IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) UNTUK PENGAMANAN *FILE* BERBASIS WEB

Yoga Nugroho[1*], Painem Painem[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]yoganugroho.k1@gmail.com, [2]painem@budiluhur.ac.id
(* : corresponding author)

Abstrak- PT. KMK GLOBAL SPORTS adalah sebuah perusahaan yang bergerak dibidang Industri Manufaktur pembuatan alas kaki. PT. KMK GLOBAL SPORTS hampir setiap hari melakukan produksi untuk proses pembuatan alas kaki seperti sepatu maupun sandal. Dalam proses pembuatan perencanaan produk alas kaki didesain oleh sang desainer untuk dilakukan proses pembuatan alas kaki tersebut, kemudian hasil dari gambar desain tersebut sangatlah rahasia. Oleh karena itu dibutuhkan aplikasi pengamanan data untuk menginput dan menyimpan data-data dengan aplikasi yang menggunakan pengamanan salah satunya menggunakan teknik kriptografi. Jika informasi tidak diamankan, maka dapat mempermudah orang lain untuk merusak atau mengambil informasi atau dokumen rahasia kemudian mereka melakukan modifikasi, pembocoran terhadap isi dari *file* tersebut dan mendistribusikannya, dengan menggunakan teknik kriptografi *Elliptic Curve Cryptography* (ECC) untuk pengamanan data ini untuk mengamankan datanya supaya isi dari data tersebut tidak diketahui oleh pihak yang tidak memiliki kepentingan yang memberikan kemudahan kepada *user* terhadap data tersebut serta dapat dimanfaatkan untuk mengamankan data. Aplikasi pengamanan *file* dengan menggunakan algoritma kriptografi *Elliptic Curve Cryptography* (ECC) dapat diimplementasikan dalam bahasa *PHP* mampu mengamankan *file yang berextention pdf, docx, doc, pptx, jpg, dan xlsx* dengan size maksimal yaitu 2048mb. Proses pengujian pada penelitian ini menggunakan 5 file yang berbeda ukuran dan extention, setelah dilakukan pengujian program dengan melihat *size* dari *file* baik yang sudah dienkripsi atau yang sudah didekripsi untuk ukuran *size file* tidak ada perubahan.

Kata Kunci: algoritma *elliptic curve cryptography* (ECC), kriptografi, *file*.

IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ALGORITHM FOR WEB-BASED FILE SECURITY

Abstract- *PT. KMK GLOBAL SPORTS is a company engaged in the Manufacturing Industry of making footwear. PT. KMK GLOBAL SPORTS almost every day produces for the process of making footwear such as shoes and sandals. In the process of making footwear product planning designed by the designer to carry out the process of making the footwear, then the results of the design drawings are very confidential. Therefore, a data security application is needed to input and store data with applications that use security, one of which uses cryptographic techniques. If the information is not secured it can make it easier for other people to destroy or take confidential information or documents then they modify, leak the contents of the file and distribute it. by using the Elliptic Curve Cryptography (ECC) cryptographic technique for securing this data to secure the data so that the contents of the data are not known by parties who have no interest which makes it easy for the user to the data and can be used to secure the data. File security applications using the Elliptic Curve Cryptography (ECC) cryptographic algorithm can be implemented in PHP, able to secure files with the extension pdf, docx, doc, pptx, jpg, and xlsx with a maximum size of 2048mb, after testing the program by looking at the size of the file both encrypted and decrypted for the size of the file there is no change.*

Keywords*: elliptic curve cryptography (ECC) algorithm, cryptography, file.*

1. PENDAHULUAN

Dengan pesatnya teknologi memungkinkan manusia untuk bertukar data tanpa memandang jarak, bertukar informasi, ataupun berkomunikasi. Sebuah perusahaan juga harus mampu memanfaatkan kemajuan teknologi dan informasi yang saat ini tengah terjadi sebagai salah satu sarana pendukung proses bisnis yang dimilikinya. Perusahaan yang mampu melakukan pemanfaatan teknologi dan informasi secara maksimal, tentu saja dapat meningkatkan daya saing dan kualitas dari perusahaan tersebut. Selain itu, hal tersebut dapat meningkatkan manajemen pengolahan perusahaan agar lebih baik dan adanya peningkatan dari segi kualitas pelayanan terhadap pelanggan. Tidak terkecuali berdasarkan perkembangan teknologi saat ini manusia banyak yang bergantung pada teknologi informasi.

Begitu banyak kasus penyadapan terhadap suatu informasi telah membuat para peneliti berpikir keras untuk menggunakannya. Untuk meminimalkan kemungkinan terjadinya tindak kejahatan di *internet* ini diperlukan teknologi keamanan informasi, yaitu sistem enkripsi (penyandian)[1]. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah kriptografi [2]. Dengan kriptografi, informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja [3].

Dalam kriptografi ada istilah yang disebut dengan enkripsi (*encryption*) yaitu proses penyamaran data dari plaintext (data asli) menjadi chipertext (data tersandi) dan dekripsi (*decryption*) yaitu proses pengembalian ciphertext menjadi plaintext kembali [4].

Algoritma kriptografi kurva eliptik mempunyai keuntungan jika dibandingkan dengan algoritma kriptografi kunci publik lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama [6]. *Elliptic Curve Cryptography* (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik berdasarkan pada struktur aljabar dari kurva elips pada daerah finite [7].

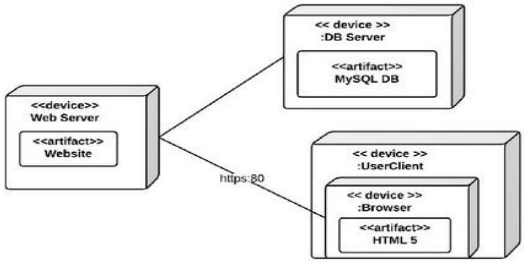
Perusahaan akan menyimpan dokumen digital atau *file* pada komputer tanpa adanya pengamanan secara baik. Untuk menjaga *file* atau dokumen tersebut aman dan memungkinkan tidak terjadinya kebocoran data atau pencurian data oleh orang yang tidak berhak maka dibutuhkan sebuah pengamanan atau dengan menggunakan teknik kriptografi untuk keamanan, dokumen atau *file* dalam bentuk *plainteks* akan diubah menjadi *ciphertext* agar tidak bisa dibaca.

Dalam dunia keamanan komputer ada banyak jenis algoritma kriptografi atau metode pengamanan data, salah satunya yaitu algoritma ECC Berbasis web ini merupakan sebuah sistem kriptografi dengan kunci public dengan memanfaatkan persamaan eliptik kurva. Fungus dari enkripsi yaitu akan merubah data atau teks sehingga tidak bisa dibaca oleh orang yang tidak punya hak akses yang disebut dengan chipertext untuk mengembalikan data tersebut agar bisa dibaca kembali maka dibutuhkan proses dekripsi fungsi tersebut untuk menjadikan *chipertext* menjadi *plaintext*.

2. METODE PENELITIAN

2.1 *Deployment* Diagram

Deployment diagram adalah suatu diagram yang menggambarkan perangkat keras dan perangkat lunak secara detail yang tersebar pada suatu infrastruktur sistem. Di dalam *diagram deployment* ini dijelaskan masing-masing komponen dan kemampuan jaringan tersebut bekerja [8].



Gambar 1. *Diagram Deployment*

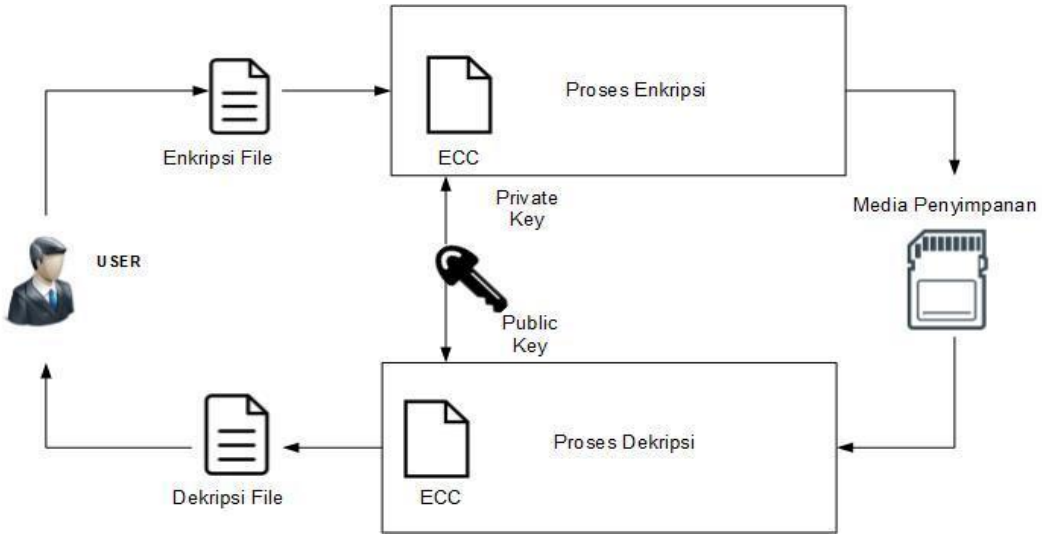
2.2 Data Penelitian

Pada bab ini dijelaskan tentang penelitian pada sistem Pengarsipan *file* pada PT. KMK Global Sports berikut berdasarkan menu item pada sistem:

a. Pada Data menu item terdapat dokumen yang dapat disimpan pada PT. KMK GLOBAL SPORTS *file* pdf, jpeg, docx, pptx.
b. Pada salah satu contoh sumber data yang digunakan dalam data penelitian ini berupa Tabel penyimpanan dokumen.
c. Pada Tabel 3.1 merupakan data dokumen pada PT. KMK GLOBAL SPORTS.
d. sebagai data penelitian dalam pembuatan pengamanan data yang penting yang telah di disimpan pada database PT. KMK GLOBAL SPORTS.

2.3 Penerapan Metode

Pada tahap penerapan metode ini menjelaskan tentang alur penggunaan metode yang akan digunakan, dan berikut alur yang digunakan pada penerapan metode, alur proses sistem. Pada tahap alur Proses Sistem ini dianalisis dalam sebuah alur. Pada tahap awal alur proses sistem enkripsi dan dekripsi dokumen harus memiliki seorang *user* untuk menjalankan program, selanjutnya *user* harus *login* terlebih dahulu, setelah itu *user* dapat menjalankan web enkripsi dan dekripsi dokumen. Berikut tahapan seperti pada Gambar 3.1. Untuk melihat proses dari Kriptografi dengan metode *Elliptic Curve Cryptography* (ECC) Untuk Pengamanan *File* Berbasis Web dapat dilihat dalam skema proses aplikasi berikut, dapat dilihat pada gambar 2.



Gambar 2. Metode *Elliptic Curve Cryptography* (ECC)

Penggunaan kurva elips dalam kriptografi dicetuskan oleh Neal Koblitz dan victor S. Miller pada tahun 1985. Kurva elips juga digunakan pada beberapa algoritma pemfaktoran integer yang juga memiliki aplikasinya dalam kriptografi, seperti *Lenstra Elliptic Curve Factorization* [9]. Algoritma kunci publik berdasarkan pada variasi perhitungan matematis yang terbilang sangat sulit dipecahkan tanpa pengetahuan tertentu mengenai bagaimana perhitungan tersebut dibuat [10]. Kurva elips dapat ditulis dengan perhitungan matematis sebagai berikut:

$$y^2 = x^3 + ax + b \pmod{p}, \quad (1)$$

a. Yang dalam hal ini parameter a, b dan bilangan prima (*p*).
b. Grup Eliptik yang dihitung dari persamaan kurva eliptik
c. Titik basis B(*x*,*y*) yang dipilih dari grup eliptik untuk operasi kriptografi.
d. *n* = order dari *B* yaitu bilangan bulat positif terkecil yang memenuhi *n*B=0*

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.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Metode

Dalam tahap ini dilakukan pembuatan aplikasi pengamanan *file* dan menerapkan metode enkripsi dengan metode ECC menggunakan bahasa PHP dan HeidiSQL. Arsitektur system yang dibuat terdiri dari login, halaman utama, master user, enkripsi, dekripsi dan menu ubah password, aplikasi ini dapat mengamankan *file* ber-extention pdf, xlsx, pptx, doc, docx, dan jpg, namun aplikasi ini hanya bisa memproses dengan maksimal ukurannya yaitu 2048mb.

3.2 Spesifikasi Database

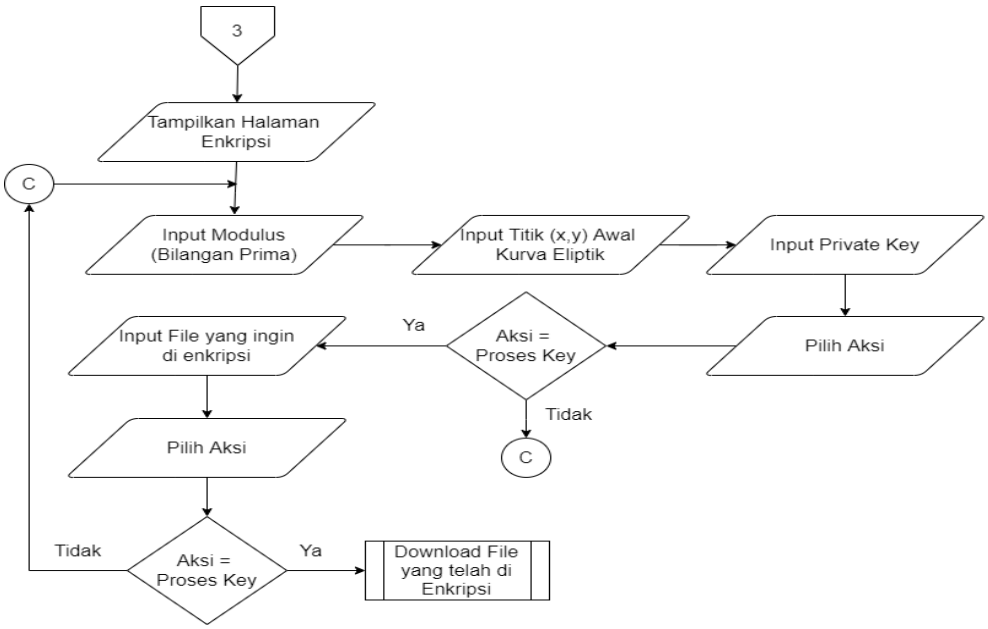
Berikut adalah Spesifikasi Database yang menyimpan *record-record* yang telah dimanipulasi oleh program sesuai spesifikasinya masing-masing. Tabel user yang terdapat di Tabel 1 dalam basis data yang digunakan. DBMS (*Database Management System*) yang digunakan dalam program ini adalah HeidiSQL dapat dilihat pada tabel 1.

Tabel 1. Spesifikasi Database

No	Nama Field	Type	Length	Keterangan
1	kd_usr	Varchar	7	Kd Pengguna
2	email	Varchar	100	Email Pengguna
3	pass_usr	text	-	Password Pengguna
4	nm_usr	Varchar	100	Nama Pengguna
5	lvl_usr	Varchar	1	Level Pengguna
6	tgl_dbat	Datetime	-	Tanggal Pengguna Buat
7	dbat_olh	Varchar	7	Dibuat Oleh Pengguna
8	tgl_dbah	Datetime	-	Tanggal Pengguna Ubah
9	dbh_olh	Varchar	7	Diubah Oleh Pengguna
10	sts_usr	Varchar	1	Status Pengguna

3.2.1 *Flowchart* Enkripsi ECC

Untuk lebih jelasnya berikut adalah proses dari *flowchart* proses enkripsi ECC, *Flowchart* proses Enkripsi ECC menjelaskan alur proses atau cara kerja algoritma ECC untuk menghasilkan *Plaintext.*



Gambar 3. *Flowchart* Proses Enkripsi ECC

Misalnya sebuah karakter yang sudah direpresentasikan menjadi titik P_m (x,y). Langkah-langkah enkripsi sebagai berikut:

a. Pengirim memilih bilangan acak *r* dengan syarat *r* terletak di dalam selang [1, *n*-1].
b. Pengirim menghitung *ciphertext* dari pesan *Pm* dengan menggunakan kunci publik penerima (*Pb*) seperti persamaan 2 dan 3.

$$C_1 = \mathrm{r} \,.\, \mathrm{B} \quad (2)$$

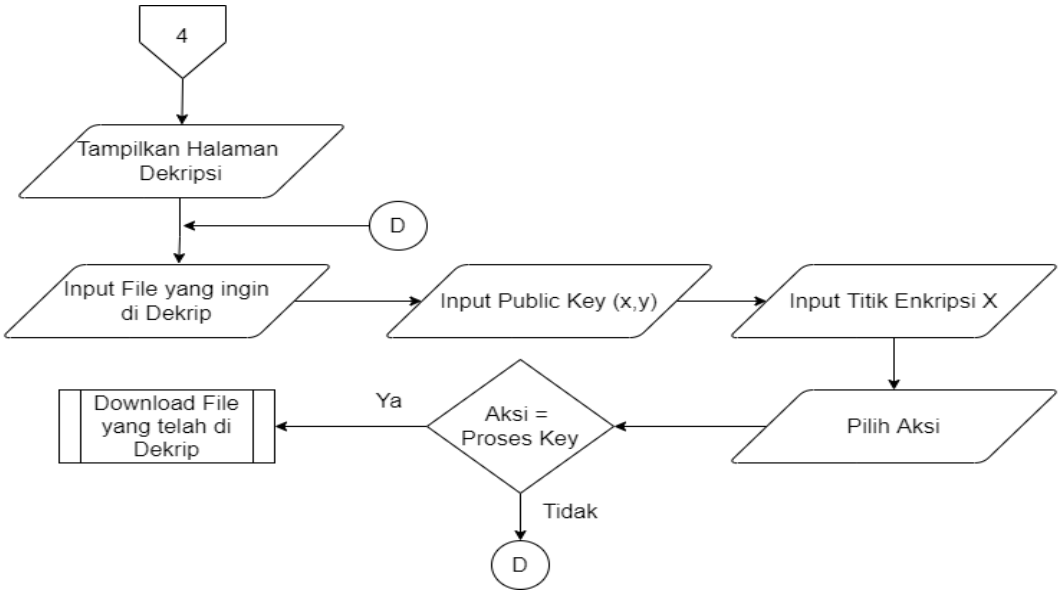
$$C_2 = P_m + \mathrm{r} \,.\, P_B \quad (3)$$

Ciphertext adalah pasangan titik $[C_1, C_2]$ atau ditulis pada persamaan 4.

$$P_c=[C_1, C_2]=[(r.B),(P_m+r.P_B)] \quad (4)$$

3.2.2 *Flowchart* Dekripsi ECC

Flowchart proses Dekripsi ECC menjelaskan alur proses atau cara kerja algoritma ECC untuk menghasilkan *Plaintext*. Untuk lebih jelasnya berikut adalah proses dari *flowchart* proses dekripsi ECC.



Gambar 4. *Flowchart* Proses Dekripsi ECC

Penerima menggunakan kunci privatnya (*d2*). Penerima melakukan langkah-langkah dekrips sebagai berikut:

a. Penerima menghitung hasil kali komponen pertama dari *P*c , yaitu *C1 = r . B*, dengan kunci privatnya, *d*2 sebagai berikut: *d2 . C1*.
b. Penerima kemudian mengurangkan komponen kedua dari *PC*, yaitu *C2 = P m + r . PB*, dengan hasil kali dari langkah 1 di atas seperti persamaan 5.

$$(P_m + r.\ P_B) - d_2.\ C_1 = P_m + r(d_2\ .\ B) - d_2(r.\ B) = P_m \quad (5)$$

Pengurangan 2 buah titik *-Q* sama dengan menjumlahkan *P* dengan hasil pencerminan *Q* terhadap sumbu *x*, seperti persamaan 6.

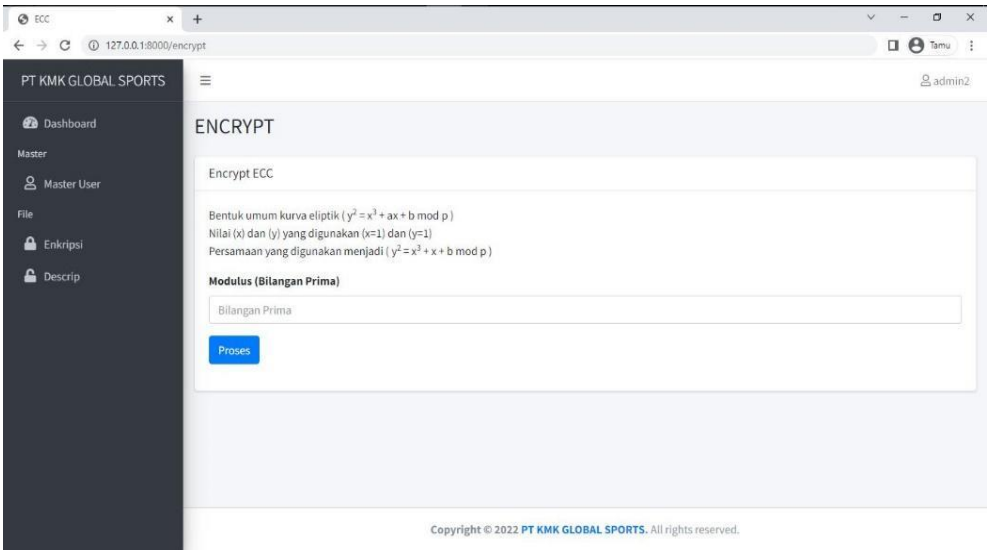
$$P - Q = P + (-Q) \quad (6)$$

yang dalam hal ini, jika $Q = (x,y)$, maka digunakan persamaan 7.

$$- Q = P + (-Q) \quad (7)$$

3.2.3 Proses Enkripsi *File*

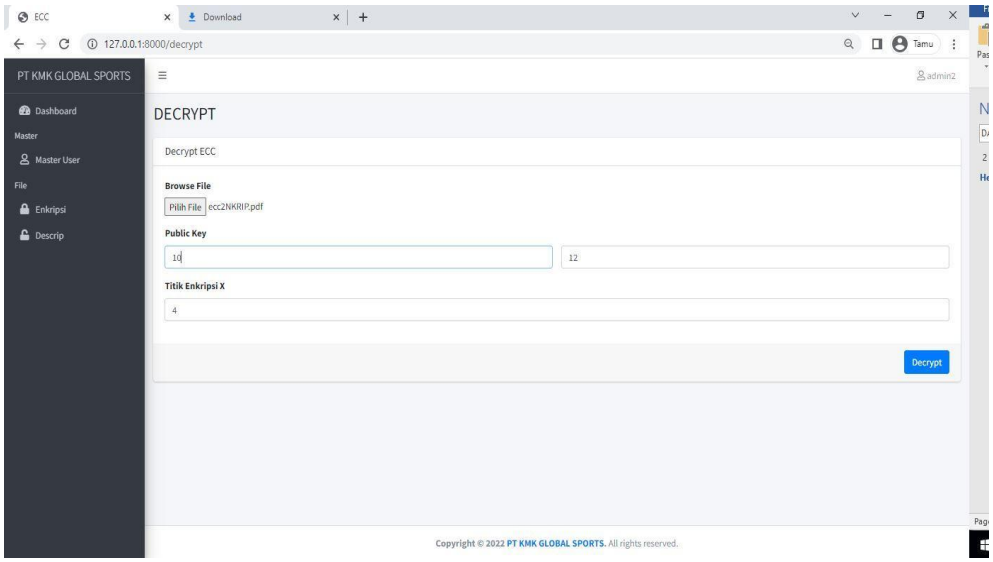
Proses enkripsi dilakukan ketika *user* melakukan klik tombol menu enkripsi. Kemudian *user* memasukan bilangan prima setelah itu klik proses maka bilangan prima akan terbuat secara otomatis, berikut Gambar 3 proses enkripsi.



Gambar 5. Proses Enkripsi *File*

3.2.4 Proses Dekripsi *File*

Proses dekripsi dilakukan ketika *user* melakukan klik tombol menu dekripsi. Kemudian user melakukan *upload file* yang akan didekripsi setelah itu *user* memasukan public *key* dan nilai titik enkripsi x, proses dekripsi dengan algoritma ECC akan bertransformasi menjadi teks yang dapat dibaca (*plaintext*), berikut Gambar 4 hasil dekripsi.

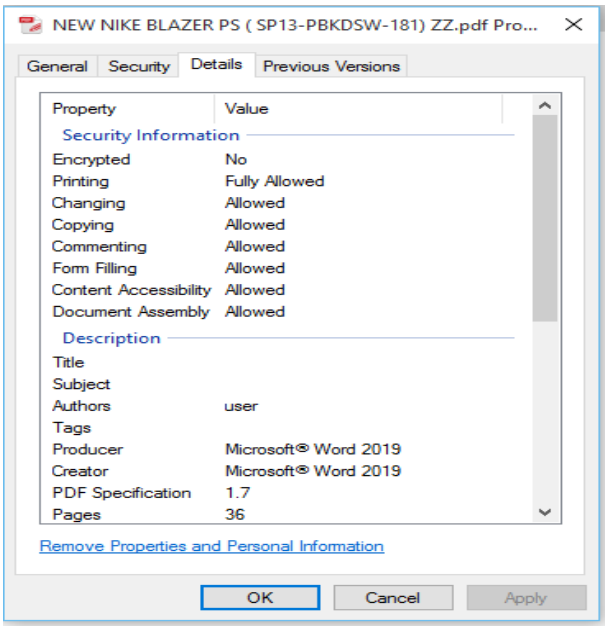


Gambar 6. Proses Dekripsi *File*

3.2.5 Pengujian Program

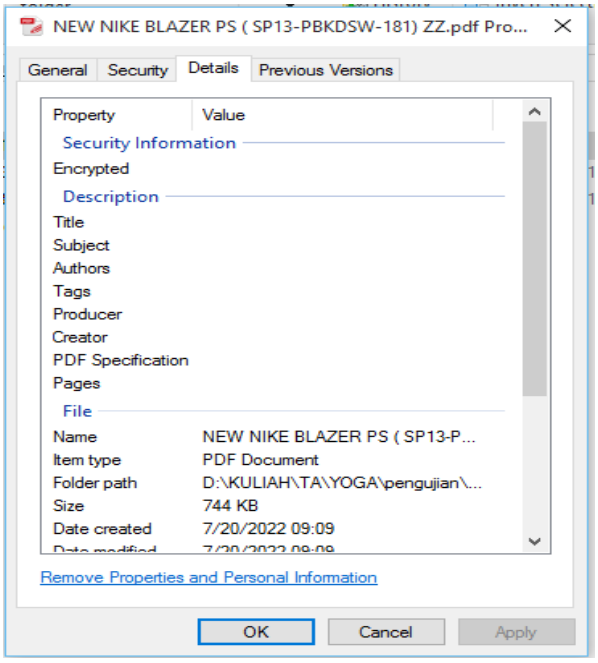
Pengujian aplikasi yang telah dibuat perlu dilakukan untuk memastikan keberhasilan jalannya aplikasi tersebut. Jika tidak diuji terlebih dahulu, bisa saja aplikasi tersebut gagal saat digunakan.

a. Pengujian *File* dengan spesifikasi Struktur *File*
   Untuk membuktikan bahwa *file* disimpan sudah dienkripsi dapat dilihat pada Gambar 5 dibawah ini. Terlihat informasi *security* enkripsi yang berarti bahwa *file* tersebut sudah dienkripsi.



Gambar 7. Tampilan Struktur File PDF Setelah Proses Enkripsi

Sedangkan Gambar 6 dibawah ini memperlihatkan adanya informasi *security file* jika ada deskripsinya enkripsi no yang berarti bahwa *file* tersebut belum dienkripsi.



Gambar 8. Tampilan informasi security file

b. Tabel Pengujian Metode *Black Box Testing*

Dalam tabel pengujian ini akan dibahas hasil proses menu melalui pengujian black box testing yang dilakukan setelah semua kebutuhan perangkat lunak maupun perangkat keras terpenuhi, pengujian aplikasi dapat dilihat pada tabel 2.

Tabel 2. Pengujian *Blackbox Testing*

No	Rancangan Proses	Hal yang diharapkan	Hasil	Keterangan
1	Mengisi *menu login*	Masuk ke halaman *Home*	Selesai	Jika di *Input* benar
2	Klik Menu *Dashbord*	Masuk Kehalaman *Dashbord*	Selesai	Tampil Halaman *Dashbord*
3	Klik menu Master	Masuk Kehalaman Master dan memiliki *form* tambah *user*, hapus *User*, *R*eset *user*, dan *Update User*	Selesai	Tampil Halaman Master *User*
4	Klik *Form* Menu Tambah *User*	Masuk ke menu Tambah User	Selesai	Tampil Halaman *Form* Tambah *User*
5	Klik *Form* Menu Hapus *User*	Masuk ke *Form* Hapus *User*	Selesai	Tampil Halaman *menu* Hapus *User*
6	Klik *Form* Menu *Update User*	*Masuk ke form Update User*	Selesai	Tampil Halaman *Form* Update *User*
7	Klik *Form* Menu Reset *User*	Masuk ke *Form* Reset *User*	Selesai	Tampil Halaman *Form* Reset *User*
8	Klik menu Enkripsi	Masuk ke Form Enkripsi	Selesai	Tampil Halaman *Form* Enkripsi *File*
9	Klik Menu Dekripsi	Masuk ke Form Dekripsi	Selesai	Tampil Halaman *Form* Dekripsi *File*
10	Klik Menu *Change Password*	Masuk Menu *Change Password*	Selesai	Tampil Halaman Form *Change Password*

c. Tabel Pengujian *File* Untuk Proses Enkripsi

Dibawah ini adalah tabel pengujian yang akan dibahas mengenai hasil antara proses-proses pada tabel 3 proses enkripsi *file* dan pada tabel 4 proses dekripsi dibawah ini.

Tabel 3. Hasil Pengujian Proses Enkripsi

No	Jenis *File*	Nama *File*	Ukuran *File* Sebelum di Enkripsi	Ukuruan *File* Setelah dienkripsi	Status
1	Pdf	NEW NIKE BLAZER PS (SP13-PBKDSW-181) ZZ	745kb	745kb	Berhasil
2	Docx	NIKE BLAZER CVS PS (SP13-PBKDSW-181) Z1 extrim	1764kb	1764kb	Berhasil
3	pptx	Nike Huarache Run GS(99802)_FA14_Mesh_#475454_ZZ.DXF	1414kb	1414kb	Berhasil
4	jpeg	PFC Nike Court Borough Low(120717)_SP17_LEA_#641379_ZZ NEW Untuk LEA	66kb	66kb	Berhasil

Tabel 4. Hasil Proses Dekripsi

No	Jenis *File*	Nama *File*	Ukuran *File* Sebelum di Enkripsi	Ukuruan *File* Setelah dienkripsi	Status
1	Pdf	NEW NIKE BLAZER PS (SP13-PBKDSW-181) ZZ	745kb	745kb	Berhasil
2	Docx	NIKE BLAZER CVS PS (SP13-PBKDSW-181) Z1 extrim	1764kb	1764kb	Berhasil
3	pptx	Nike Huarache Run GS(99802)_FA14_Mesh_#475454_ZZ.DXF	1414kb	1414kb	Berhasil
4	jpeg	PFC Nike Court Borough Low(120717)_SP17_LEA_#641379_ZZ NEW Untuk LEA	66kb	66kb	Berhasil

4. KESIMPULAN

Dari hasil aplikasi yang dikembangkan dan analisis terhadap masalah terdapat beberapa kesimpulan, antara lain:

a. Aplikasi pengamanan *file* dengan menggunakan bahasa php dapat menggunakan metode Algoritma ECC yang dapat dijalankan.
b. Aplikasi ini dapat mengamankan data yang berupa file ber-extention pdf, xls, xlsx, doc, docx, jpg dan pptx pada PT KMK Sports dengan teknik kriptografi menggunakan metode ECC sehingga file yang terenkripsi sulit untuk dibaca.

UCAPAN TERIMA KASIH

Orang tua, keluarga, saudara, Bapak Dr. Ir. Wendi Usino, M.Sc, MM selaku Rektor Universitas Budi Luhur**,** Bapak Dr. Deni Mahdiana, M.M., M.Kom. selaku Dekan Fakultas Teknologi Informasi Universitas Budi

Luhur, Bapak Dr. Indra, S.Kom., M.T.I. selaku ketua Program Studi Teknik Informatika pada Fakultas Teknologi Informasi Universitas Budi Luhur, Ibu Painem, M.Kom. selaku dosen Pembimbing, Seluruh pegurus PT. KMK Global Sports yang telah mengizinkan saya melakukan riset di PT. PT. KMK Global Sports.

DAFTAR PUSTAKA

[1] Brahmana Putra, A.B,. Kusyanti, A., & Data, M. Implementasi Algoritme Grain V1 Untuk Enkripsi Gambar Pada Aplikasi Berbasis Web. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* , vol. 2, no. 12, pp. 7157-7164, 2018.

[2] Santoso. H., & Siambaton, Z. Aplikasi Pengamanan Ekstensi *File* Menggunakan Kriptografi *One Time Pad* (Otp) Dan *Elliptic Curve Cryptography* (Ecc). *JISTech*, vol. 5, no. 1, pp. 22-38, 2020.

[3] E. I. Sari, "Perancangan Aplikasi Kriptografi Asimetris Dengan Menerapkan Metode *Elliptic Curve Cryptography*," *MEANS: Media Informasi Analisa dan Sistem*, vol. 3, no. 1, pp. 24-28, 2018.

[4] Y. Wiharto and A. Irwan, "Enkripsi Data Menggunakan *Advanced Encryption Standard* 256," *Jurnal Kilat*, vol. 7, no. 2, pp, 91-99, 2018.

[5] Y. Putra, Y. Yunus and Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma *Advanced Encryption Standard* (AES) terhadap Seragan *Cross Site Scripting*," *Jurnal Sistim Informasi dan Teknologi*," vol. 3, no. 2, pp. 56-63, 2021.

[6] Saepulrohman, A, & Negara, T. P. Implementasi Algoritma Tanda Tangan Digital Berbasis Kriptografi Kurva Eliptik Diffie-Hellman, *KOMPUTASI*, vol.18, no.1, pp. 22– 28, 2021.

[7] H. Santoso and M. Z. Siambaton, "Aplikasi Pengamanan Ekstensi *File* Menggunakan Kriptografi *One Time Pad* (Otp) dan *Elliptic Curve Cryptography* (Ecc)," *JISTech: Journal of Islamic Science and Technology*, vol. 5, no. 1, pp. 22-38, 2020.

[8] M. A. Putra, et al, "Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen File Dengan Algoritma *Triple* DES Berbasis Web," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 57-69, 2022.

[9] U. W. Latifah and P. W. Prasetyo, "Implementasi Kriptografi Kurva Eliptik Elgamal Di Lapangan Galois Prima Pada Proses Enkripsi Dan Dekripsi Berbantuan Software Python," *Journal of Fundamental Mathematics and Applications (JFMA)*, vol. 4, no. 1, pp. 45-60, 2021.

[10] G. I. Taopan, M. Boru and A. Fanggida, "Pengamanan Portable Document Format (Pdf) Menggunakan Algoritma Kriptografi Eliptik," J-*ICON*, vol. 10, no. 1, pp. 47-54, 2022.