

# KRIPTOSISTEM MENEZES VANSTONE

(A Menezes Vanstone Cryptosystem)

Kiswara Agung Santoso

Departemen Matematika, FMIPA, Universitas Jember  
Jl. Kalimantan 37 Jember, 68111, Jawa Timur, Indonesia  
Email: [kiswara.fmipa@unej.ac.id](mailto:kiswara.fmipa@unej.ac.id)

**Abstract.** Many kinds of cryptosystem models we have known. Generally if input of plaintext is alphabet so ciphertext is alphabet or real number that can be transform to alphabet. This paper will introduce a type of cryptosystem that have special output. Its model is Menezes Vanstone cryptosystem. The plaintext of its method is pair of real number and ciphertext was produced is pair of real number too. If we want to know the meaning of ciphertext have to transform from real number to alphabet.

**Keywords:**

**MSC 2020:**

## 1. Pendahuluan

Kemajuan di bidang teknologi dan komputer telah memungkinkan seseorang untuk melakukan transaksi bisnis secara *cashless*, selain itu juga dapat mengirimkan informasi kepada temannya secara online. Kegiatan tersebut tentu saja akan menimbulkan resiko bila informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak.

Untuk mengantisipasi hal tersebut di atas maka muncullah ilmu pengetahuan yang mempelajari tentang pengkodean suatu teks yang lebih dikenal dengan nama Kriptografi. Banyak cara maupun algoritma yang digunakan dalam pengkodean ini, salah satunya adalah dengan menggunakan metode Menezes Vanstone pada  $Z_p$ . Kriptosistem ini merupakan modifikasi dari beberapa kriptosistem yang lain seperti kriptosistem ElGamal yang mempunyai domain elliptic curve. Pada prinsipnya metode ini adalah mengubah plainteks yang berbentuk kumpulan abjad (kata/kalimat) menjadi ciphertexts yang berbentuk bilangan dan pasangan terurut dari angka-angka hasil pengkodean. Metode ini merupakan cabang atau variasi dari Elliptic Curve Cryptosistem yang telah lama dikenal di dalam sistem pengkodean. Disini penulis mencoba menelaah kembali sistem pengkodean ini dengan harapan para pembaca dapat memahami serta mengembangkan atau menemukan sistem pengkodean yang baru.

### Quadratic Residu

Definisi : Misalkan  $p$  adalah suatu bilangan ganjil prima dan  $x$  adalah bilangan bulat maka  $x$  disebut **quadratic residu** modulo  $p$  jika  $y^2 \equiv x \pmod{p}$  dengan  $y \in Z_p$  dan  $1 \leq x \leq p-1$ .  $x$  disebut **quadratic non-residu modulo  $p$**  jika

$x \not\equiv 0 \pmod{p}$  dan bukan quadratic residu modulo  $p$ .

Contoh : 1, 3, 4, 5, dan 9 adalah quadratic residu modulo 11 ( $Z_{11}$ ) karena:

$$\begin{aligned} (\pm 1)^2 \pmod{11} &= (\pm 10)^2 \pmod{11} = 1, & (\pm 5)^2 \pmod{11} &= (\pm 6)^2 \pmod{11} = 3 \\ (\pm 2)^2 \pmod{11} &= (\pm 9)^2 \pmod{11} = 4, & (\pm 4)^2 \pmod{11} &= (\pm 7)^2 \pmod{11} = 5 \\ (\pm 3)^2 \pmod{11} &= (\pm 8)^2 \pmod{11} = 9. \end{aligned}$$

Definisi : Jika  $p$  bilangan prima positif maka  $x^{p-1} \equiv 1 \pmod{p}$

Teorema Euler's Criterion :

Jika  $p$  bilangan prima maka  $x$  adalah quadratic residu jika dan hanya jika :

$$x^{(p-1)/2} \equiv 1 \pmod{p}$$

Bukti : misalkan  $x = y^2 \pmod{p}$  dan berdasarkan definisi bahwa  $x^{p-1} \equiv 1 \pmod{p}$  untuk setiap  $p$  bilangan ganjil prima maka :

$$\begin{aligned} x^{(p-1)/2} &\equiv (y^2)^{(p-1)/2} \pmod{p} \\ &\equiv y^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

Definisi : Jika  $p$  bilangan ganjil prima dan sembarang bilangan bulat  $a \geq 0$  maka dapat didefinisikan *Legendre symbol*  $(a/p)$  sebagai berikut :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{jika } a \equiv 0 \pmod{p} \\ 1 & \text{jika } a \text{ quadratic residu modulo } p \\ -1 & \text{jika } a \text{ quadratic non-residu modulo } p \end{cases}$$

### Menezes Vanstone

Definisi : Misalkan bilangan ganjil prima  $p > 3$  maka suatu Fungsi pembangkit pada  $Z_p$  didefinisikan :

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

Yang mempunyai solusi :  $\{(x, y) \mid x, y \in Z_p^* \times Z_p^*\}$

Fungsi tersebut kemudian dibentuk menjadi grup Abelian dengan aturan sbb:

$$\text{Misalkan } \begin{cases} P = (x_1, y_1) \\ Q = (x_2, y_2) \end{cases} \quad \text{Jika } \begin{cases} x_1 = x_2 \\ y_1 = -y_2 \end{cases} \left. \vphantom{\begin{matrix} P \\ Q \end{matrix}} \right\} P + Q = 0$$

dari bentuk di atas dapat disimpulkan bahwa  $-(x, y) = (x, -y)$

$$P + Q = \begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{utk } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & \text{utk } P = Q \end{cases}$$

Diketahui plaintext  $(P) = Z_p^* \times Z_p^*$ ; ciphertext  $(C) = E \times Z_p^* \times Z_p^*$

Dengan kunci  $K = \{(E, \alpha, \beta) : \beta = a\alpha, \text{ dan } a \in E\}$ .

$\alpha$  adalah pasangan berurutan  $(x, y)$  yang didapat dari fungsi pembangkit yang telah

didefinisikan di atas yaitu :  $y^2 \equiv x^3 + ax + b \pmod{p}$ . Nilai  $\alpha$  dan  $\beta$  bersifat public dan  $a$  bersifat rahasia (secret)

## 2. Hasil dan Pembahasan

Berikut algoritma Elliptic Menezes Vanston Cryptosystem :

### Proses encoding

1. Tentukan bilangan random  $k \in Z_{11}$  dan  $a$  sebagai private key
2. Tentukan nilai  $\alpha$  yang merupakan pasangan berurutan dari fungsi pembangkit
3. Konversi pasangan huruf yang akan dikodekan menjadi bilangan. Misalkan plaintext adalah  $(x_1, x_2)$
4. Hasil pengkodean adalah pasangan berurutan  $c_{k(x,k)} = (y_0, y_1, y_2)$  dimana :

$$y_0 = k\alpha, \quad \beta = a\alpha$$

$$(c_1, c_2) = k\beta$$

$$y_1 = c_1 \cdot x_1 \pmod{p}$$

$$y_2 = c_2 \cdot x_2 \pmod{p}$$

Hasil pengkodean dari sebuah pasangan berurutan dengan dua elemen menjadi sebuah pasangan berurutan dengan tiga elemen dimana elemen pertama juga merupakan pasangan berurutan

### Proses decoding

1. Misalkan ciphertext yang akan didecode adalah  $(y_0, y_1, y_2)$
2.  $(c_1, c_2) = a \cdot y_0$
3.  $d_{k(y)} = (y_1 c_1^{-1} \pmod{p}, y_2 c_2^{-1} \pmod{p})$

Hasil encoding dari ciphertext ke plaintext adalah sebuah pasangan berurutan dengan tiga elemen menjadi sebuah pasangan berurutan dengan dua elemen

### Contoh :

Misalkan  $p=11$ ,  $a=1$  dan  $b=6$  sehingga didapat suatu fungsi pembangkit pada  $Z_p$  :

$$y^2 \equiv x^3 + x + 6 \pmod{11}$$

Misalkan huruf yang kita kodekan adalah JB, sehingga bila ditransfer ke bentuk bilangan menjadi pasangan berurutan **(9,1)**. Andaikan bilangan acak yang kita pilih pada  $Z_{11}$  adalah **6**.

Menurut kriteria Euler konstanta yang merupakan quadratic residu modulo 11 adalah : 1, 3, 4, 5, 9 karena :

$$1^5 \equiv 1 \pmod{11} \quad 3^5 \equiv 1 \pmod{11} \quad 4^5 \equiv 1 \pmod{11}$$

$$5^5 \equiv 1 \pmod{11} \quad 9^5 \equiv 1 \pmod{11}$$

bila pada kurva diatas kita ambil nilai  $x$  yang memenuhi syarat maka dapat dibuat suatu tabel solusi seperti berikut :

| X  | $y^2 \equiv x^3 + x + 6 \pmod{11}$ | Y    |
|----|------------------------------------|------|
| 2  | 5                                  | 4, 7 |
| 3  | 3                                  | 5, 6 |
| 5  | 4                                  | 2, 9 |
| 7  | 4                                  | 2, 9 |
| 8  | 9                                  | 3, 8 |
| 10 | 4                                  | 2, 9 |

Nilai y di atas didapat karena perhitungan sebagai berikut :

$$4^2 = 5 \pmod{11} \quad 7^2 = 5 \pmod{11} \quad 5^2 = 3 \pmod{11} \quad 6^2 = 3 \pmod{11}$$

$$2^2 = 4 \pmod{11} \quad 9^2 = 4 \pmod{11} \quad 3^2 = 9 \pmod{11} \quad 8^2 = 9 \pmod{11}$$

Misalkan plainteks = (9,1), fungsi pembangkit  $\alpha = (2,7)$  dan private key ( $a = 7$ ) dan nilai  $k = 6$  maka dapat dihitung :

proses enkripsi :

$$\beta = 7 \cdot \alpha$$

$$\alpha + \alpha = (2,7) + (2,7)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 4 + 1}{2 \cdot 7} = \frac{13}{14} \pmod{11}$$

$$= 13 \cdot 4 \pmod{11} = 8 \pmod{11}$$

$$x_3 = \lambda^2 - x_1 - x_2 = 64 - 2 - 2$$

$$= 60 \pmod{11} = 5 \pmod{11}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 8(2 - 5) - 7$$

$$= -31 \pmod{11} = 2 \pmod{11}$$

$$\therefore 2\alpha = (5,2)$$

$$2\alpha + \alpha = (5,2) + (2,7)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{7 - 2}{2 - 5} = \frac{5}{-3} \pmod{11}$$

$$= 5 \cdot -4 \pmod{11} = 2 \pmod{11}$$

$$x_3 = \lambda^2 - x_1 - x_2 = 4 - 5 - 2$$

$$= -3 \pmod{11} = 8 \pmod{11}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 2(5 - 8) - 2$$

$$= -8 \pmod{11} = 3 \pmod{11}$$

$$\therefore 3\alpha = (8,3)$$

$$4\alpha = (10,2);$$

$$5\alpha = (3,6);$$

$$6\alpha = (7,9)$$

Ulangi proses di atas hingga didapat  $\beta = 7.\alpha = (7,2)$

$$x = (x_1, x_2) = (9,1) ; k = 6, \text{ sehingga dapat dihitung}$$

$$y_0 = k\alpha = 6.(2,7) = (7,9)$$

$$(c_1, c_2) = k\beta = 6.(7,2) = (8,3)$$

Sehingga didapat nilai  $c_1 = 8$  dan  $c_2 = 3$

$$y_1 = c_1x_1 \bmod p = 8 \times 9 \bmod 11 = 6$$

$$y_2 = c_2x_2 \bmod p = 3 \times 1 \bmod 11 = 3$$

Jadi hasil encoding adalah  $y = (y_0, y_1, y_2) = ((7,9), 6, 3)$ .

proses dekripsi :

Diketahui kode  $y = ((7,9), 6, 3)$ .

Untuk menguraikan kembali kita harus menghitung dahulu

$$(c_1, c_2) = a.y_0 = 7.(7,9) = (8,3)$$

Dan selanjutnya

$$\begin{aligned} x &= (y_1c_1^{-1} \bmod p, y_2c_2^{-1} \bmod p) \\ &= (6 \times 8^{-1} \bmod 11, 3 \times 3^{-1} \bmod 11) \\ &= (6 \times 7 \bmod 11, 3 \times 4 \bmod 11) \\ &= (9,1) \end{aligned}$$

Jadi ciphertext telah di decode kembali menjadi plaintext yaitu  $(9,1) = JB$ .

### 3. Kesimpulan

Dari tulisan di atas dapat disimpulkan bahwa Menezes Vanston Cryptosystem merupakan salah satu sistem pengkodean yang mengkodekan plainteks dalam bentuk abjad menjadi cipherteks dalam bentuk pasangan berurutan dari bilangan-bilangan pada dimensi yang telah ditentukan.

### Daftar Pustaka

- [1] A.J. Menezes Vanstone, A., (1993), *Elliptic Curve Cryptosystem and their implementation*. Journal of Crptology, 6, hal 209 – 204.
- [2] V.Miller. (1986). *Uses of Elliptic Curve in cryptography. Lecture notes in computer science*. Proceeding of SECURICOM. Hal 127 – 137.
- [3] Douglas Stinson, D., (1997), *Cryptography Theory and Practice*. CRC Press. Boca Raton London.
- [4] A.J. Menezes, A.J., (1993), *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publisher.

- [5] Konheim, A.G., (1981). *Cryptography A Primer*. John Wiley and Sons.