Penggabungan modifikasi *hill cipher* dan *elliptic curve cryptography* untuk meningkatkan keamanan pesan

Hana Nur Azizah*, Rini Marwati dan Isnie Yusnitha

Departemen Pendidikan Matematika
Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam
Universitas Pendidikan Indonesia
*Surel: hananurazizah1601@gmail.com

ABSTRAK. Seiring perkembangan teknologi, pesan rahasia semakin rentan untuk diretas. Oleh karena itu, pengamanan terhadap pesan rahasia perlu ditingkatkan. Kriptografi mempelajari teknik atau algoritma untuk mengamankan pesan, diantaranya adalah *hill cipher* dan *elliptic curve cryptography* (ECC). *Hill cipher* merupakan suatu kriptosistem yang menggunakan matriks sebagai kuncinya, dengan kunci matriks yang umum digunakan merupakan suatu matriks berukuran$n \times n$. *Elliptic curve cryptography* menggunakan titik-titik pada kurva eliptik yang merupakan suatu lapangan atas bilangan prima dengan operasi penjumlahan titik. Dalam penelitian ini disajikan pengembangan kriptosistem *hill cipher* dan *elliptic curve cryptography* dengan cara menggabungkan kedua kriptosistem tersebut. Dalam penggabungan tersebut, dilakukan suatu modifikasi sehingga *hill cipher* yang digunakan dapat memiliki suatu kunci matriks yang berukuran $m \times n$. Kriptografi gabungan *hill* cipher dan *elliptic curve cryptography* ini menggunakan 95 karakter dari bilangan ASCII. Selain itu, hasil penelitian diimplementasikan menjadi suatu program komputer. Penggabungan kedua kriptosistem ini bertujuan untuk meningkatkan keamanan suatu pesan yang bersifat rahasia sehingga pesan tersebut lebih sulit untuk diretas.

Kata Kunci: *Hill Cipher*, Modifikasi *Hill Cipher*, *Elliptic Curve Cryptography*

TITLE. *Combination of modification hill cipher and elliptic curve cryptography to improve safety message*

ABSTRACT. *As technology develops, secret messages are increasingly vulnerable to be hacked. Therefore, the security level of the messages needs to be improved. The studies of Cryptography shows several techniques or algorithms to secure the messages, including hill cipher*

and elliptic curve cryptography (ECC). Hill cipher is a cryptosystem that uses matrices as the keys, which usually uses matrices. Elliptic curve cryptography uses points on the elliptic curve, which are a field over prime numbers with addition operation. This research develops a cryptosystem by combining both hill cipher and elliptic curve cryptography. The study modified the hill cipher such that it can use matrices as the keys. Moreover, the developed cryptosystem uses 95 characters from ASCII numbers. Finally, the development of hill cipher and elliptic curve cryptography is implemented into a computer program. Hence, the combined cryptosystem is expected to be able to strengthen the security of the message, therefore it is difficult to be hacked.

Keywords: *Hill Cipher, Modified Hill Cipher, Elliptic Curve Cryptography*

1. PENDAHULUAN

Kriptografi adalah seni untuk mengamankan sebuah pesan yang bersifat rahasia dengan cara menyamarkannya agar tidak dapat dimengerti oleh siapapun kecuali pihak yang berhak mengetahuinya. Namun, seiring perkembangan teknologi dan informasi dari masa ke masa seringkali pesan rahasia tersebut diretas oleh pihak yang tidak berhak mengetahui pesan tersebut sehingga pengirim pesan harus meningkatkan keamanan pesan dengan mengembangkan kriptografi, diantaranya adalah memperbanyak jumlah kemungkinan kunci kriptografi atau menggabungkan dua buah kriptosistem.

Hill cipher sangat sulit untuk diretas dengan metode *ciphertext-only attack* karena sifat linearitasnya, yaitu setiap karakter memiliki keterikatan satu sama lain. Tetapi dengan metode *known plaintext attack*, seorang kriptanalis dapat mengkriptanalisis *ciphertext* ketika memiliki sebagian *plaintext*nya, sehingga *hill cipher* menjadi tidak begitu aman akibatnya peningkatan keamanan harus dilakukan. Salah satu cara untuk meningkatkan keamanan pesan adalah menggabungkan *hill cipher* dengan *elliptic curve cryptography* [1]. *Elliptic curve cryptography* dipilih karena hanya membutuhkan kunci dengan jumlah bit yang jauh lebih sedikit dibandingkan dengan kriptografi asimetri lain dan sulit untuk diretas karena perkalian skalarnya sulit untuk diimplementasikan.

Hidayat dan Alawiyah [2] mengemukakan bahwa *hill cipher* dapat menggunakan matriks persegi panjang $m \times n$, dengan $m > n$ dan $n > 1$ sebagai kuncinya dengan memanfaatkan matriks *pseudo-inverse*. Dasar teori matriks yang digunakan dalam kriptosistem *hill cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Dengan memanfaatkan teori *pseudo-inverse* [3], penggunaan kunci matriks tidak hanya matriks persegi saja, tapi juga dapat menggunakan kunci matriks persegi panjang $m \times n$, dengan $m \geq n$ dan $n > 1$.

Elliptic curve cryptography [4] menggunakan kurva eliptik pada lapangan $\mathbb{Z}_{\boldsymbol{p}}$. Bentuk umum kurva eliptik tersebut adalah

$$y^2 \equiv x^3 + ax + b \; mod \; p$$

di mana $p > 3$ bilangan prima, $a, b \in \mathbb{Z}_p$ dan memenuhi $4a^3 + 27b^2 \not\equiv 0 \; (mod \; p)$, dengan sebuah titik khusus $\mathcal{O}$ yang dinamakan titik *infinity* (titik di tak hingga).

Lebih lanjut, himpunan titik-titik pada kurva eliptik yang memenuhi sifat-sifat diata akan membentuk suatu grup dengan operasi penjumlahan yang akan dijelaskan lebih terperinci pada bagian hasil dan pembahasan.

Kumar, Suneetha & ChandrasekhAR [5] memodifikasi *elliptic curve cryptography* sehingga menghasilkan *ciphertext* berupa teks sehingga sulit untuk mengetahui bahwa kriptosistem yang digunakan adalah *elliptic curve cryptography*.

Dalam penelitian ini, dikembangkan sebuah kriptosistem melalui penggabungan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* menggunakan 95 karakter yang terdapat pada tabel ASCII [6] dimulai dari karakter ke-32 sampai ke-126. Kemudian dari kriptosistem ini dikonstruksi suatu program aplikasi komputer menggunakan *MATLAB.*

2. METODOLOGI

Pada penelitian ini, tahapan-tahapan yang perlu dilakukan adalah sebagai berikut:

1. Studi literatur mengenai peningkatan keamanan kriptosistem, *hill cipher* dan *elliptic curve cryptography*.
2. Model dasar yang digunakan adalah kriptosistem *hill cipher* yang telah dimodifikasi sehingga dapat memiliki kunci matriks persegi panjang dan *elliptic curve cryptography*.
3. Merancang sebuah kriptosistem gabungan antara kriptosistem *hill cipher* dan *elliptic curve cryptography* dengan kunci kriptosistem *hill cipher* adalah sebuah matriks persegi panjang. *Plaintext* dan *ciphertext* yang digunakan berupa karakter alfanumerik yang terdapat pada tabel ASCII dimulai dari karakter ke-32 sampai ke-126.
4. Setelah kriptosistem gabungan terbentuk, dilakukan validasi untuk mengetahui apakah *ciphertext* hasil proses enkripsi penggabungan kriptosistem *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* dapat mengembalikan *plaintext* saat melalui proses dekripsi atau tidak.

3. HASIL DAN PEMBAHASAN

Pada kriptosistem *hill cipher* [2], matriks kunci $K \in \mathbb{Z}_p^{m \times n}$ yang dapat digunakan adalah matriks yang memenuhi

a. $rank(K) = n$. (matriks *K full column rank*)
b. Definisikan $T = K^T$, hitung TK. Nilai $\det(TK)$ harus memiliki invers modulo terhadap p. $(gcd(\det(TK), p) = 1)$.
c. Hitung matriks $M = (TK)^{-1} \cdot T$, dengan
$$(TK)^{-1} = \det^{-1}(TK) \cdot adj(TK)$$
d. M memenuhi

- $KMK = K$
- $MKM = M$
- $(KM)^* = KM$
- $(MK)^* = MK$

Untuk proses enkripsi dihitung menggunakan rumus

$$e_k(x) = Kx$$

untuk melakukan dekripsi dilakukan dengan menggunakan rumus

$$d_k(y) = My$$

Ketika akan melakukan proses enkripsi, panjang *plaintext* harus dihitung sehingga panjang *plaintext mod* kolom matriks $\equiv 0$. Jika tidak, tambahkan spasi sehingga memenuhi syarat tersebut. Mempartisi *plaintext* pada proses enkripsi disesuaikan dengan jumlah kolom matriks K, sedangkan untuk mempartisi *ciphertext* pada proses dekripsi disesuaikan dengan jumlah kolom matriks M.

Elliptic curve cryptography [4] menggunakan kurva eliptik pada lapangan $\mathbb{Z}_p$. Bentuk umum kurva eliptik tersebut adalah

$$y^2 \equiv x^3 + ax + b \; mod \; p$$

di mana $p > 3$ bilangan prima, $a, b \in \mathbb{Z}_p$ dan memenuhi $4a^3 + 27b^2 \not\equiv 0 \; (mod \; p)$, dengan sebuah titik khusus $\mathcal{O}$ yang dinamakan titik *infinity* (titik di tak hingga). Untuk menjumlahkan titik pada kurva eliptik pada lapangan $\mathbb{Z}_p$, misalkan:

1. $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$, $P, Q \in E$ dan
   $$P + Q = (x_3, y_3)$$
   untuk mencari titik koordinatnya, gunakan rumus:
   $$x_3 = (\lambda^2 - x_1 - x_2) \; mod \; p$$
   $$y_3 = (\lambda(x_1 - x_3) - y_1) \; mod \; p$$
   dengan gradien
   $$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & jika \; P \neq Q \\ (3{x_1}^2 + a)(2y_1)^{-1}, & jika \; P = Q \end{cases}$$
2. Misal $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$, $P, Q \in E$
   jika $x_1 = x_2$ dan $y_1 = -y_2$ maka
   $$P + Q = \mathcal{O}$$
3. Misal $P = (x_1, y_1)$ maka
   $$P + \mathcal{O} = \mathcal{O} + P = P$$

Sedangkan untuk perkalian titik dengan suatu skalar $k \in \mathbb{N}$, pengoperasiannya sama dengan menjumlahkan titik tersebut sebanyak $k - 1$ kali terhadap dirinya sendiri.

Pada kriptosistem *elliptic curve cryptography*, misalkan telah disepakati $E(\mathbb{Z}_p)$ dan generator G. Misalkan kunci privat Alice dan Bob adalah α dan β. Kunci Publik Alice dan Bob adalah

$$A_1 = \alpha G \qquad B_1 = \beta G$$

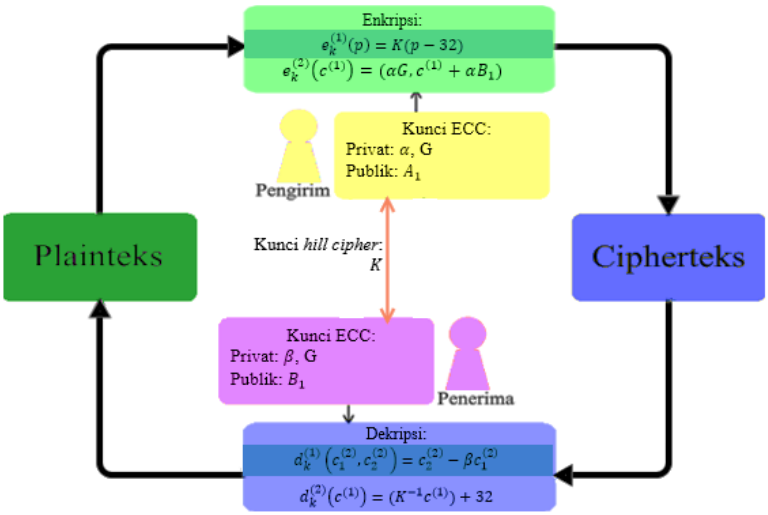
Proses enkripsinya adalah

$$e_K(P_m, \alpha) = (\alpha G\,, P_m + \alpha B_1)$$

di mana $P_m \in E$ adalah *plaintext* yang dikirimkan oleh Alice. Proses dekripsinya adalah

$$d_K(\alpha G\,, P_m + \alpha B_1) = (P_m + \alpha B_1) - (\beta \alpha G)$$

Berikut skema algoritma penggabungan modifikasi *hill cipher* dan *elliptic curve cryptography*



Gambar 1. Skema alur modifikasi kriptografi *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography*

Skema pada Gambar 1 dapat diwujudkan dalam langkah-langkah sebagai berikut: 1. Pembangkitan kunci; 2. Proses Enkripsi; 3. Proses Dekripsi.

Dalam proses pembangkitan kunci, pengirim dan penerima melakukan pembangkitan kunci publik dan kunci privat yang kemudian akan saling menukar kunci publik. Berikut langkah-langkah pembangkitan kunci publik dan kunci privat.

1. Menyepakati suatu kunci privat $K \in \mathbb{Z}_p^{m \times n}$.

2. Menyepakati sebuah kurva eliptik atas $\mathbb{Z}_p$ kemudian mencari E dengan elemen $E = 95$. Pilih sebuah titik $G \in E$ dan bentuk suatu tabel konversi untuk mengonversi karakter ke dalam titik-titik pada kurva eliptik.
3. Pengirim dan penerima membangkitkan nilai-nilai $\alpha, \beta, G, A_1, B_1$.

Diperoleh kunci publik adalah 2-*tuple* (A_1, B_1) dan kunci privat 4-*tuple* (K, G, α, β).

Setelah menerima kunci publik, pengirim kemudian melakukan enkripsi terhadap *plaintext*. Langkah-langkah enkripsi adalah sebagai berikut.

1. Menentukan sebuah *plaintext* berupa karakter alfanumerik.
2. Menghitung jumlah karakter pada *plaintext* tersebut. Apabila jumlah karakter $\not\equiv 0 \; mod \; n$ maka tambahkan suatu karakter sehingga jumlah karakter $\equiv 0 \; mod \; n$. Kemudian konversikan setiap karakter *plaintext* menjadi desimal ASCII.
3. Partisi *plaintext* $p_1, \dots, p_k$ dengan setiap partisi berelemen sejumlah kolom kuncinya. Seluruh elemen dikurangi dengan 32 sehingga diperoleh partisi
$$(p_1 - 32), \dots, (p_k - 32)$$
4. Menghitung
$$c_i^{(1)} = K(p_i - 32)$$
dengan hasil setiap perhitungan dibulatkan ke dalam modulo 95.
5. Hasil perhitungan tersebut dikonversi ke dalam titik-titik pada kurva eliptik sesuai dengan tabel konversi yang telah dibuat.
$$c_i^{(1)} = (x, y) \in E$$
6. Kemudian dihitung
$$\left(c_1^{(2)}, c_2^{(2)}\right) = (\alpha G, c^{(1)} + \alpha B_1)$$
7. Seluruh $\left(c_1^{(2)}, c_2^{(2)}\right)$ yang diperoleh dikonversi kembali menjadi bilangan sesuai dengan tabel konversi yang telah dibuat kemudian ditambah dengan 32. Hasil perhitungan tersebut dikonversi ke dalam karakter ASCII.
8. Diperoleh *ciphertext* berupa karakter alfanumerik.

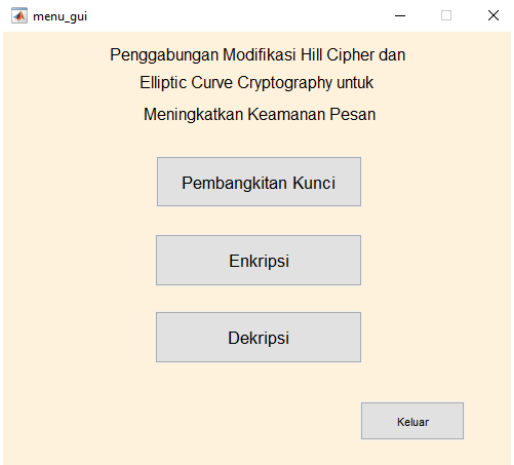
Setelah menerima *ciphertext*, penerima kemudian melakukan dekripsi untuk mengembalikan *plaintext*. Langkah-langkah dekripsi adalah sebagai berikut

1. Konversi setiap karakter *ciphertext* ke dalam desimal ASCII kemudian dikurangi dengan 32. Hasil perhitungan tersebut dikonversi ke dalam titik-titik pada kurva eliptik sesuai dengan tabel konversi yang telah dibuat.

$$c_i^{(2)} = (x, y) \in E$$

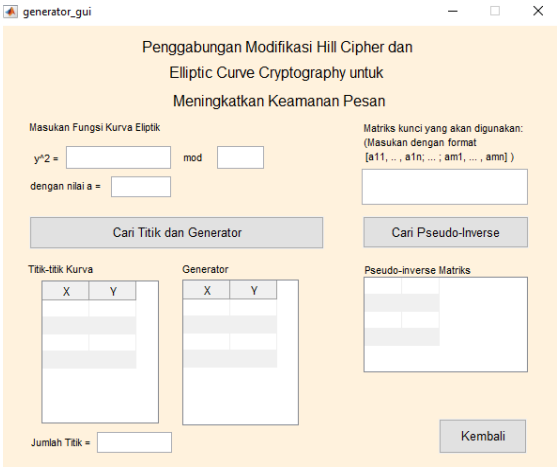
2. Menghitung
$$c_i^{(1)} = c_2^{(2)} - \beta c_1^{(2)}$$
kemudian hasil perhitungan dikonversi ke dalam bilangan pada tabel konversi yang dimiliki.
3. Partisi *ciphertext* $c^{(1)}$ menjadi $c_1^{(1)}, \dots, c_k^{(1)}$ dengan setiap partisi berelemen sejumlah kolom *pseudo-inverse* kuncinya.
4. Menghitung
$$p_i = \left(K^{-1} c_i^{(1)}\right) + 32$$
dengan hasil setiap perhitungan $\left(K^{-1} c_i^{(1)}\right)$ dibulatkan ke dalam modulo 95. Diperoleh $p_1, \dots, p_k$.
5. Hasil perhitungan tersebut dikonversi ke dalam karakter ASCII.
6. Pengirim memperoleh *plaintext*.

Program aplikasi komputer dibuat untuk memudahkan proses perhitungan yang dibutuhkan karena kriptografi yang terlah dibentuk memiliki perhitungan yang cukup rumit. Program aplikasi komputer menggunakan bahasa pemograman *MATLAB R2016a*. Cara pemakaian serta validasi program aplikasi untuk proses enkripsi dan dekripsi adalah sebagai berikut.



Gambar 2. Tampilan Menu Utama

Pada tampilan utama pada Gambar 2, *user* dapat memilih apa yang akan dilakukan. Apabila *user* memilih keluar, maka aplikasi akan ditutup.

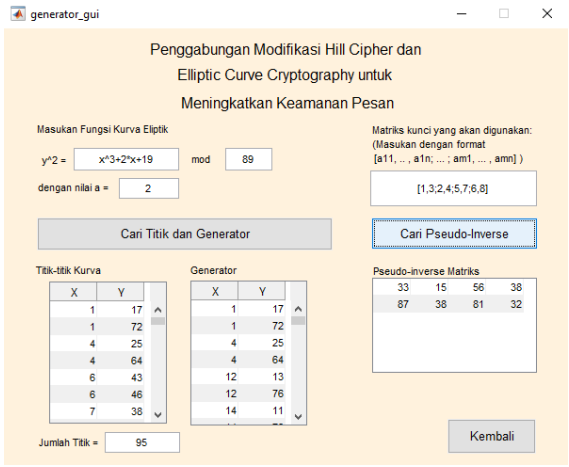


Gambar 3. Tampilan Pembangkitan Kunci

Pada Gambar 3, *user* dapat mengecek apa saja titik-titik pada kurva eliptik yang akan digunakan serta generatornya dengan mengisi fungsi $y^2 = x^3 + ax + b$ dan modulo yang digunakan serta nilai a dalam persamaan kurva eliptik pada *text box*. *User* juga dapat mengecek *pseudo-inverse* matriks kunci yang akan digunakan apakah memiliki *pseudo-inverse* atau tidak. Misalkan *user* akan menggunakan fungsi $y^2 \equiv x^3 + 2x + 19 \; mod \; 89$ dan matriks

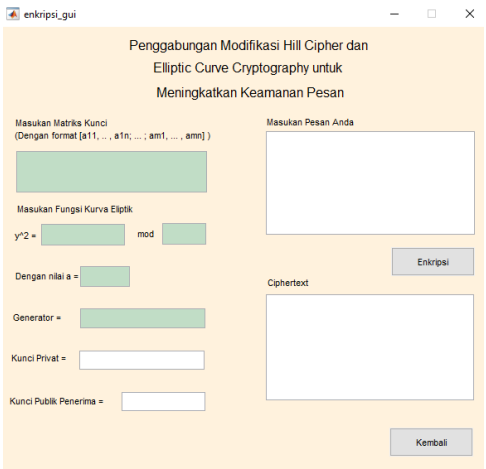
$$K = \begin{bmatrix} \overline{1} & \overline{3} \\ \overline{2} & \overline{4} \\ \overline{5} & \overline{7} \\ \overline{6} & \overline{8} \end{bmatrix}$$

sebagai kuncinya dengan $m = 4$ dan $n = 2$ kemudian *user* memasukan data tersebut. Apabila kunci tersebut dapat digunakan, diperoleh hasil seperti pada Gambar 4.



Gambar 4. Hasil Pembangkitan Kunci

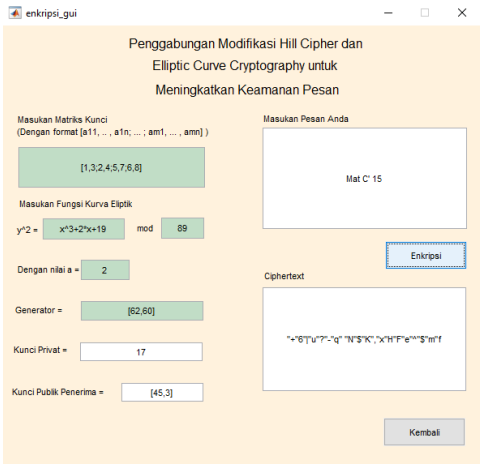
Selanjutnya pengirim dan penerima pesan menyepakati generator yang digunakan kemudian memilih kunci privat dan publik masing-masing. Ketika akan melakukan enkripsi, pengirim sebagai *user* akan melihat tampilan program seperti pada Gambar 5.



Gambar 5. Tampilan Program Enkripsi

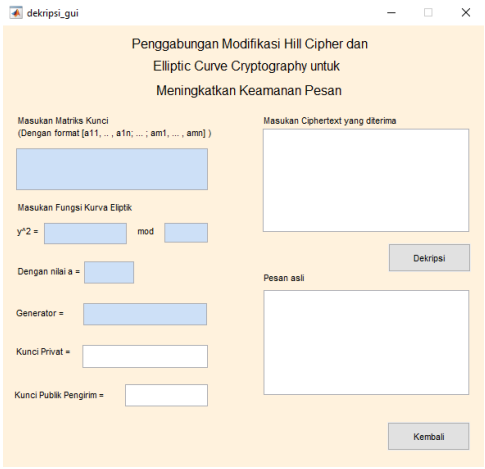
Pada Gambar 5, *user* dapat melakukan enkripsi terhadap pesan yang akan dikirimkan. *User* harus memasukkan beberapa informasi seperti kunci privat dan kunci publik pada *text box* yang disediakan. Misalkan pengirim dan menerima telah menyepakati kunci $G = (62,60)$. Pengirim menentukan kunci $\alpha = 17$ dan telah mendapatkan kunci publik penerima $B_1 = (45,3)$. Setelah memasukan kunci yang akan digunakan, *user* juga harus

memasukan pesan apa yang akan dikirimkan, misalkan pesannya adalah "Mat C' 15". Karena $panjang\ pesan = 9, 9\ mod\ 2 \not\equiv 0$ maka akan dilakukan penambahan karakter misal "." sehingga $panjang\ pesan = 10, 10\ mod\ 2 \equiv 0$. Setelah seluruh informasi dimasukan maka akan muncul *ciphertext* yang diperoleh seperti pada Gambar 6. Jika *user* memilih kembali maka *user* akan dibawa kembali pada tampilan utama.



Gambar 6. Hasil Proses Enkripsi

Ciphertext tersebut dikirimkan kepada penerima. Penerima sebagai *user* yang harus mendekripsi *ciphertext* akan melihat tampilan program seperti pada Gambar 7.

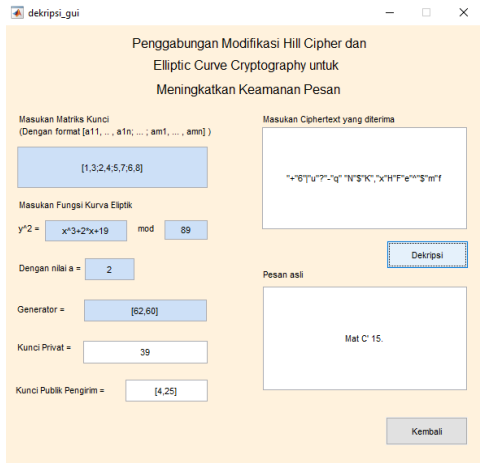


Gambar 7. Tampilan Proses Dekripsi

Pada Gambar 7, *user* dapat melakukan dekripsi dengan memasukkan beberapa informasi seperti kunci privat dan kunci publik pada *text box* yang disediakan. Penerima menentukan kunci privat $\beta = 39$ dan telah menerima kunci publik pengirim $A_1 = (4{,}25)$. Setelah memasukan kunci yang akan digunakan, *user* juga harus memasukan *ciphertext* apa yang diperoleh, yaitu

"+"6"|"u"?"-"q" "N"$"K","x"H"F"e"^"$"m"f

Setelah seluruh informasi dimasukan maka akan muncul pesan asli yang dikirimkan oleh pengirim seperti pada Gambar 8. Jika *user* memilih kembali maka *user* akan dibawa kembali pada tampilan utama.



Gambar 8. Hasil Proses Dekripsi

Pesan yang diperoleh adalah “Mat C’ 15.” karena telah dilakukan suatu proses penambahan karakter.

4. KESIMPULAN

Pengembangan kriptografi yang diperoleh dari penggabungan kriptosistem *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* adalah suatu kriptosistem yang memiliki tiga tahapan: pembangkitan kunci, enkripsi, dan dekripsi dengan $\mathcal{P}$ dan $\mathcal{C}$ merupakan himpunan karakter alfanumerik. *Hill cipher* dapat diretas dengan metode *known plaintext attack*, seorang kriptanalis dapat mengkriptanalisis *ciphertext* ketika memiliki sebagian *plaintext*nya, sehingga *hill cipher* menjadi tidak begitu aman. *Elliptic curve cryptography* umumnya digunakan untuk menyamarkan pesan berupa titik-titik pada kurva eliptik dan menghasilkan *ciphertext* berupa titik-titik pada kurva eliptik. Kriptosistem gabungan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* menghasilkan *ciphertext* berupa teks sehingga sulit untuk mengetahui bahwa kriptosistem yang digunakan adalah *elliptic curve cryptography*. Selain itu, penggabungan ini dapat mempersulit kriptanalisis karena selain kriptanalis harus meretas kedua algoritma tersebut dengan tingkat keamanan yang tinggi, kemungkinan kunci yang dapat digunakan lebih luas akibat modifikasi *hill cipher*. Program aplikasi digunakan untuk mempermudah proses pembangkitkan kunci, enkripsi, dan dekripsi. Program tersebut dapat digunakan oleh pengirim maupun penerima pesan.

5. DAFTAR PUSTAKA

[1] Agrawal, K. & Gera, A. (2014). Elliptic Curve Cryptography with *Hill cipher* Generation for Secure Text Cryptosystem. *International Journal of Computer Applications*, 106 (1), hlm. 18 – 24.

[2] Hidayat, A. & Alawiyah, T. 2013. Enkripsi dan Dekripsi Teks menggunakan Kriptosistem *hill cipher* dengan Kunci Matriks Persegi Panjang. *Jurnal Matematika Integratif*, 9 (1), hlm. 39-51.

[3] Jacob, B. 1990. *Linear Algebra*. New York: W.H.Freeman and Company.

[4] Stinson, D. R. 2006. *Cryptography Theory and Practice* (3rd ed.). Boca Raton: CRC Press.

[5] Kumar, D. S., Suneetha CH., & ChandrasekhAR, A. 2012. Encryption of Data Using Elliptic Curve Over Finite Fields. *International Journal of Distributed and Parallel System (IJDPS)*, 3 (1), hlm. 301-308.

[6] http://www.asciitable.com/