Jurnal Riset Komputer (JURIKOM), Vol. 6, No. 4, Agustus 2019
ISSN 2407-389X (Media Cetak)
Hal: 395-400

Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Penyandian Pesan Pada Aplikasi Chatting Client Server Berbasis Desktop

Putri S E A Damanik

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338 Medan, Indonesia

Abstrak

Masalah keamanan pada komputer menjadi isu terpenting pada era teknologi informasi saat ini. Banyak kejahatan cyber yang terjadi salah satunya yang terkait dengan manipulasi data pada jaringan. Masalah terpenting pada keamanan komputer adalah masalah keamanan data yang dikirimkan. Contoh data yang sangat perlu diamankan adalah pesan pada apliksi chatting. Selain mencegah informasi yang terbaca oleh pihak lain, penyandian pesan sangat memungkinkan efektiftas dalam pengiriman informasi yang bersifat rahasia. Salah satu jenis algoritma asimetris yang memiliki 2 kunci berbeda untuk enkripsi dan dekripsi dalam metode penyembunyian pesan (Kriptografi) dimana pengirim pesan terlebih dahulu menggunakan kunci publik (public key)dalam menyandikan pesan, dan untuk mendekripsikan pesan tersandi penerima akan menggunakan kunci rahasia (private key). Algoritma Elliptic Curve Cryptography terbilang cukup rumit dalam perhitungannya, karena perhitungannya berbeda dengan perhitungan biasa.

Kata Kunci: Keamanan , PrivateKey, Client, Server.

Abstract

The problem of security on computers is the most important issue in the current era of information technology. Many cyber crimes that occur one of which is related to data manipulation on the network. The most important problem with computer security is the security of the data that is sent. Examples of data that really need to be secured are messages in chat applications. In addition to preventing information from being read by other parties, encoding of messages greatly enables the effectiveness of sending confidential information. One type of asymmetric algorithm that has 2 different keys for encryption and decryption in the method of hiding messages (Cryptography) where the sender of the message first uses the public key (public key) to encode the message, and to decrypt the encrypted message the recipient will use a secret key (private key). The Elliptic Curve Cryptography algorithm is quite complicated in its calculations, because the calculations are different from ordinary calculations.

Keywords: Security, PrivateKey, Client, Server.

1. PENDAHULUAN

Salah satu pengamanan data yang wajib diperhatikan adalah pesan pada aplikasi Chatting. Pesan merupakan suatu informasi yang disampaikan kepada orang lain, sedangkan Chatting adalah suatu feature / program untuk berkomunikasi langsung sesama pemakai yang sedang terhubung dalam suatu jaringan. Komunikasi bisa berupa teks (text chat) atau suara (voice chat). Chatting client server bersifat rahasia, yang artinya pesan atau informasi yang ada didalamnya penting dan tidak boleh diketahui oleh pihak yang tidak terkait. Hal ini lah yang membuat penyandian pesan bersifat jaringan Peer To Peer pada aplikasi Chatting Client server ini dapat diterapkan untuk dilakukan pengamanannya. Jaringan Peer To Peer adalah salah satu model jaringan yang terdiri dari dua atau lebih komputer, dimana setiap station atau komputer yang terdapat didalam lingkungan jaringan tersebut bisa saling berbagi. Salah satu komputer bertindak sebagai client ataupun server, client sebagai penerima pesan. Pesan yang dikirimkan oleh server harus di enkripsikan terlebih dahulu sebelum dikirim ke client. Dengan demikian meskipun pesan terbaca oleh pihak lain maka makna dari pesan yang telah dienkripsikan tidak akan mudah bahkan tidak akan dimengerti oleh pihak lain yang berusaha membacanya. Selain harus didekripsikan, tentu metode dalam pemecahannya pun hanya akan dipahami oleh client dan server [1]. Metode dalam pengamanan pesan ini menggunakan salah satu metode yang sulit dipecahkan. Elliptic Curve Cryptography (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik berdasarkan pada struktur aljabar dari kurva elips pada daerah finite. Elliptic Curve Cryptography (ECC) juga merupakan teknik kriptografi asimetri yang menggunakan dua buah kunci berbeda dalam proses enkripsi dan dekripsi. Kedua kunci tersebut dikenal dengan private key yang digunakan untuk enkripsi data dan public key yang digunakan untuk enkripsi data [2]..

2. LANDASAN TEORI

2.1 Algoritma *Elliptic Curve Crypthography (ECC)*

Elliptic Curve Cryptography (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik berdasarkan pada struktur aljabar dari kurva ellips pada daerah finite. Penggunaan kurva elips dalam kriptografi dicetuskan oleh Neal Koblitz dan victor S. Miller pada tahun 1985. Kurva elips juga digunakan pada beberapa algoritma pemaktoran integer yang juga memiliki aplikasinya dalam kriptografi, seperti *Lenstra Elliptic Curve*

Factorization. Algoritma kunci publik berdasarkan pada variasi perhitungan matematis yang terbilang sangat sulit dipecahkan tanpa pengetahuan tertentu mengenai bagaimana perhitungan tersebut dibuat [2].
Kurva ellips dapat ditulis dengan perhitungan matematis sebagai berikut:

$$y^2 = x^3 + ax + b \quad (1)$$

Dalam kriptografi kunci asimetris, harus ditentukan terlebih dahulu nilai parameter yang akan digunakan dan telah disepakati oleh pihak yang akan berkomunikasi. Parameter yang digunakan dalam ECC yaitu nilai *a* dan *b*, bilangan prima *p* dalam persamaan kurva eliptik bidang terbatas serta titik generator *G* yang dipilih dari kurva eliptik. Pendekatan enkripsi dengan ECC ini dapat dijelaskan dalam contoh kasus misalnya Alice ingin menerima pesan yang terinkripsi dari Bob.

1. Pembangkitan Kunci Privat dan Kunci Publik
   Bob membangkitkan kunci privat $n_B$dengan cara memilih bilangan acak yang nilainya diantara [1,*p*-1]. Dengan kunci privat tersebut, Bob membangkitkan kunci publik P_B=n_B.G.
2. Enkripsi
   Misalnya pesan yang akan dikirim adalah pesan *m*. Alice meng-*encode* pesan *m* menjadi sebuah titik P_m, dari kurva eliptik. Lalu memilih bilangan acak *k* yang nilai diantara [1,p-1]. Alice menghasilkan cipherteks, C_m={(kG),(P_m+kP_B)} dimana *G* adala titik generator dan P_B adalah kunci publik Bob.
3. Deskripsi
   Untuk melakukan deskripsi cipherteks C_m, Bob mula-mula mengalikan ttik pertama dari cipherteks dengan kunci privatnya $n_B$dan kemudian mengurangkan titik kedua dari cipherteks dengan hasil perkalian tersebut.
   P_m+knP_B-n_B(kG)= P_m+k(n_BG)- n_B(kG)= P_m (2)
   Lalu Bob men-decode P_m menjadi pesan *m* semula.

3. ANALISA DAN PEMBAHASAN

Kriptografi kurva eliptik merupakan metode kriptografi yang menggunakan titik-titik pada kurva eliptik sebagai kunci untuk melakukan proses enkripsi dan deskripsi. Kekuatan dari kriptografi ini adalah banyaknya titik yang terdapat pada sebuah kurva dan sulitnya mengetahui kurva yang digunakan. Kriptografi eliptik menggunakan dua buah kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi eliptik adalah sebuah titik pada kurva yang kita pilih sendiri, sedangkan kunci privatnya adalah angka yang bersifat acak. Kunci publik diperoleh dengan melakukan operasi perkalian antara kunci privat dengan titik P yang kita pilih.

1. Proses pembentukan Kunci
   Adapun proses pembentukan kurva dan pembentukan kunci pada kriptografi kurva eliptik adalah sebagai berikut:
   a. Menentukan bilangan prima (p) dengan syarat p>3 untuk Fp
      Bilangan prima yang akan digunakan pada tahap ini adalah bilangan prima yang akan dihasilkan dari pembangkit bilangan acak Rabin-Miller. Adapun apabila kita ingin uji apakah suatu bilangan merupakan bilangan prima atau tidak, maka dapat diuji dengan cara berikut ini:
      Misalnya diambil bilangan prima 17, kemudian diambil nilai n=2 kemudian dihitung Greatest Common Divisor (GDC) atau pembagi bersama terbesar dari 17 adalah (13,2)=1
      $n^{p-1} \equiv 1 (mod\ p) = 217-1 = 65536 \equiv 1\ (mod\ 17)$
      Maka 17 adalah bilangan prima karena tidak habis dibagi, sehingga didapat p=17
   b. Menentukan bentuk persamaan kurva eliptik
      Persamaan kurva eliptik adalah y^2=x^3+ ax + b *(mod p)* dimana nilai a, b dibuat secara acak untuk koefisiennya. Pada sistem ini, sebagai salah satu batasan masalah, maka ditetapkan bahwa nilai a=1 dan b=1 sedangkan p kita gunakan 17, sehingga persamaan kurva eliptik menjadi:
      y^2=x^3+ x + 1 *(mod 17)*
      Sehingga : $4a^3+27b^2 \neq 0$ *(mod* 17)
      $4.1^3+27.1^2$ (mod 17)
      =31 (mod 17)
      =14 ≠0
      Maka persamaan y^2=x^3+ x + 1*(mod 17)* merupakan persamaan kurva eliptik.
   c. Menentukan titik-titik pada kurva
      Setelah kurva eliptik didapatkan, maka kita perlu menentukan titik-titik pada kurva. Dari titik-titik yang telah ditentukan tersebut, kemudian pilih salah satu secara acak. Misalnya pada contoh diatas, bilangan prima 17, selanjutnya kita cari elemen-elemen grup eliptik E_{17} atas F_p, dengan F_p = {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16}. Namun sebelum menentukan elemen-elemen E_{17}(1,1) terlebih dahulu kita perlu mencari *quadratic residue modulo* 17 (QR_{17}).
   d. Membuat kunci privat 1 dan kunci privat 2

Kunci privat 1 dan 2 ditentukan dengan nilai acak dimana nilai tersebut harus merupakan elemen dari {2,3,.....,p-1} dalam F_p. Misalnya pilih kunci privat1=6 dan kunci privat 2=9

e. Menghitung kunci publik 1 dan kunci publik 2
Kunci publik dihitung oleh masing-masing pengguna dengan melakukan operasi perkalian titik antara titik P dengan kunci rahasia masing-masing.
KP_1=KR_1*P
=6 * (15,12)
=(15,12) + (15,12) +(15,12) +(15,12) + (15,12) + (15,12)
=(13,16) + (15,12) +(15,12) +(15,12) + (15,12)
=(9,5) +(15,12) +(15,12) + (15,12)
=(4,16)+(15,2)=(10,5)
Jadi kunci publik 1 adalah (10,5)
Sedangkan pada pengguna 2, kunci privat 2=9 dan titik P(15,12) maka:
KP_2=KR_2*P
=9* (15,12)
=(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)
=(13,16)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)
=(10,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)+(15,12)
= (9,5) +(15,12) +(15,12) +(15,12) + (15,12) +(15,12)
= (10,5) +(15,12) +(15,12) +(15,12)
=(13,1) +(15,12) +(15,12)= (15,5) +(15,12)=(4,12)
Jadi kunci publik 2 adalah (4,12)

2. Proses Enkripsi
Proses enkripsi ini dilakukan oleh pengguna 1 yang akan mengirim pesan kepada pengguna 2, adapun cara enkripsi adalah sebagai berikut:

a. Sebagai langkah awal, pengguna memilih sebuah angka acak yang akan dijadikan kunci rahasia bangkitan (*private*1_gen) yang akan disimbolkan dengan k. Nilai k dapat dipilih dalam interval k={2,3,...p-1} dalam F_{17}. Kita misalkan kunci rahasia bangkitan yang kita pilih adalah 1.
b. Pengguna kemudian menghitung kunci rahasia bersama bangkitan (key1_gen) dengan cara:
Key1_gen= private1_gen*kunci publik 2
=1*(4,12)=(4,12)
c. Selanjutnya pengguna mengambil nilai absis dari key1_gen diatas. Karena nilai key1_gen adalah (4,12) maka absisnya adalah 4, jadi xkey1_gen=4
d. Setelah semua langkah diatas selesai, pengguna sudah bisa mengenkripsi pesan dengan menggunakan ketentuan:
C1=k*P
C2= m⊕ xkey1_gen (pesan yang akan dienkripsi di XOR kan dengan xkey1_gen).
Maka hasil yang didapat adalah C1berupa titik, sedangkan C2,C3 dan seterusnya berupa bilangan integer yang akan dikirim kepada pengguna 2.

Tabel 1. Konversi Karakter Ke Kode ASCI

CHAR	ASCII (DEC)
P	80
U	85
T	84
R	82
I	73
D	68
A	65
M	77
A	65
N	78
I	73
K	75

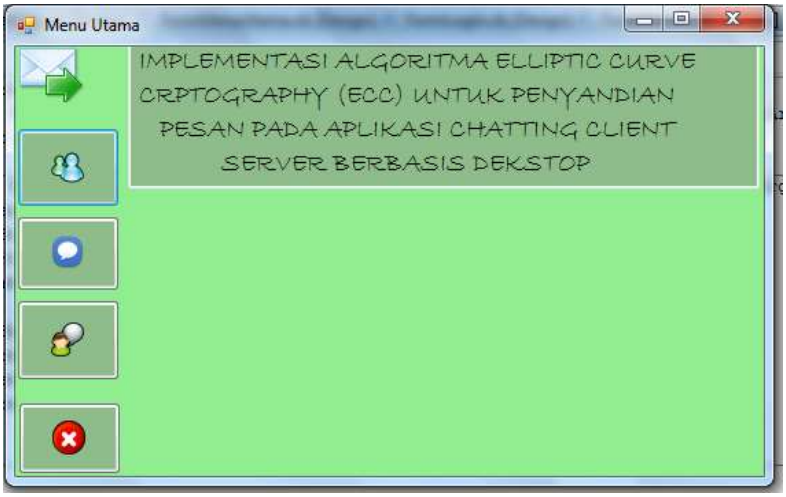
4. IMPLEMENTASI

Perancangan aplikasi kriptografi pesan teks telah dirancang dan dibuat dengan menggunakan aplikasi Microsoft Visual Studio 8 dan bahasa pemograman Visual Basic. Adapun tampilan halaman yang dirancang penulis adalah sebagai berikut :

1. Tampilan Halaman Login User Server/Client

Gambar 1. Tampilan Halaman Login

2. Tampilan Halaman Menu Utama

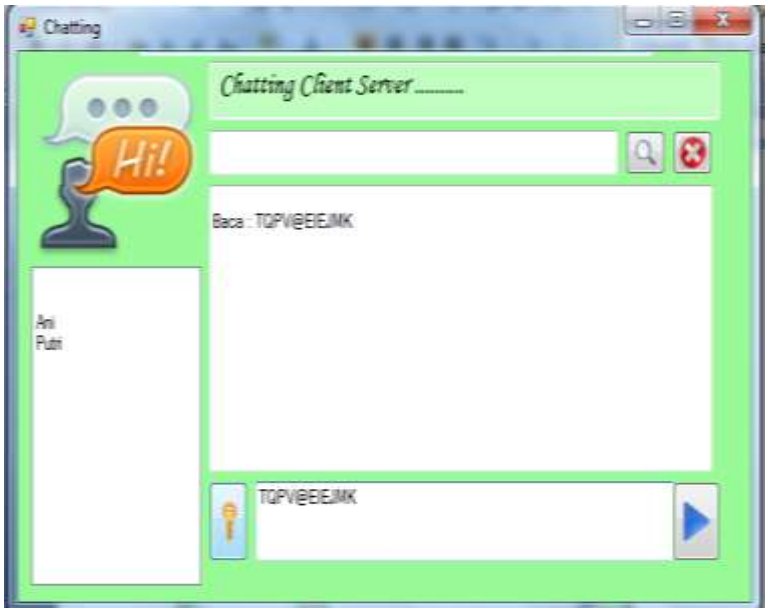


Gambar 2. Tampilan Halaman Menu Utama

3. Tampilan Halaman Menu Utama

Gambar 3. Tampilan Pesan Masuk

Pesan yang dikirim oleh server dan telah diterima oleh client akan tampil pada halaman Chatting Client dan kemudian akan dibaca dan dilakukan pendekripsian. Proses dekripsi pada ciphertext seperti gambar berikut:



Gambar 4. Tampilan Dekripsi Pesan

Gambar 5. Tampilan Pesan Terdekripsi.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan penulis pada aplikasi chatting client server berbasis dekstop menggunakan teknik kriptografi yang dibangun maka dapat disimpulkan :

1. Konsep pengiriman pesan berdasarkan jaringan peer to peer dimana client dan server terhubung dalam jaringan untuk dapat melakukan pengiriman pesan.
2. Penerapan algoritma Elliptic Curve Cryptography pada aplikasi chatting client server berbasis dekstop ini dapat pengamankan isi pesan, Dengan ini penggunaan algoritma Elliptic Curve Cryptography (ECC) dapat mengamankan pesan teks, serta dapat menyajikan enkripsi dan dekripsi pesan teks dengan tepat.
3. Aplikasi penyandian pesan teks dengan menerapkan algoritma Elliptic Curve Cryptography (ECC) telah selesai dirancang dan dapat dijadikan salah satu alternatif aplikasi chatting client server.

REFERENCES

[1] M. Zunaidi, B. Andika and S. , "Membentuk Jaringan PEER TO PEER Menggunakan Kabel FIREWIRE IEEE-1394 Dengan Metode Bridge," Jurnal Ilmiah SAINTIKOM, vol. 13, pp. 107-120, 2014.
[2] E. B. Harjono and e. a. , Analisis Kripto Sistem Algoritma AES Dan Elliptic Curve Cryptography (ECC) Untuk Kemanan Data, Vols. Vol 1, No 2, 2017.
[3] Logika Dan Algoritma, Surabaya: Politeknik Elektronik Negerei Surabaya, 2013.
[4] D. Ariyus, Pengantar Ilmu Kriptografi, Teori, Analisis, Dan Implementasi, S. Suyanto, Penyunt., Yogyakarta: Andi, 2008.
[5] A. J. Manezes dan e. a. , Handbook Of Applied Cryphtography, Newyork: CRC Press, 1996.
[6] S. Nurhayani, "Implementasi Penggunaan Teknik Steganografi Metode LSB & Polybus Square Cipher pada Citra Digital," Vols. Vol 1, No 3.
[7] Suprapto, Bahasa Pemograman, R. A. Avianti, Penyunt., Dapartemen Pendidikan Nasional, 2008.
[8] Darmayuda Ketut, Pemograman Aplikasi Database Dengan Microsoft Visual Basic.Net 2008, Informatika, 2009.
[9] Dony Ariyus, Pengantar Ilmu Kriptografi Teori Dan Analisis dan Implementasi, Yogyakarta, Andi Offset, 2008
[10] Wahana Komputer, SQL Server 2102, Andi, 2013.