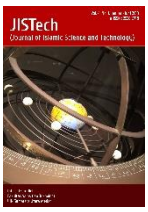


JISTech (Journal of Islamic Science and Technology)

JISTech, 5(1), 22-38, Januari-Juni 2020

ISSN: 2528-5718

http://jurnal.uinsu.ac.id/index.php/jistech

APLIKASI PENGAMANAN EKSTENSI FILE MENGGUNAKAN KRIPTOGRAFI ONE TIME PAD (OTP) DAN ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Heri Santoso[1], Mhd. Zulfansyuri Siambaton[2]

[1]Univeristas Islam Negeri Sumatera Utara
[2]Univeristas Islam Sumatera Utara
Email : herisantoso@uinsu.ac.id, zulfansyuri@ft.uisu.ac.id

ABSTRAK

Keamanan suatu data rahasia sangat penting untuk dijaga. Apalagi dengan semakin berkembangnya teknologi. Kriptografi merupakan cabang ilmu yang berperan dalam keamanan dan kerahasiaan suatu data. Untuk mengamankan data tersebut dalam dilakukan penerapan ilmu kriptografi yang bertujuan untuk mengubah data asli (plaintext) menjadi data terenkripsi (ciphertext), Tulisan ini bertujuan untuk menambah pengetahuan dan referensi tentang bagaimana cara kerja algoritma One Time Pad dalam mengamankan data untuk ekstensi file. Dan juga bagaimana cara kerja algoritma *Elliptic Curve Cryptography* dalam mengamankan data menggunakan kunci publik. Pembahasan ini akan menghasilkan sebuah aplikasi yang dapat digunakan untuk mengenkripsi ekstensi file.

Kata Kunci : Kriptografi, *One Time Pad*, *Elliptic Curve Cryptography*, Enkripsi, Pengamanan.

PENDAHULUAN

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting pada sistem informasi saat ini. Hal ini di sebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya suatu teknikteknik yang baru yang disalahgunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Ironisnya, teknik yang digunakan untuk mengancam keamanan data selalu setingkat lebih maju dari pada teknik yang digunakan untuk mengamankan

data.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Kriptografi merupakan salah satu komponen yang tidak dapat diabaikan dalam membangun keamanan data pada komputer. Algoritma One Time Pad ditemukan pada tahun 1917 oleh Major Joseph Mauborgne. Algoritma ini termasuk ke dalam kelompok algoritma kriptografi simetri. One Time Pad (pad = kertas blok not) berisi barisan karakter - karakter kunci yang dibangkitkan secara acak, dan pengacakannya tidak menggunakan rumus tertentu. Jika kunci tersebut benar-benar acak, digunakan hanya sekali, serta terjaga kerahasiannya dengan baik, maka metode penyandian OTP ini sangat kuat dan tidak dapat dipecahkan. Namun Algoritma ini memiliki beberapa kelemahan, kunci yang digunakan harus benar-benar acak, panjang kunci juga harus sama dengan panjang pesan.

Algoritma ECC-ElGamal diakui sebagai algoritma dengan keamanan yang baik walaupun menggunakan kunci yang lebih pendek dari algoritma lain, seperti RSA. Algoritma ini bergantung pada kunci untuk enkripsi dan dekripsinya. Walaupun keamanan algoritma ini sudah cukup baik, keamanan tersebut masih dapat ditingkatkan dengan menambahkan faktor waktu pada algoritma enkripsi tersebut . Kriptografi kurva eliptik mendasarkan keamanannya pada permasalahan matematis kurva eliptik yang berbeda dengan persamalahan matematis logaritma diskrit dan pemfaktoran bilangan bulat biasa karena tidak ada algoritma waktu subeksponensial yang diketahui untuk memecahkan permasalahan matematis logaritma diskrit kurva eliptik (Elliptic Curve Discrete Logarithm Problem). Karena alasan tersebutlah maka algoritma kriptografi kurva eliptik mempunyai keuntungan jika dibandingkan dengan algoritma kunci publik lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Dan untuk data yang mau diamankan kita menggunakan beberapa ekstensi file, alasannya sudah banyak data yang diamankan menggunakan file text.

KAJIAN PUSTAKA

Kriptografi

Kriptografi (cryptography) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan), jadi kriptografi berarti "secret writing" (tulisan rahasia). Definisi kriptografi ada beberapa yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. namun saat ini kriptografi lebih dari sekadar privacy, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudiation*.

Algoritma Kriptografi

Algoritma kriptografi atau sering disebut dengan cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi ada dua macam, yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*).

Algortima *One Time Pad*

One Time Pad ini ditemukan pada tahun 1917 oleh Major Yoseph Mouborgne dan Gilbert Vernam pada perang dunia ke dua.metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan. Suatu algoritma dikatakan aman, apabila tidak ada cara untuk menemukan plaintext-nya Sampai saat ini, hanya algoritma *One Time Pad* (OTP) yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas. Algoritma *One Time Pad* adalah salah satu jenis algoritma simetri (konvensional). Panjang kunci sama dengan panjang plainteks.

Secara teoritis, teknik *one-time pad* merupakan teknik enkripsi yang sempurna (perfect encryption) asalkan proses pembuatan kunci benar

acak.

Secara historis, enkripsi *one-time pad* digunakan oleh misi diplomatik berbagai negara di masa lalu untuk komunikasi rahasia. Semacam buku kode yang dibuat secara acak dan tidak boleh diguna-ulang harus dibawa oleh kurir yang dipercaya untuk didistribusikan ke perwakilan diplomatik negara yang bersangkutan. Setiap pengiriman naskah rahasia, kunci sebesar naskah rahasia diambil dari buku kode untuk mengenkripsi naskah. Kunci yang sudah digunakan untuk enkripsi tidak boleh digunakan lagi untuk enkripsi selanjutnya.

One-time pad dapat digunakan untuk komunikasi sangat rahasia dengan volume yang tidak terlalu besar, namun untuk penggunaan skala besar dalam suatu sistem teknologi informasi, one-time pad tidak praktis. Walaupun tidak digunakan secara langsung, konsep one-time pad ditiru" dalam teknik enkripsi stream cipher.

Algoritma Elliptic Curve Cryptography

Elliptic Curve Cryptography atau Kriptografi Kurva Eliptik adalah sebuah algoritma kriptografi kunci publik, yaitu algoritma dimana setiap pihaknya memiliki sepasang kunci privat dan kunci publik. Kunci privat hanya dimiliki oleh pribadi-pribadi yang berkepentingan, sedangkan kunci publik disebarluaskan ke semua pihak.

Pendekatan yang dilakukan untuk menghasilkan algoritma Kriptografi Kurva Eliptik adalah dengan menggunakan struktur matematika yang sangat unik yang memungkinkan pemrosesan titik dengan memiliki dua buah titik dalam sebuah kurva eliptik dan menghasilkan sebuah titik lain yang ada pada kurva tersebut. Struktur yang unik ini memberikan keuntungan dalam kriptografi dikarenakan kesulitan untuk menemukan 2 buah titik yang menentukan sebuah titik tertentu tersebut tidak dapat ditemukan dengan mudah. Tingkat kesulitan untuk menemukan 2 buah titik termasuk dalam golongan yang rumit sama seperti kesulitan untuk memperhitungkan 4 variasi eksponensial yang digunakan dalam algoritma RSA yang telah banyak diimplementasikan. Untuk memecahkan Kriptografi Kurva Eliptik sendiri dibutuhkan perhitungan

matematis yang sangat tinggi.

Kriptografi Kurva Eliptik terdiri dari beberapa operasi basic dan juga aturan yang mendefinisikan penggunaan dari operasi operasi basic seperti penambahan, pengurangan, perkalian dan perpangkatan yang didefinisikan sesuai dengan kurvakurva yang ada.Operasi matematika yang digunakan pada Elliptic Curve Cryptography didefinisikan dengan persamaan

$$y2 = x3 + ax + b \text{ dengan } 4a3 + 27b2 \neq 0$$

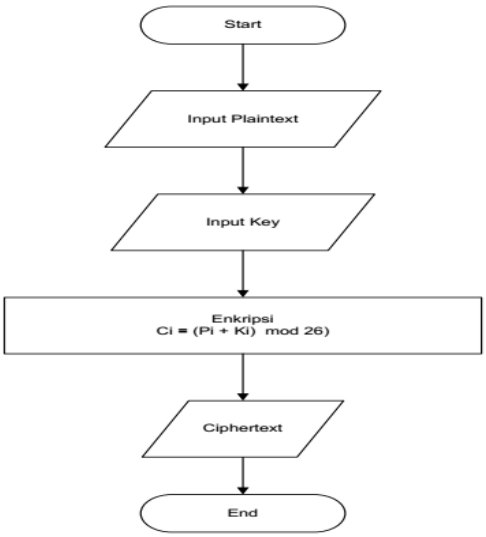
Ekstensi File

Ekstensi file merupakan sebuah penanda yang ditetapkan sebagai akhiran untuk sebuah nama file komputer. Ekstensi file memperlihatkan karakteristik dari isi file serta tujuan penggunaannya. Secara umum, ekstensi file mengandung 3 (tiga) karakter. Terdiri dari gabungan antara huruf dan angka yang secara textual mewakili jenis dari file tersebut. Ekstensi file terletak di akhir nama file dengan karakter titik sebagai pemisah keduanya. Sebagai contoh file dengan nama Musik.mp3. Ini dapat diartikan bahwa Musik adalah nama file dan mp3 adalah ekstensinya, sedangkan tanda titik digunakan sebagai pemisah diantara keduanya. Ekstensi file sering dianggap sebagai metadata yang digunakan oleh sistem operasi untuk mengetahui informasi dari file tersebut. Sebagai contoh, file dengan nama Baca.txt adalah jenis file text, sedangkan Laporan.xls merupakan file dokumen dengan jenis excel.

METODE PENELITIAN

Konsep Metode One Time Pad

Proses Enkripsi One Time Pad



Gambar 1. Flowchart proses Enkripsi OTP

Sebuah plaintext yaitu ASWIN dan memiliki sebuah kunci yaitu CRASH (panjang kunci harus sama dengan plaintext dan sebalikanya jangan ada karakter yang diulang).

Pertama kita harus mendapatkan kode ascii dari plaintext.

Tabel I Kode ASCII Plaintext

Karakter	ASCII
A	0
S	18
W	22
I	8
N	13

Hal yang sama juga harus dilakukan pada kunci yang dipilih.

Tabel II Kode ASCII Kunci

Karakter	ASCII
C	2
R	17
A	0
S	18
H	7

Rumus dari enkripsi One Time Pad yaitu :

Ci = (Pi + Ki) mod 26

Keterangan rumus :

Ci = Cipherteks (Ciphertext),

Pi = Plainteks (Plaintext),

Ki = kunci (Key).

Langkah selanjutnya yaitu plaintext dan kunci diubah menjadi angka sesuai dengan tabel yang telah diberikan, berikut ini proses enkripsinya :

C1 = (P1 + K1) mod 26

= (0 + 2) mod 26

= (2) mod 26

= 2

C1 = 2

Maka C1= 2 huruf ciphertext dengan nilai 2 adalah **C**.

C2 = (P1 + K1) mod 26

= (18 + 17) mod 26

= (35) mod 26

= (35) mod 26

= 9

C2 = 9

Maka C2= 9 huruf ciphertext dengan nilai 9 adalah **J**.

C3 = (P1 + K1) mod 26

= (22 + 0) mod 26

= (22) mod 26

= 22

C3 = 88

Maka C3= 22 huruf ciphertext dengan nilai 22 adalah **W**.

C4 = (P1 + K1) mod 26

= (8 + 18) mod 26

= (26) mod 26

= 0

C4 = 0

Maka C4= 0 huruf ciphertext dengan nilai 0 adalah **A**.

$C_5 = (P_1 + K_1) \bmod 26$

$= (13 + 7) \bmod 26$

$= (20) \bmod 26$

$= 20$

$C_5 = 20$

Maka C_5= 20 huruf ciphertext dengan nilai 20 adalah **U**.

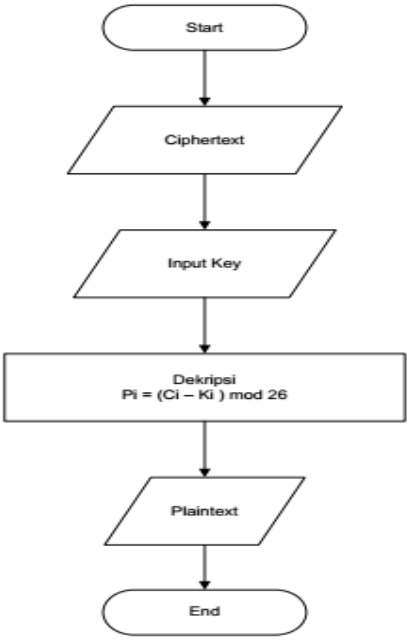
Dengan melakukan konsep yang sama maka didapatkan hasil sebagai berikut :

Plaintext = “ASWIN”

Key = “CRASH”

Ciphertext = “CJWAU”

Proses Dekripsi One Time Pad



Gambar 2. Flowchart Proses Dekripsi OTP

Ciphertext = “CJWAU”

Key = “CRASH”

Tabel kode ASCII dari ciphertext dapat dilihat dibawah ini :

Tabel III Kode ASCII Ciphertext

Karakter	ASCII
C	2
J	9
W	22
A	0
U	20

Rumus dekripsi dari One Time Pad yaitu :

Pi = (Ci – Ki) mod 26

Keterangan rumus :

Ci = Cipherteks (Ciphertext),

Pi = Plainteks (Plaintext),

Ki = kunci (Key).

Proses Dekripsi :

P1 = (C1 – K1) mod 26

= (2 – 2) mod 26

= (0) mod 26

= 0

Maka P1= 0 huruf ciphertext dengan nilai 0 adalah **A**.

P2 = (C1 – K1) mod 26

= (9 – 17) mod 26

= (-8) mod 26

= 18

Maka P2= 18 huruf ciphertext dengan nilai 18 adalah **S**.

P3 = (C1 – K1) mod 26

= (22 – 0) mod 26

= (22) mod 26

= 22

Maka P3= 22 huruf ciphertext dengan nilai 22 adalah **W**.

P4 = (C1 – K1) mod 26

= (0 – 18) mod 26

= (-18) mod 26

= 8

Maka P4= 8 huruf ciphertext dengan nilai 8 adalah **I**.

P5 = (C1 – K1) mod 26

= (20 – 7) mod 26

= (13) mod 26

= 13

Maka P5= 13 huruf ciphertext dengan nilai 13 adalah **N**.

Dengan melakukan konsep yang sama maka didapatkan hasil sebagai berikut :

Ciphertext = “CJWAU”

Key = “CRASH”

Plaintext = “ASWIN”

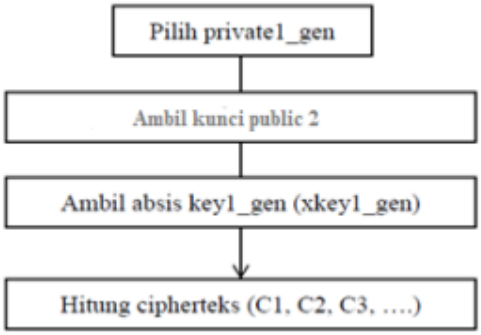
Konsep Metode Elliptic Curve Cryptography

Kriptografi kurva eliptik merupakan metode kriptografi yang menggunakan titik –titik pada kurva eliptik sebagai kunci untuk melakukan proses enkripsi dan dekripsi. Kekuatan dari kriptografi ini adalah banyaknya titik yang terdapat pada sebuah kurva dan sulitnya mengetahui kurva yang digunakan.

Kriptografi kurva eliptik menggunakan dua kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi kurva 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 dari kurva.

Proses Enkripsi Elliptic Curve Cryptography

Proses enkripsi pada kriptografi kurva eliptik tahapan – tahapan dalam melakukan proses enkripsi adalah:



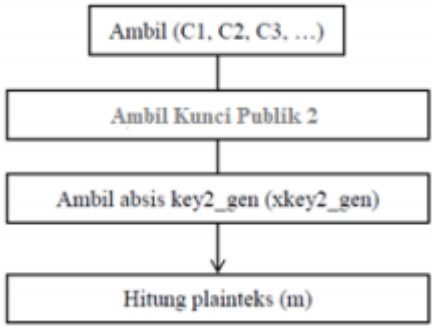
Gambar 4. Tahapan Proses Enkripsi Kriptografi Kurva Eliptik

Gambar 6. Flowchart Proses Enkripsi ECC

Proses Dekripsi Elliptic Curve Cryptography

Tahapan – tahapan dalam melakukan dekripsi pada kriptografi kurva

eliptik adalah:

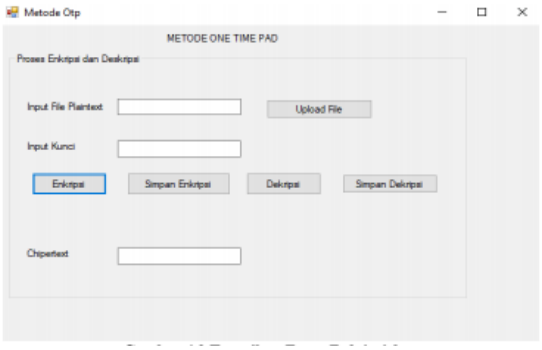


Gambar 6. Tahapan Proses Dekripsi Kriptografi Kurva Eliptik

Gambar 7. Proses Dekripsi ECC

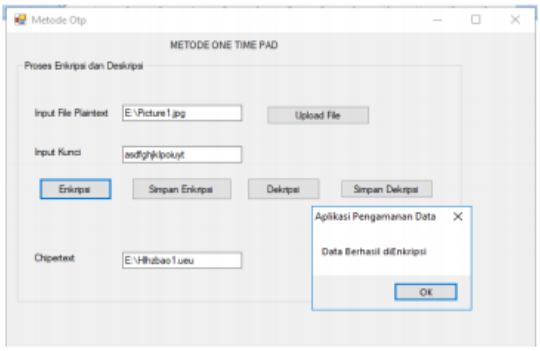
IV. HASIL DAN PEMBAHASAN

Pada tahapan ini kita akan melihat hasil dari Algoritma One Tome Pad dan ECC yang diterapkan pada sistem.



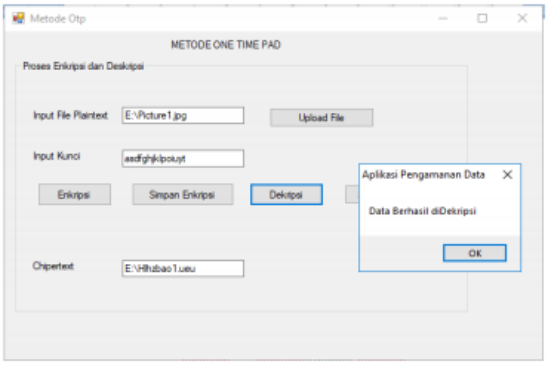
Gambar 8. Tampilan Metode OTP

Pada halaman ini, pengguna bisa memasukan file teks yang ingin dienkripsi dengan menekan tombol "Uploud File", kemudian kita memasukkan kunci, sepanjang plainteks. Selanjutnya menekan tombol enkripsi dan ciphertext akan menampilkan hasil enkripsi. Seperti terlihat pada gambar dibawah ini:



Gambar 9. Form Proses Enkripsi OTP

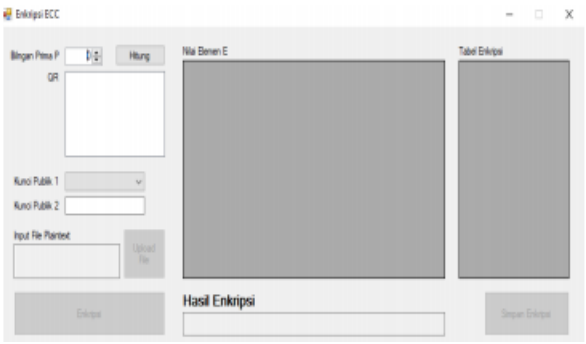
Pada halaman ini juga , pengguna memasukan file teks yang sudah dienkripsi dengan menekan tombol "Uploud File", kemudian kita memasukkan kunci, sepanjang ciphertext. Selanjutnya menekan tombol dekripsi dan plaintext akan menampilkan hasil dekripsi. Seperti terlihat pada gambar dibawah ini:



Gambar 10. Form Proses Dekripsi OTP

Tampilan Form Enkripsi Algoritma Elliptic Curve Cryptography

Pada tampilan ini, menampilkan proses enkripsi dan detil langkah – langkah perhitungan untuk proses enkripsi, seperti ditampilkan pada gambar berikut:

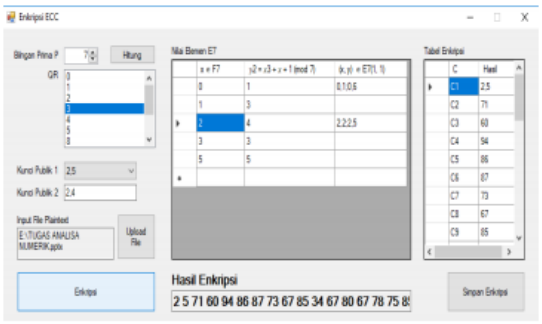


Gambar 11. Form Proses Enkripsi ECC

Pada halaman ini, pengguna bisa memasukkan sendiri sebuah bilangan prima, pengguna kemudian menghitung elemen – elemen titik yang terdapat pada kurva dengan menekan tombol hitung, detil proses perhitungan akan ditampilkan pada text area di sebelahnya.

Selanjutnya pengguna memasukan file teks yang ingin dienkripsi dengan menekan tombol “Uploud File” dimana isi dari teks yang akan dienkripsi akan langsung tampak pada textbox di sampingnya. Kemudian pengguna tinggal menekan tombol “Enkripsi” aplikasi akan mengkonversikan setiap karakter pada pesan kita menjadi ascii code, akan ditampilkan pada teks area di sebelah kanan dan hasil enkripsi akan terlihat textbox , setelah selesai dienkripsi kemudian pengguna akan menekan

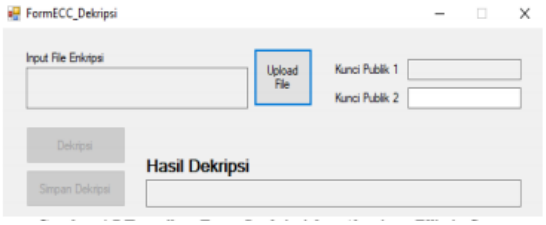
tombol “Simpan Enkripsi”. Seperti terlihat pada gambar dibawah ini:



Gambar 12. Tampilan Form Enkripsi Dan Algoritma Elliptic Curve Cryptography Setelah Semua Data Dimasukkan

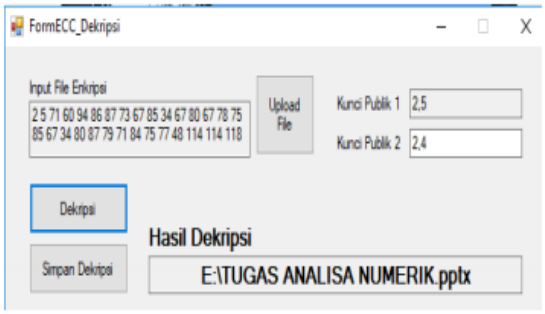
Tampilan Form Dekripsi Algoritma Elliptic Curve Cryptography

Pada form dekripsi ini, akan ditampilkan proses mendekripsikan cipherteks yang didapat dari proses sebelumnya kembali menjadi plainteks semula seperti terlihat pada gambar berikut:



Gambar 13. Tampilan Form Dekripsi Algoritma Elliptic Curve Cryptography

Pada proses deskripsi pengguna memasukan file teks yang sudah dienkripsi dengan menekan tombol “Uploud File”, kemudian pengguna memasukan kunci publik yaitu 4, 12 setelah itu tekan tombol “Dekripsi”, dan hasilnya dapat dilihat pada gambar dibawah ini:



Gambar 4.8 Tampilan Form Deskripsi Algoritma Elliptic Curve

KESIMPULAN

Setelah melakukan pengujian, maka dapat ditarik kesimpulan sebagai berikut :

1. Enkripsi plainteks dengan menggunakan Algoritma One Time Pad dapat melindungi informasi yang terdapat dalam file teks tersebut. Proses Enkripsi menggunakan One Time Pad adalah jumlah karakter kunci harus sepanjang karakter plaintext.
2. Enkripsi plainteks dengan menggunakan Algoritma Elliptic Curve Cryptography dapat melindungi informasi yang terdapat dalam file teks tersebut. Proses enkripsi untuk merubah satu titik ke titik yang lain yang digunakan sebagai cipherteks (sandi) digunakan algoritma ECC dan untuk proses dekripsi merubah satu titik (cipherteks) ke titik semula (plainteks) digunakan algoritma ECC.
3. Untuk proses enkripsi menggunkan algoritma One Time Pad, semua jenis file dapat diproses dengan baik, sedangkan untuk algoritma Elliptic Curve Cryptography beberapa file seperti gambar dan video tidak dapat di enkripsi dengan baik.
4. Untuk keamanan data menggunakan algoritma Elliptic Curve Cryptography aman sekali karena mengunakan kunci publik dan privat dan untuk algoritma One Time Pad cukup aman karena kunci sama plainteksnya berbeda.

DAFTAR PUSTAKA

[1]Aprilia, Shieny. 2009 *Analisis dan Implementasi Elliptic Curve Cryptography dan Aplikasinya pada Sistem File Save Game Nintendo Wii*. Departemen Teknik Informatika – ITB

[2]Garefalakis,Theodoulos. *Primality Testing, Integer Factorization, and Discrete Logarithms*. 2000. Toronto:Department of ComputerScience, University of Toronto.

[3]Indriani, Susi. 2011. *Kriptografi Kurva Eliptik dengan Proses Pertukaran Kunci Diffie-Hellman*. Skripsi. Medan, Indonesia : Universitas Sumatera Utara.

[4]Munir Rinaldi, 2006, *Kriptografi*, Informatika Bandung.

[5]Schneier, B. 1997. *Applied Cryptography, 2nd Edition*. New York: John-Willey & Sons.

[6]Sentot ,Kromodimoeljo , 2009, *Teori dan Aplikasi Kriptografi*.

[7]Tirtawinata, Kevin. 2010. *Studi dan Analisis Elliptic Curve Cryptography*. Bandung:STEI – ITB