PENGAMANAN *PORTABLE DOCUMENT FORMAT* (PDF) MENGGUNAKAN ALGORITMA KRIPTOGRAFI ELIPTIK

Gever Imanuel Taopan[1], Meiton Boru[2] dan Adriana Fanggidae[3]

[1,2,3] Program Studi Ilmu Komputer, Fakultas Sains dan Teknik, Universitas Nusa Cendana, Kupang, Indonesia
[1]Email: taopangever630@gmail.com
[2]Email: meitonboru@staf.undana.ac.id
[3]Email: adrianafanggidae@staf.undana.ac.id

ABSTRAK

Penggunaan dokumen digital telah banyak digunakan pada berbagai kalangan, organisasi ataupun instansi. Salah satu dokumen digital yang sering digunakan adalah portable document format (PDF). Diperlukan sebuah algoritma yang diterapkan dalam perangkat lunak, sehingga dapat mengamankan dokumen tersebutdari pihak-pihak yang dapat merugikan. Salah satu algoritma yang dapat digunakan adalah *elliptic curve cryptography* (ECC). ECC mempunyai keunggulan pada tingkat keamanan sebuah data dengan kunci yang tidak terlalu panjang. Enkripsi dilakukan pada 16 *Byte* dari *header* PDF dengan menggunakan 7 parameter ECC yaitu bilangan prima, koefisien A, koefisien B, titik basis, kunci rahasia, kunci publik dan K. Bilangan prima yang digunakan yaitu 67, 71, 151, 199, 229, dan 239. Sedangkan parameter yang lain dipilih secara *random.* Setiap bilangan prima tersebut dilibatkan untuk enkripsi 4 jenis ukuran *file*, yaitu 1KB–2MB , 2MB–4MB, 4MB–6MB, dan lebih besar dari 6MB, di mana masing-masing jenis ukuran *file* memiliki 5 *file* yang berbeda. Dilakukan 3 kali percobaan untuk setiap *file*, sehingga terdapat 360 percobaan. Dari 360 percobaan tersebut, terdapat ±53,33% masuk pada kelas korelasi yang sangat rendah, ±34,72% pada kelas rendah, ±10% pada kelas sedang dan ±1,94% pada kelas kuat. Secara keseluruhan rata-rata korelasi yang dihasilkan sebesar 0,212282779. Oleh karena itu, penggunaan algoritma ECC untuk enkripsi *header* PDF cukup baik. Pada proses enkripsi juga terjadi kenaikan ukuran *file* sebesar 64 *Byte*, akan tetapi saat dekripsi ukuran *file* kembali ke ukuran semula.
Kata kunci: ECC, Prima, *header* PDF

ABSTRACT

The use of digital documents has been widely used in various groups, organizations or agencies. One of the digital documents that often used is the Portable Document Format (PDF). An algorithm needed to implemented in the software, so that it can secure these documents from parties who can harm. One of the algorithms that can be used is Elliptic Curve Cryptography (ECC). ECC has an advantage on the level of data security with a key not too long. Encryption carried out on a 16 Bytes PDF header using 7 ECC parameters, prime number, coefficient A, coefficient B, base point, secret key, public key and K. The prime numbers used are 67, 71, 151, 199, 229, and 239. Other parameters chosen randomly. Each prime number involved for encryption of 4 types of file size, 1KB-2MB, 2MB-4MB, 4MB-6MB, and more than 5MB, where each type of file size has 5 different files. There were 3 trials for each file, so there were 360 trials. The 360 trials, there were ±55.33% in the very low correlation class, ±34.72% in the low class, ±10% in the medium class and ±1.94% in the strong class. Overall the average correlation generated is 0.212282779. Therefore, the use of the ECC algorithm for encryption the header of PDF is quite good. In the encryption process there is also an increase in file size by 64 Bytes, but when decrypting the file size returns to its original size.
Key words**:** ECC, *Prime*, PDF *header*

1. PENDAHULUAN

Dalam era teknologi 4.0, penggunaan dokumen elektronik sebagai tempat penyimpanan berbagai informasi penting telah dianggap sebagai sesuatu yang lazim dilakukan. Hal ini karena terdapat berbagai manfaat yang dirasakan, baik dalam segi waktu ataupun biaya [1]. Terdapat beberapa dokumen elektronik yang umumnya dipakai pada setiap instansi, perusahaan ataupun organisasi untuk meningkatkan kualitas penyimpanan ataupun penyajian informasi, dokumen elektronik tersebut berekstensi .docx, .xls, .pptx dan .pdf [2]. Salah satu dokumen elektronik yang cukup diminati adalah PDF. Keunggulan utama dari dokumen elektronik tersebut dapat dibuka di komputer manapun atau bahkan *smartphone* tanpa adanya perubahan pada data atau isinya.

Setiap informasi atau data yang dianggap penting bagi sebuah instansi, perusahaan ataupun

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)

organisasi yang disimpan dalam dokumen elektronik PDF, sudah tentu tidak ingin diakses secara bebas bagi orang-orang yang tidak berwenang. Oleh karena itu, dibutuhkan sebuah metode yang dapat mengamankan dokumen elektronik tersebut, sehingga hanya orang-orang yang memiliki kewenangan yang dapat mengaksesnya. Ilmu dan seni untuk menjaga kerahaisaan data atau dokumen yang disebut kriptografi, dapat digunakan untuk data atau dokumen tersebut [3]. Salah satu algoritma kriptografi yang dapat diterapkan untuk mengamankan PDF adalah algoritm kriptografi kurva eliptik atau *elliptic curve cryptography* (ECC). Sebelumnya telah ada penelitian yang menggunakan algoritma MD5 dan RC4 untuk mengamankan PDF [4].

Pengamanan PDF menggunakan ECC dilakukan dengan cara mengenkripsi 16 *Byte* karakter dari *header* struktur PDF. Dalam penelitian ini akan diuji pengaruhnya bilangan prima dan ukuran *file* terhadap nilai korelasi yang dihasilkan

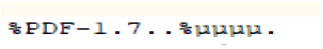
2. MATERI DAN METODE

Dokumen

Dokumen merupakan sekumpulan informasi penting yang ditulis dengan tangan ataupun menggunakan komputer. Pada era teknologi 4.0 saat ini, sudah menjadi hal yang sangat lazim bahwa pembuatan dokumen sering dilakukan menggunakan komputer, sehingga muncul sebutan bagi dokumen tersebut, yaitu *e-document* atau dokumen elektronik.

Portable Document Format

Portable Document Format (PDF) merupakan salah satu dokumen elektronik yang umum dipakai pada perangkat teknologi komputer ataupun *mobile.* Salah satu keunggulan dari dokumen elektronik tersebut adalah tidak adanya perubahan terhadap data ataupun isinya ketika dibuka pada komputer ataupun *mobile* yang berbeda. Seperti dokumen elektronik lainnya, PDF memiliki struktur *file*, yaitu *header, body area/ object, cross reference table* dan *trailer*. Dalam penelitian ini difokuskan 16 *Byte* atau 16 karakter dari *header*, yang mana akan dienkripsi menggunakan ECC. *Header* berisikan informasi tentang spesifikasi *file* PDF. Contoh 16 *Byte* dari *header* PDF dapat dilihat pada gambar 1.



Gambar 1. *Byte* dari *header* PDF

Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik penyandian yang berlandaskan matematika [5]. Dalam dunia komputer dan teknologi, kriptografi dikembangkan untuk dapat mengamankan *file* ataupun *document* digital dari pihak yang tidak berwenang. Terdapat dua istilah umum dalam kriptografi, yaitu *plaintext* dan *chipertext. Plantext* merupakan pesan asli yang belum disandikan. Sedangkan *chipertext* merupakan pesan yang telah disandikan. Pesan dapat berupa video, audio, citra digital, dan dukumen teks.

Kriptografi Kurva Eliptik

Kriptografi kurva eliptik atau *elliptic curve cryptography* (ECC) merupakan salah satu dari algoritma kriptografi yang dapat digunakan dalam pengamanan data pada komputer. Algoritma ini dikembangkan oleh Victor Miller dan Neal Koblitz pada tahun 1985, yang mana alogirtma ini memiliki keunggulan jika dibandingkan dengan algoritma kriptografi RSA, yaitu peggunaan kunci yang lebih pendek namun memiliki tingkat keamanan yang sama [6]. Penggunaan kunci yang pendek sangat bermanfaat pada perangkat yang menggunakan memori yang sangat terbatas.

Bilangan Prima

Bilangan Prima merupakan bilangan yang tidak dapat dibagi oleh nilai apapun selain nilai prima itu sendiri dan 1 (satu) [7]. Bilangan pirma memiliki pengaruh besar dalam kriptografi [8]. Oleh karena itu, ECC merupakan salah satu algoritma yang mendasarkan algoritmya pada bilangan prima.

Kuadratik Residu

Bila p adalah bilangan prima, maka a adalah residu kuadratik modulus p jika dan hanya memenuhi persamaan 1.

$$a^{(p-1)/2} \equiv 1 \; mod \; p \quad \text{..... (1)}$$

Bilangan-bilangan yang merupakan kuadratik residu, memiliki dua buah akar, yaitu seperti persamaan 2 dan 3.

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)

$y_1 = a^{(p+1)/4} \ mod\ p$ ..... (2)
$y = p - y1$ ..... (3)

***Finite Field* Bilangan Prima (F_p)**

Finite field bilangan prima (F_p) merupakan medan berhingga, yang mana dalam setiap operasi matematika (perkalian, pembagian, penjumlahan, pengurangan dan modulus) selalu menghasilkan nilai bulat yang terdapat dalam rentang nilai 0 sampai dengan *p*-1 [9].
ECC pada F_p memiliki bentuk umum seperti pada persamaan 4.

$y^2 = x^3 + Ax + B \ mod\ p$ ..... (4)

Dengan *A*, *B* ∈ Z_p merupakan konstanta yang memenuhi syarat $4A^3+27B^2 \neq 0$ *mod p*.

Grup Siklik

Grup siklik merupakan suatu orde dari suatu grup yang setiap unsurnya dapat ditulis sebagai perpangkatan (positif atau negatif) atau perkalian dari suatu unsur tetap dari grup itu [10]. Terdapat beberapa hal yang perlu diperhatikan, antara lain:

- Jika *G* merupakan grup siklik dengan generator *g* yaitu $G = \{ g^n | n \in Z\}$, maka grup *G* itu cukup ditulis dengan <*g*> atau (*g*).
- Penulisan $G= \{g^n | n \in Z\}$ yang menyatakan bahwa *G* grup siklik dengan generator *g*, biasa dipakai untuk grup *G* yang operasi binernya multiplikatif (perkalian), sedangkan grup *G* yang operasi binernya aditif (penjumlahan) dinotasikan $G=\{ng|n \in Z\}$.
- Operator perkalian pada grup G (G, *) dapat dikenakan secara berulang untuk elemen yang sama. Analoginya sama dengan perhitungan pangkat a^i, yaitu pengoperasian * pada *a* sebanyak *i* kali seperti persamaan 5.

  $a^i = a * a * a * \ldots * a$ ..... (5)

  Titik-titik *ECC* (kecuali titik *infinity O*) pada F_p dapat bertindak sebagai pembangkit (*generator*) sehingga membentuk grup siklik.

Penjumlahan Titik

Penjumlahan 2 buah titik $P(x_1,y_1)$ dan $Q(x_2,y_2)$ selalu menghasilkan sebuah titik pada ECC. Berikut merupakan aturan penjumlahan titik dalam ECC:

1. Penjumlahan Titik Berbeda $P + Q \ mod\ p = R$.
   Jika $P(x_1,y_1)$ dan $Q(x_2, y_2)$ adalah titik berbeda dengan $x1 \neq x_2$ maka penjumlahan operasi 2 titik pada *ECC* $P(x_1, y_1)+Q(x_2, y_2)$ *mod p* = $R(x_3, y_3)$. Titik R dapat dicari dengan persamaan 6, 7 dan 8.

   $\lambda = \frac{y_1 - y_2}{x_1 - x_2} (mod\ p)$ ..... (6)
   $x_3 = \lambda^2 - x_1 - x_2 \ (mod\ p)$ ..... (7)
   $y_3 = \lambda - (x_1 - x_3) - y_1 \ mod\ p$ ..... (8)
2. Penjumlahan Titik yang Sama (penggandaan titik) $P + P \ mod\ p = R$.
   Jika *P* dan *Q* adalah titik yang sama $x_1 = x_2$ dan $y_1 = y_2$ maka ditulis $P + P \ mod\ p = R$. Untuk mencari titik *R* dari penjumlahan titik yang sama, dapat digunakan persamaan 9, 10, dan 11.

   $\lambda = \frac{3x_1^2 + A}{2y_1} (mod\ p)$ ..... (9)
   $x_3 = \lambda^2 - 2x_1 \ mod\ p$ ..... (10)
   $y_3 = \lambda - (x_1 - x_3) - y_1 \ mod\ p$ ..... (11)
   Jika $y_1 = 0$, maka λ tidak terdefenisi sehingga $P + P \ mod\ p = 0$, yaitu menghasilkan sebuah titik di *infinity*.

Proses Pengamanan File Menggunakan Algoritma Kurva Eliptik

Terdapat 5 proses utama dalam mengamankan *file* menggunakan ECC, yaitu menentukan parameter ECC, pembentukan kunci (publik dan rahasia), merepresentasi pesan atau *plaintext* menjadi titik-titik kurva, ekripsi dan dekripsi.

Menentukan Paramater ECC

Pengirim dan penerima menyepakati parameter, yakni sebagai berikut:

1. Kurva eliptik $y^2 \equiv x^3 + ax + b$ (mod *p*), yang dalam hal ini parameter *a*, *b* dan bilangan prima (*p*).
2. Grup eliptik yang dihitung dari persamaan kurva eliptik.

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)

3. Titik basis $B(x,y)$ yang dipilih dari grup eliptik untuk operasi kriptografi.
4. n = order dari B yaitu bilangan bulat positif terkecil yang memenuhi $n*B=O$.

Pembentukan Kunci

Setiap pengguna membangkitkan pasangan kinci publik dan kunci privat milikya. Tabel 1 merupakan kunci pengirim dan penerima pesan.

Tabel 1 Kunci Pengirim dan Penerima Pesan

Pengguna	Kunci Privat	Kunci Publik
Pengirim Pesan	d_1, dipilih dari selang [1, p-1]	$P_A = d_1 . B$
Penerima Pesan	d_2, dipilih dari selang [1, p-1]	$P_B = d_2 . B$

Merepresentasi Pesan Menjadi Titik-Titik

Plaintext yang akan dienkripsi terlebih dahulu ribubah menjadi titik-titik P(x,y) yang terdapat dalam himpunan titik-titik kurva yang telah dibangun menggunakan persamaan 4. Berikut merupakan modifikasi dari algoritma Koblitz untuk merepresentasikan pesan menjadi titik:

1. Tetapkan sebuah kurva eliptik $y^2 = x^3 + Ax + B \ mod \ p$, Misalkan kurva eliptik memiliki n buah titik.
2. Misalkan karakter-karakter penyusun plainteks adalah angka 0, 1 ,…, 9 dan huruf A, B,…, Z. Kodekan huruf A, B, …, Z dengan nilai selanjutnya yaitu 10, 11, 12, … 35.
3. Konversi setiapPilih sembarang nilai k (pengirim dan penerima menyepakati nilai ini), misalnya k=20. karakter di dalam pesan dengan nilai antara 0 sampai 35.
4. Pilih sembarang nilai k (pengirim dan penerima menyepakati nilai ini), misalnya k=20.
5. Misalkan sebuah karakter bernilai m. Hitung $x = mk + 1 \ mod \ p$ dan subtitusikan ke dalam y. Sedangkan hasil baginya (q) ditampung dalam sebuah array yang nantinya akandisisipkan pada *trailer* dari strukutr *file* PDF.
6. Jika tidak ada nilai y yang memenuhi, ulangi $x = mk + 2 \ mod \ p$, $x = mk + 3 \ mod \ p$ sampaipada $x = mk + k - 1$. Hasil langkah 6 adalah titik (x,y) sebagai hasil pengkodean nilai m menjadi sebuah titik pada kurva eliptik. Peluang nilai m tidak dapat diasosiasikan dengansebuah titik di kurva eliptik adalah $1/2^k$.

Enkripsi Pesan

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

1. Pengirim memilih bilangan acak r dengan syarat r terletak di dalam selang [1, n-1].
2. Pengirim menghitung *ciphertext* dari pesan P_m dengan menggunakan kunci publik penerima (P_b) seperti persamaan 12 dan 13.

$C_1 = r . B$ ..... (12)

$C_2 = P_m + r . P_B$..... (13)

Ciphertext adalah pasangan titik $[C_1, C_2]$ atau ditulis pada persamaan 14.

$P_c=[C_1, C_2]=[(r.B),(P_m+r.P_B)]$..... (14)

Dekripsi Pesan

Penerima menggunakan kunci privatnya (d_2). Penerima melakukan langkah-langkah dekrips sebagai berikut:

1. Penerima menghitung hasil kali komponen pertama dari P_c , yaitu $C_1 = r . B$, dengan kunci privatnya, d_2 sebagai berikut: $d_2 . C_1$.
2. Penerima kemudian mengurangkan komponen kedua dari P_C, yaitu $C_2 = P_m + r . P_B$, dengan hasil kali dari langkah 1 di atas seperti persamaan 15.

$(P_m + r.P_B) - d_2.C_1 = P_m + r(d_2 . B) - d_2(r.B) = P_m$ ..... (15)

Pengurangan 2 buah titik $-Q$ sama dengan menjumlahkan P dengan hasil pencerminan Q terhadap sumbu x, seperti persamaan 16.

$P - Q = P + (-Q)$ ..... (16)

yang dalam hal ini, jika $Q = (x,y)$, maka digunakan persamaan 17.

$-Q = P + (-Q)$..... (17)

Merepresentasikan Titik Menjadi Pesan

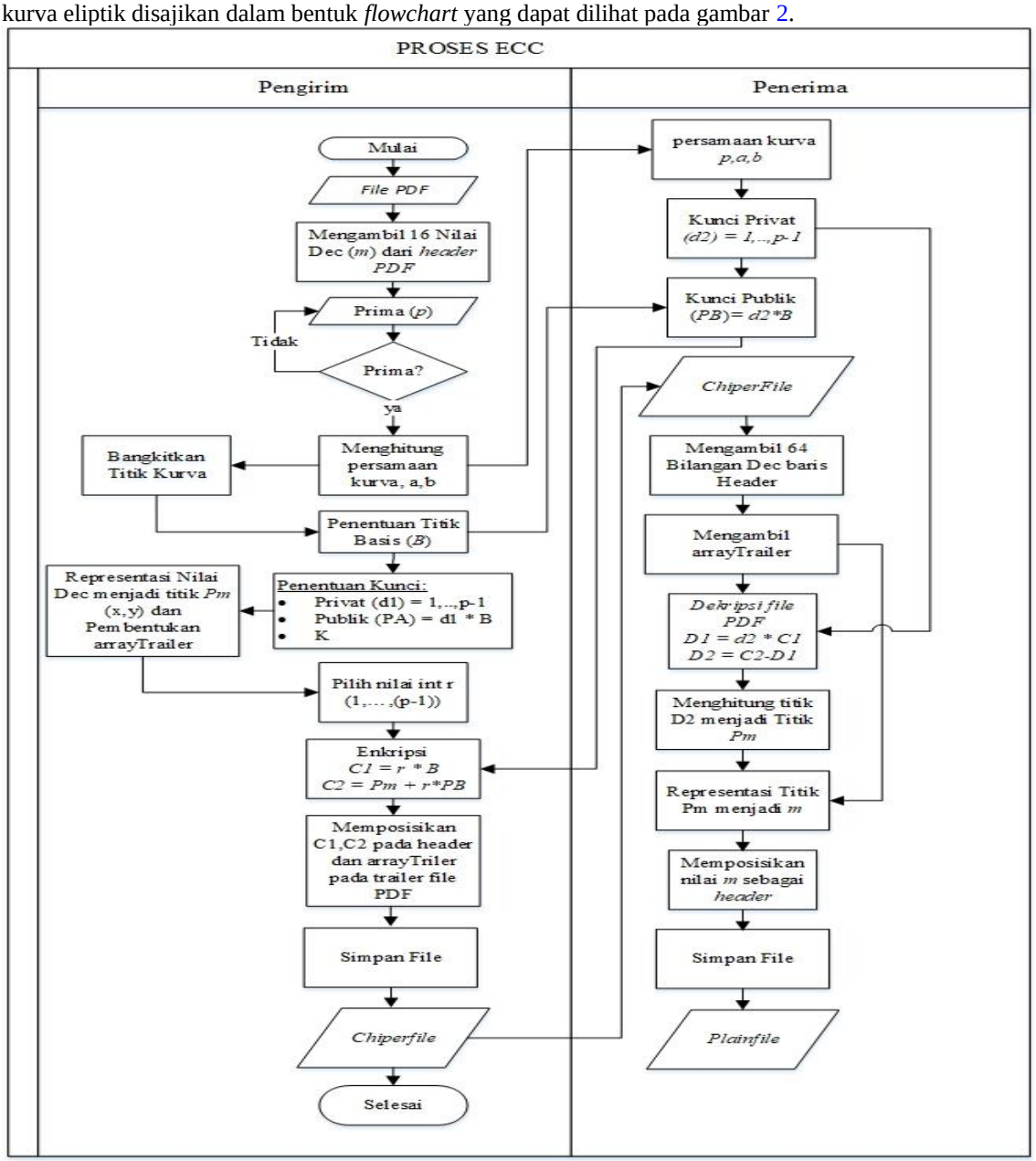
Langkah-langkah dalam melakukan *decoding* atau mengubah titik menjadi pesan:

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)

1. Mengambil hasil bagi ke-i yang terdapat pada *trailer file PDF* dan nilai *x* pada titik P_m
2. Menghitung *a* = (hasil bagi ke-*i* . prima) + *x*. Variabel *a* yang digunakan bukan variabel *a* yang terdapat paramter *ECC*, namun variabel *a* ini hanya sebagai penampung.
3. *m* = (*a* - 1)/*k*

Gambaran Umum

Gambaran umum sistem yang diusulkan untuk mengamankan PDF dengan algoritma kriptografi kurva eliptik disajikan dalam bentuk *flowchart* yang dapat dilihat pada gambar 2.



Gambar 2. *Flowchart* sistem pengamanan PDF menggunakanalgoritma ECC

3. HASIL DAN PEMBAHASAN

Hasil Pengujian

Pengujian yang dilakukan adalah pengujian korelasi. Dengan tujuan untuk mengetahui nilai kemiripan antara 2 variabel, yaitu *plainfile* dan *chiperfile.* Apabila nilai korelasi yang dihasilkan mendekati 0 (nol), maka kedua variabel tersebut memiliki nilai kemiripan yang rendah atau *chiperfile* yang dihasilkan benar-benar teracak. Apabila nilai variabel yang dihasilkan mendekat 1 (satu), maka *chiperfile* dan *plainfile* memiliki nilai kemiripan yang tinggi atau *chiperfile* yang dihasilkan tidak benar-benar teracak. Korelasi

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)

memiliki 5 kelas, yaitu sangat rendah (0,00–0,199), rendah (0,20–0,399), sedang (0,40–0,599), kuat (0,60–0,799) dan sangat kuat (0,80–1,000).

Terdapat 5 Jenis ukuran *file* PDF yang dienkripsi, yaitu 1KB–2MB, 2MB–4MB, 4MB–6MB dan lebih dari 6 MB. Masing-masing ukuran *file* tersebut memiliki 3 *file*, yang mana masing-masing *file* tersebut diuji sebanyak 3 kali percobaan. Sehingga terdapat 360 percobaan. Dengan menggunakan parameter yang terdapat pada tabel 2, didapatkan rata-rata korelasi yang dapat dilihat pada tabel 3.

Tabel 2. Parameter ECC

No. Pecobaan	Koef. A	Koef. B	Index Titik Basis	Kunci Rahasia	Indeks K
1	30	34	34	4	12
2	4	13	55	19	24
3	22	46	12	11	43

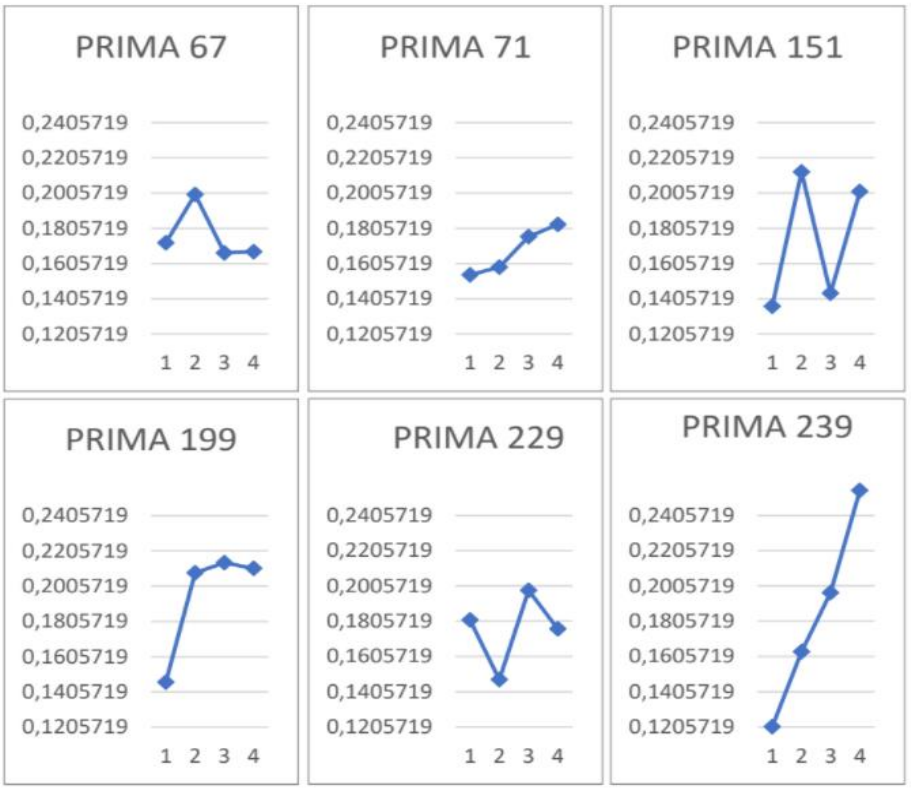
Tabel 3. Rata-rata Korelasi

NO	PRIMA	UKURAN FILE	RATA- RATA KORELASI
1	67	1KB–2MB	**0,271260276**
		2MB–4MB	**0,211663151**
		4MB–6MB	**0,273907953**
		Lebih besar dari 6MB	**0,305174777**
		Rata-rata	**0,265501539**
2	71	1KB–2MB	**0,22224537**
		2MB–4MB	**0,154170779**
		4MB–6MB	**0,247085914**
		Lebih besar dari 6MB	**0,225071265**
		Rata-rata	**0,212143332**
3	151	1KB–2MB	**0,171775327**
		2MB–4MB	**0,068374552**
		4MB–6MB	**0,168495388**
		Lebih besar dari 6MB	**0,112876845**
		Rata-rata	**0,130380528**
4	199	1KB–2MB	**0,209623202**
		2MB–4MB	**0,166775232**
		4MB–6MB	**0,16552112**
		Lebih besar dari 6MB	**0,248651741**
		Rata-rata	**0,197642824**
5	227	1KB–2MB	**0,172952617**
		2MB–4MB	**0,265692186**
		4MB–6MB	**0,3164282**
		Lebih besar dari 6MB	**0,326260207**
		Rata-rata	**0,270333302**
6	239	1KB–2MB	**0,155379619**
		2MB–4MB	**0,157209107**
		4MB–6MB	**0,199862171**
		Lebih besar dari 6MB	**0,197551726**
		Rata-rata	**0,177500656**
Rata-rata Korelasi Seluruh Pengujian			**0,20891703**

Berdasarkan tabel 3, rata-rata korelasi dari keseluruhan percobaan adalah 0,20891703, yang mana merupakan korelasi yang masuk dalam kategori rendah. Korelasi tersebut tidak dipengaruhi oleh ukuran *file* ataupun parameter ECC yang digunakan termasuk bilangan prima. Jadi, tidak dapat dikatakan bahwa semakin besar bilangan prima yang digunakan atau semakin besan ukuran *file* yang digunakan maka korelasi yang dihasilkan semakin kuat atau semakin lemah. Grafik pada gambar 3 menunjukan hubungan antara bilangan prima dan ukuran *file* terhadap korelasi yang dihasilkan. Nilai 1, 2, 3 dan 4 pada sumbu *x* merupakan nilai yang mewakili ukuran *file* secara berturut-turut yaitu 1KB–2MB, 2MB–4MB, 4MB–6MB dan lebih dari 6 MB. Sedangkan sumbu *y* merupakan korelasi.

Dari 360 percobaan, sebaran kelas nilai korelasinya dapat dilihat pada tabel 4. Dari hasil enkripsi, ukuran *file* bertambah menjadi 64 *Bytes*. Hal ini karena 1 *character* pada *header* yang dienkripsi, akan menjadi 4 *character*. Sehingga dari 16 *character* yang dienkripsi akan menjadi 64 *character*. Ukuran *file* akan kembali pada ukuran *file* semula setelahdidekripsi.

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)



Gambar 3. Hubungan Bilangan Prima dan ukuran *file* terhadap korelasi

Tabel 4. Sebaran kelas korelasi

Kelas Korelasi	Ukuran File				Total *file*	Persen-tase (%)	Rata-rata Korelasi
	1KB–2MB	2MB–4MB	4MB–6MB	> 6MB			
(0,00 – 0,199)	54	48	40	50	192	53,3	0,097702511
(0,20 – 0,399)	29	32	41	23	125	34,72	0,283341735
(0,40 – 0,599)	7	7	9	13	36	10	0,491353081
(0,60 – 0,799)	0	3	0	4	7	1,94	0,650927247
0,80 – 1,000)	0	0	0	0	0	0	0

Pembahasan

ECC mampu mengamankan *file* PDF dengan baik. Hal ini didukung dengan nilai korelasi yang dihasilkan berdasarkan 360 percobaan, yaitu 0,20891703 (rendah). Korelasi yang dihasilkan tidak dipengaruhi oleh bilangan primaataupun ukuran *file* yang dipilih.

File PDF yang telah dienkripsi tidak dapat diakses karena *header* dari *file* tersebut telah teracak bahkan jumlah *character* akan bertambah. Bertambah jumlah *character* dari 16 menjadi 64, diakibatkan oleh algoritma ECC itu sendiri, bukan diakibatkan oleh ukuran *file* . Jadi, setiap *file* PDF yang dienkripsi akan mengalami kenaikan ukuran *file* sebesar 64 *Bytes* dan akan kembali pada ukuran semula setelah didekripsi.

4. KESIMPULAN DAN SARAN

Kesimpulan

Penerapan algoritma ECC melakukan pengamanan terhadap *file* PDF dapat dilakukan dengan baik yaitu dengan nilai korelasi yang dominanterhadap kelas yang sangat rendah yaitu (0,00-0,199) dengan persentase ±53,33% dari 360 percobaan. Sedangkan rata-rata dari 360 percobaan tersebut adalah 0,212282779.

PDF yang dienkripsi akan mengalami kenaikan ukuran sebesar 64 *bytes.* Hal ini dikarenakan setiap 1 *byte* yang dienkripsi akan menjadi 4 *byte*, sehingga 16 *byte header* PDF yang dienkripsi akan menjadi 64

byte. Ukuran *file* tersebut akan kembali semula setelah dilakukan dekripsi.

Saran

Penggunaan ECC mengharuskan pengirim dan penerima mengingat semua parameter yang disepakati. Keterbatasan daya ingat manusia mengakibatkan tidak teringatnya akan satu atau beberapa parameter yang digunakan. Hal ini akan berdampak pada proses enkripsi dan dekripsi. Oleh karena itu, dibutuhkan sebuah teknik baru, sehingga tidak semua parameter harus diingat.

Untuk menghasilkan nilai korelasi yang mendekati 0 (nol), parameter yang dipilih masih dilakukan secara manual atau *trial and arror*. Sehingga dibutuhkan sebuah algoritma yang mampu memilih dengan pasti parameter-parameter yang akan menghasilkan korelasi yang selalu mendekati 0.

Dokumen digital tidak hanya berupa PDF. Oleh karena itu, penelitian selanjutnya dapat mengembangkan untuk dapat mengamankan *ms office, word, excel* dan jenis dokumen elektronik lainnya.

DAFTAR PUSTAKA

[1] M. Rifauddin, "Pengelolaan arsip elektronik berbasis teknologi," *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, vol. 4, no. 2, pp. 168–178, 2016, doi: 10.24252/kah.v4i27.

[2] A. G. Berliani and I. Krismayani, "Penerimaan Aplikasi e-dokumen di PT Pelindo III Cabang Tanjung Emas Semarang," *Jurnal Ilmu Perpustakaan*, vol. 6, no. 4, pp. 261–270, 2019.

[3] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," *MEANS*, pp. 93–99, Dec. 2017, doi: 10.54367/means.v2i2.144.

[4] M. L. Belo, D. R. Sina, and Y. Y. Nabuasa, "Algoritma Md5 Dan Rc5 Untuk Pengamanan File Pdf," *J-Icon: Jurnal Komputer dan Informatika (JICON)*, vol. 8, no. 1, pp. 68–75, 2020, doi: 10.35508/jicon.v8i1.2396.

[5] 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.

[6] N. Adianson, Y. Yupianti, and A. Kurniawan, "Analisa Perbandingan Performansi Rsa (Rivest Shamir Adleman) Dan Ecc (Elliptic Curve) Pada Protokol Secure Socket Layer (Ssl)," *JURNAL MEDIA INFOTAMA*, vol. 11, no. 1, pp. 71–80, 2015, doi: 10.37676/jmi.v11i1.254.

[7] A. P. Naufal, "Teori Bilangan di Balik GIMPS: Misi Mencari Bilangan Prima Mersenne Terbesar yang Diketahui." https://informatika.stei.itb.ac.id/, 2020. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Makalah/Makalah-Matdis-2020%20(173).pdf

[8] Y. Andrian, "Perbandingan Penggunaan Bilangan Prima Aman Dan Tidak Aman Pada Proses Pembentukan Kunci," *Creative Information Technology Journal*, vol. 1, no. 3, pp. 194–203, 2014, doi: 10.24076/citec.2014v1i3.21.

[9] A. N. Azizah, S. Zaki, and N. P. Puspita, "Kriptografi Kurva Eliptik Atas Lapangan Galois Prima GF (p) Dengan basis 95," in *SENATIK 2016*, Semarang, 2016, pp. 68–75. [Online]. Available: http://prosiding.upgris.ac.id/index.php/SENATIK2016/senatik/paper/view/1061

[10] E. Fauziah and R. H. Siregar, "Menentukan Grup Siklik Hingga dengan Pascal," *JIUP*, vol. 2, no. 3, p. 138, Sep. 2017, doi: 10.32493/informatika.v2i3.1442.

ISSN:2337-7631 (printed)
ISSN: 2654-4091 (online)