§KÛ5\·Ü,#ï ▯¸U àM▯ \Û©tè¨ ;	167 75 219 53 92 183 220 44 35 239 26 12 143 20 184 85 25 224 77 157 224 92 219 169 116 150 232 168 3 59	00:00:00.0 562943	271057613 ; 45897803	73346531 ; 45897803	0 101992762 19587297 200119013 13318324 107539348 92746545 80615903 0	00:00:11.43 81121	0 125 66 193 122 95 9 37 0	00:00:19. 8353477	FAUZIHARIS MKK113143 1010680B+ XX	00:00:00.0969 813
48 33 35 37 39 90 167 24 4	198039	FAUZIHARIS MKK1131431 010680B+XX	30	ç !q®½▯¾ ▯ˆIý-q¶▯a	32 231 22 33 113 174 189 141 59 190 24 137 20 136 73 253 30 173 113 182 157 194 97 79 182 156 16 112 143 173	00:00:00.0 367459	326658263 ; 59898889	256182649 ; 59898889	228051145 116442324 40968019 287240651 210072992 114332924 151604730 28735356 166444334	00:00:16.49 88304	48 33 35 37 39 90 167 24 4	00:01:17. 0298392	FAUZIHARIS MKK113143 1010680B+ XX	00:00:00.4704 659
91 93 92 91 77 95 83 92 95	73	FAUZIHARIS MKK1131431 010680B+XX	30	ú▯«"!Ü¢n▯ ▯q.®õCå- Öæái9	11 250 153 99 171 34 33 220 162 110 127 106 18 149 28 158 42 113 46 174 245 67 229 45 16 214 230 225 105 57	00:00:00.0 368227	142286087 ; 139971857	36795377 ; 139971857	77737061 3529835 115854131 77737061 40370538 131021734 120529482 115854131 131021734	00:00:39.71 34408	91 93 92 91 77 95 83 92 95	00:00:11. 0667534	FAUZIHARIS MKK113143 1010680B+ XX	00:00:00.1078 715
77 253 224 191 214 85 9 87 91	17019	FAUZIHARIS MKK1131431 010680B+XX	30	«ÉÄ7 ▯H °2¿Ü0µDGî Äó▯▯Ò¾çÝ³	145 119 72 26 176 50 191 220 48 181 68 71 238 196 143 130 109 157 59 8 210 190 231 221 179	00:00:00.0 384389	453026051 ; 419877635	137451899 ; 419877635	203639061 236411508 72072254 309408900 332249961 205335988 307496611 201572884 84635430	00:01:59.59 69341	77 253 224 191 214 85 9 87 91	00:00:41. 5772650	FAUZIHARIS MKK113143 1010680B+ XX	00:00:00.1264 143