Perbandingan antara Penggunaan Algoritma Paillier dan ECC pada Aplikasi *E-Voting*

Eka Sunandika – 13517130
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517130@std.itb.ac.id

***Abstract*—*E-voting* digunakan sebagai alternatif dari pemilu yang diadakan secara konvensional. Penerapannya dapat memberikan efektivitas dalam waktu dan biaya. Permasalahan pada penggunaan *e-voting* adalah keamanan surat suara yang harus dijaga. Terdapat algoritma kriptografi kunci publik yang dapat dimanfaatkan untuk menyelesaikan permasalahan tersebut. Algoritma Paillier dan ECC dapat digunakan dalam aplikasi *e-voting* sesuai dengan jenis sistem.**

Keywords*— *Algoritma, e-voting, ECC, Kriptografi, Paillier

I. Latar Belakang

Hampir seluruh negara didunia melakukan pemilihan untuk memilih pemimpin negara atau kepala daerahnya. Cara yang dilakukan biasanya dengan mengadakan pemilu. Contohnya di Indonesia yang rutin mengadakan pemilu presiden tiap 5 tahun sekali dan Pilkada 2020 yang dilakukan serentak pada bulan desember ini. Pemilu di Indonesia diadakan secara konvensional dengan pemilih yang perlu dating ke tempat pemungutan suara (TPS) dan menyoblos calon sesuai pilihan yang diinginkan pada surat suara. Panitia pemilu akan pengumpulkan surat suara tersebut untuk dilakukan perhitungan. Calon yang mendapat suara terbanyak akan menjadi pemenang dalam pemilu tersebut. Pemilu yang dilakukan secara konvensional memiliki permasalahan dalam proses perhitungan suara yang membutuhkan waktu lama, sehingga menjadi kurang efektif. Selain itu juga cukup menghabiskan waktu karena pemilih harus dating ke TPS.

Terdapat alternatif dalam penyelenggaraan pemilu yang sudah digunakan oleh beberapa negara seperti Kanada, Belanda, dan Estonia, yaitu dengan menerapkan *e-voting*. Penerapannya dapat memberikan efektivitas dalam waktu tetapi tentunya masih punya permasalahan yang harus diatasi. Permasalahan utama dalam penerapan *e-voting* adalah masalah keamanan surat suara. Hal tersebut dapat diselesaikan dengan menerapkan kriptografi yang baik pada aplikasi *e-voting* yang digunakan.

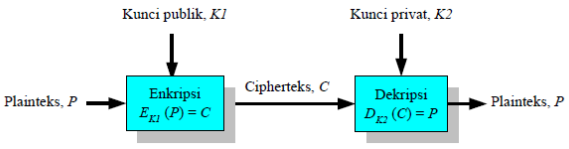
II. Dasar Teori

A. Kriptografi

Kriptografi berasal dari Bahasa Yunani “cryptós” dan “gráphein” yang memiliki arti *secret writing*. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan (Scheneier, 1996). Layanan yang diberikan kriptografi adalah kerahasiaan pesan, keaslian pesan, keaslian pengirim dan penerima pesan, dan anti penyangkalan. Terdapat beberapa istilah pada kriptografi. Pesan memiliki makna sebagai suatu informasi yang dapat dipahami dalam berbagai bentuk seperti teks, gambar, music, video, dll. Pihak yang mengirim pesan disebut pengirim dan yang menerima disebut penerima. Cipherteks merupakan pesan yang disandikan sehingga tidak bermakna agar tidak bisa dibaca oleh pihak lain. Enkripsi merupakan proses untuk merubah pesan (plainteks) menjadi cipherteks dan proses mengembaliannya disebut dengan dekripsi. Kemudian ada cipher yang merupakan sebutan untuk algoritma dalam melakukan enkripsi dan dekripsi. Dalam melakukan enkripsi dan dekripsi, terdapat parameter yang disebut dengan kunci. Algoritma pada kriptografi dibagi menjadi dua, yaitu algoritma kriptografi simetri yang kunci enkripsi dan dekripsinya sama dan algoritma kriptografi kunci publik yang kunci enkripsi dan kunci dekripsinya berbeda. Kriptografi dapat digunakan dalam berbagai hal. Menjaga kerahasiaan pesan merupakan hal yang penting dilakukan pada era digital ini yang selalu memanfaatkan internet untuk berkomunikasi dan bertukar informasi.

B. Algoritma Kriptografi Kunci Publik

Ide kriptografi kunci publik muncul pada tahun 1976 untuk menggantikan kriptografi kunci simetris yang memiliki permasalahan dalam mengirim kunci rahasianya ke penerima. Pada kriptografi kunci publik terdapat sepasang kunci yang dimiliki oleh pengirim dan penerima, yaitu kunci publik untuk mengenkripsi pesan dan kunci privat untuk mendekripsi pesan. Alur pengiriman pesan dapat dilihat pada gambar 1.



Gambar 1. Alur pengiriman pesan algoritma kriptografi kunci publik (sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Kunci-Publik-2020.pdf)

Pengirim pesan melakukan enkripsi menggunakan kunci publik yang dimiliki oleh penerima pesan. Untuk melakukan enkripsi pesan tersebut, penerima pesan menggunakan kunci

privat miliknya. Kunci rahasia tidak perlu dikirim seperti pada kriptografi kunci simetris, sehingga cara ini menjadi lebih aman. Kunci publik dapat dikirim melalui saluran yang tidak aman tanpa perlu mengkhawatirkan pesan dapat disadap oleh pihak lain karena kunci ini hanya digunakan untuk enkripsi. Selain itu, kelebihan yang didapat adalah pasangan kunci publik dan privat tidak perlu sering diubah dan dapat digunakan untuk jangka lama. Algoritma kriptografi kunci publik ini dapat diaplikasikan pada berbagai hal seperti salah satunya dalam *E-Voting*.

C. Algoritma Paillier

Algoritma Paillier dibuat oleh Pascal Paillier pada tahun 1999. Algoritma ini digunakan dalam kriptografi kunci publik. Dasar dari algoritma kriptografi ini adalah permasalahan untuk melakukan komputasi pada kelas residu n-th yang sulit dilakukan dan asumsi mengenai keputusan residualitas komposit tersebut merupakan hipotesis yang rumit. Skema pada algoritma Paillier secara homomorfik, yaitu dapat melakukan kalkulasi pada data yang sudah dienkripsi tanpa perlu didekripsi terlebih dahulu. Jika terdapat kunci public dan hasil enkripsi dari m_1 dan m_2, maka dapat dilakukan komputasi terhadap $m_1 + m_2$.

Proses pembangkitan kuncinya dilakukan sebagai berikut:

1. Memilih dua bilangan prima besar secara acak untuk p dan q yang memenuhi gcd(pq,(p-1)(q-1)) = 1 untuk memastikan kedua angka tersebut memiliki panjang yang sama.
2. Melakukan komputasi $n = pq$ dan $\lambda = lcm(p-1, q-1)$. Lcm merupakan *Least Common Multiple*.
3. Memilih bilangan integer acak g yang memenuhi $g \in \mathbb{Z}^*_{n^2}$.
4. Memastikan n dapat membagi g dengan melakukan pengecekan $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$. Dengan fungsi L merupakan $L(x) = \frac{x-1}{n}$.

Kunci publik pada algoritma ini adalah (n, g) dan kunci privat nya (λ, μ). Proses enkripsi yang dilakukan sebagai berikut:

1. Pesan yang ingin dienkripsi memiliki simbol m dan harus memenuhi $0 \leq m < n$.
2. Memilih secara acak r yang memenuhi $0 < r < n$ dan $r \in \mathbb{Z}^*_n$ dan memastikan $gcd(r, n) = 1$.
3. Kalkulasi cipherteks dengan cara $c = g^m \cdot r^n \bmod n^2$.

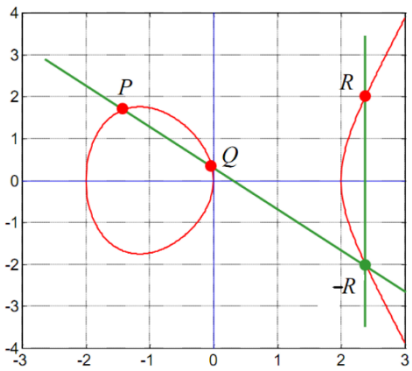
Untuk proses dekripsi yang dilakukan untuk mengubah cipherteks menjadi plainteks, dilakukan sebagai berikut:

1. Cipherteks yang ingin didekripsi memiliki simbol c, dimana $c \in \mathbb{Z}^*_{n^2}$.
2. Kalkulasi plainteks dengan cara $m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$.

D. Algoritma ECC

Elliptic Curve Cryptography merupakan kriptografi kunci public yang dikembangkan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985. Komputasi yang dilakukan pada algoritma ini berbasis kurva eliptik. Dibandingkan dengan algoritma lainnya seperti RSA, ECC memiliki ukuran kunci yang lebih kecil dengan tetap mempertahankan keamanannya. Kunci ECC sepanjang 160 bit memiliki keamanan yang sama dengan kunci RSA 1024 bit. Terdapat konsep aljabar abstrak yang mendasari ECC, yaitu grup dan medan. Grup adalah sistem aljabar yang terdiri dari himpunan G dan operasi biner * dengan notasi <G, *>. Medan merupakan himpunan elemen yang memiliki simbol F dengan dua operasi biner penjumlahan (+) dan perkalian (-). Medan berhingga memiliki simbol F_p dan Medan Galois memiliki notasi $GF(p^n)$

Kurva eliptik merupakan kurva yang memiliki bentuk persamaan $y^2 = x^3 + ax + b$ dengan syarat $4a^3 + 27b^2 \neq 0$. Terdapat beberapa operasi pada kurva eliptik, salah satunya adalah penjumlahan seberti pada gambar 2.



Gambar 2. Penjumlahan titik pada kurva eliptik (Sumber: Andreas Steffen, Elliptic Curve Cryptography, diakses di https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/ECC-2020-Bagian2.pdf)

Gambar 2. Memberikan gambaran mengenai penjumlahan titik. Garis yang ditarik melalui P dan Q akan memotong kurva pada titik $-R$. Pencerimanan dari titik $-R$ terhadap sumbu x adalah titik R yang merupakan hasil dari penjumlahan titik P dan Q. Kurva eliptik membentuk grup <G, +>.

ECC didasari oleh *Elliptic Curve Discrete Logarithm Problem* (ECDLP) yang merupakan permasalahan dalam kesulitan menghitung k dari P dan Q pada kurva eliptik. Kunci publik pada algoritma ECC adalah Q dan kunci privatnya adalah k, dengan P adalah titik sembarang pada kurva eliptik. Kurva eliptik didefinisikan pada medan berhingga atau Galois Field pada kriptografi. Kurva eliptik memiliki bentuk pada $GF(p)$ sebagai $y^2 = x^3 + ax + b \bmod p$, dengan p merupakan bilangan prima. Selain itu, juga terdapat grup eliptik yang merupakan himpunan titik – titik pada kurva eliptik dan sebuah operasi biner +. Pengguna harus membangkitkan pasangan kunci publik dan privat ketika ingin menggunakan algoritma ini.

E. E-Voting

E-voting atau pemungutan suara elektronik adalah pemungutan suara yang dilakukan secara elektronik menggunakan suatu sistem atau mesin dalam pengambilan suara dan perhitungannya. Pemungutan suara dapat dilakukan untuk berbagai hal seperti pemilihan presiden, kepala daerah, dan lain – lain. *E-voting* dapat dilakukan menggunakan mesin bernama EVM atau menggunakan komputer yang terhubung dengan internet. Proses yang dilakukan pada sistem ini yaitu melakukan pembuatan surat suara, menerima input suara, merekam suara, melakukan enkripsi pada data dan mengirimkannya ke server, dan melakukan perhitungan untuk menghasilkan hasil pemilu. Sistem juga harus mampu mampu memastikan keamanan, akurasi, integritas, kecepatan, privasi, auditabilitas,

aksesibilitas, efektif dalam biaya, skalabilitas, dan memerhatikan keberlanjutan lingkungan. *E-voting* dapat dilakukan pada suatu tempat menggunakan mesin yang disediakan oleh penyelenggara pemilu atau dapat dilakukan secara *remote* dengan internet menggunakan *smartphone* atau komputer pribadi.

Penggunaan *e-voting* dapat memberikan manfaat seperti perhitungan suara yang lebih cepat, mengurangi biaya dalam pembuatan surat suara dan memperkerjakan petugas, dan dapat memberikan kemudahan terhadap pemilih disabilitas. *E-voting* yang dilakukan secara *remote* juga dapat menghemat waktu pemilihan suara karena pemilih tidak perlu dating ke tempat dan bisa dilakukan dari lokasinya masing – masing. Selain manfaat yang didapat, terdapat beberapa kendala yang mungkin terjadi dalam menerapkan *e-voting*. Sistem yang dibuat merupakan perangkat lunak yang kompleks dan masih mungkin terjadi beberapa kecurangan seperti jumlah suara yang dimanipulasi oleh pihak lain. Keamanan merupakan permasalahan utama *e-voting* dalam mengirim suara ke server dan pengaksesasan sistem.

Gambar 3. Mesin *e-voting* yang dibuat Premier Election Solution (sumber: https://upload.wikimedia.org/wikipedia/commons/thumb/2/2a/Urna_eletr%C3%B4nica.jpeg/330px-Urna_eletr%C3%B4nica.jpeg)

Sistem pada *e-voting* memiliki beberapa jenis, seperti *paper-based electronic voting system, direct-recording electronic* (DRE) *voting system, public network DRE voting system, online voting*, dan lain – lain. DRE merupakan mesin pemilihan suara yang cukup populer digunakan. DRE memiliki layar untuk menampilkan pilihan dan menggunakan tombol atau secara *touchscreen* dalam mengaksesnya. Suara yang diterima akan disimpan dalam komponen memori yang dapat dicabut atau juga sistem dapat mengirimkan data ke server untuk diolah. *Online voting* merupakan jenis sistem yang mudah untuk dilakukan karena biasanya menggunakan *smartphone* pribadi dalam melakukan pemilihan suara, tetapi memiliki beberapa permasalahan dalam keamanan. Selain itu dapat menjadi permasalahan apabila daerah yang menerapkan *e-voting* masih kesulitan mendapat akses internet atau bahkan masih ada yang belum memiliki *smartphone*.

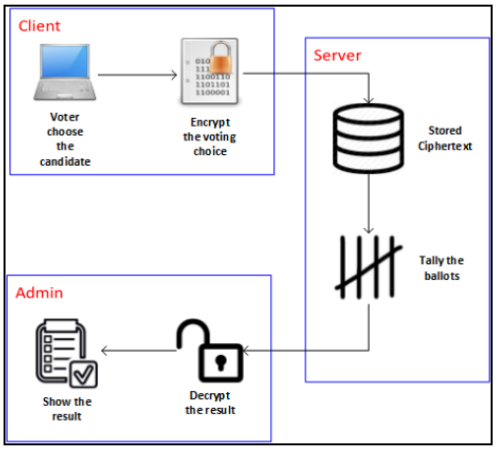
Kriptografi digunakan sebagai solusi untuk meningkatkan keamanan dalam *e-voting*. Sistem yang dibangun dapat menjadi lebih aman dan memberikan kemudahan kepada pemilih dalam proses verifikasi pilihannya. Transparansi lebih terjamin untuk dapat mengetahui bahwa pemilih sudah melakukan pemilihan dan pilihannya disimpan pada sistem. Selain itu juga dapat menjamin keamanan agar surat suara yang dikirim melalui jaringan atau internet ke server tidak dapat diubah atau dilihat oleh orang lain.

III. Penggunaan Algoritma Kriptografi pada Aplikasi *E-Voting*

A. Algoritma Paillier

Algoritma Paillier dapat digunakan pada sistem *e-voting*. Algoritma ini memiliki properti homomorfik, sehingga tanpa melakukan dekripsi pada cipherteks dapat dilakukan perhitungan terhadap jumlah data pada pesan. Hal tersebut dapat digunakan untuk menghitung jumlah suara yang masuk dengan tetap menjaga kerahasiaan pilihan dari pemilih.

Pada perbandingan yang akan dilakukan, sistem *e-voting* menggunakan algoritma Paillier yang diterapkan pada aplikasi komputer yang terhubung dengan internet. Surat suara yang masuk ke sistem akan langsung dienktripsi dan disimpan pada server. Proses dekripsi dilakukan oleh *administrator* untuk dapat mengakses hasil dari voting.



Gambar 4. Desain sistem. (sumber: Shafa, Surya, & Fairuz. *Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm*)

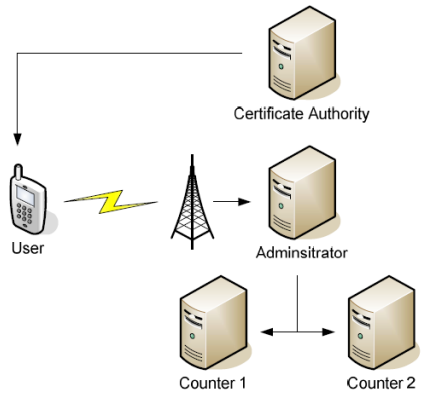
Proses pembangkitan kunci, enkripsi, dan dekripsi dilakukan menggunakan cara seperti pada dasar teori. Selain itu juga terdapat proses homomorfik pada algoritma Paillier yang dapat digunakan untuk menghitung jumlah suara masuk. Cipherteks didekripsi dengan cara $D(E(m^1, r^1) \cdot E(m^2, r^2) \bmod n^2) = m^1 + m^2 \bmod n$.

B. Algoritma ECC

Algoritma ECC dapat digunakan pada sistem *e-voting*. Panjang kuncinya yang pendek membuat algoritma ini cocok untuk digunakan pada sistem *e-voting* yang menggunakan perangkat *mobile phone*, karena tidak menghabiskan banyak memori. Selain itu, alasan lain penggunaan sistem ini karena sudah banyak orang yang memiliki *mobile phone* sehingga memberikan kemudahan dan fleksibilitas dalam pelaksanaan pemilu.

Pada perbandingan yang dilakukan, sistem *e-voting* menggunakan *mobile phone*. Terdapat beberapa entitas dalam proses pengambilan suara, yaitu pengguna yang memberikan suara, *certificate authority* yang memberikan sertifikat kepada pengguna, *administrator* yang melakukan pengecekan kepada

pengguna yang memenuni syarat, dan *counter* yang melakukan perhitungan hasil suara. Skema pada *e-voting* dapat dilihat pada gambar 5.



Gambar 5. Skema *e-voting* menggunakan *mobile phone*. (sumber: Tohari, Jiankun, & Song. An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography)

Pengiriman pesan dalam jaringan dilindungi dengan algoritma ECC. Teknik ini digunakan agar pesan tidak bisa dibaca oleh pihak lain karena proses pengiriman dilakukan pada jaringan yang tidak aman. ECC dapat memberikan keamanan yang tinggi tetapi membutuhkan kemampuan komputasional yang tinggi juga, sehingga dibutuhkan perangkat yang memenuhi spesifikasi agar mampu melakukan enkripsi. Tiap entitas pada skema harus menyiapkan pasangan kunci dan mempublikasikan kunci publiknya masing- masing.

Proses yang terjadi pada gambar 5 adalah sebagai berikut:

1. Pengguna menerima sertifikat dari CA
2. Pengguna mengkonfirmasi sertifikat ke *administrator*
3. *Administrator* melakukan pengecekan terhadap kelayakan dan ketersediaan sertifikat pengguna.
4. Jika tahap 3 terpenuhi, pengguna akan menerima daftar kandidat.
5. Pengguna melakikan enkripsi pada pilihannya menggunakan kunci publik *administrator* dan dikirim ke *administrator*. Pesan sudah mendapat ditandai menggunakan kunci privat pengguna.
6. *Administrator* melakukan pengecekan dengan mendekripsikan pesan untuk mendapat nilai tanda pesan untuk memastikan pengguna tidak mengirim berulang kali. Jika sudah benar. Pesan akan dienkripsi dan dikirim ke *counter* 1 dan *counter* 2.
7. *Counter* 1 dan 2 akan memverifikasi *signature* dari pesan yang dikirim *administrator.*
8. *Counter* 1 dan 2 akan bertukar pesan yang sudah didekripsi. Jika pesannya sama, maka pesan tersebut disetujui dan memberikan *acknowledge* ke *administrator*.
9. *Administrator* mengirim *acknowledge* tersebut ke pengguna untuk memberikan kabar bahwa pilihannya sudah diterima dan valid.

IV. ANALISIS

Analisis dilakukan dengan membandingkan efektivitas dari penggunaan dua algoritma berbeda pada aplikasi *e-voting*. Sistem *e-voting* yang menggunakan algoritma Paillier menggunakan komputer yang terhubung dengan internet, sedangkan sistem yang menggunakan algoritma ECC menggunakan *mobile phone* yang terhubung pada jaringan.

A. Algoritma Paillier

Beberapa tes dilakukan pada algoritma Paillier untuk melakukan pengujian efektivitas, yaitu tes keunikan cipherteks, tes dekripsi, tes homomorfik, tes faktor perluasan pesan, dan tes *runtime*. Panjang *p* dan *q* yang digunakan adalah 16 bit, dimana $p = 50543$ dan $q = 65053$.

Tabel 1. Hasil tes keunikan cipherteks. (sumber: : Shafa, Surya, & Fairuz. *Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm)*

No.	***Plaintext* (m)**	***Random r***	***Ciphertext* (C)**
1	7	49819	5091673028 311841742
2	7	40942	5014329154 833019458
3	7	40942	5014329154 833019458
4	30	16765	9399729716 89839058
5	30	27529	8423042122 639404412

Pada tabel 1 akan diberikan hasil tes keunikan cipherteks yang dibentuk oleh algoritma Paillier. Keunikan pada cipherteks dihasilkan oleh nilai *r*. Plainteks yang sama akan menghasilkan cipherteks yang berbeda dengan nilai *r* yang berbeda.

Tabel 2. Hasil tes dekripsi. (sumber: : Shafa, Surya, & Fairuz. *Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm)*

No.	***Plaintext (m)***	***Ciphertext (C)***	***Decryption result***	***Conclusion***
1	900	2782712007130197049	900	True
2	1799238234	4431658342509263100	1799238234	True
3	3287973779	1391923990969058026	0	False
4	3287973787	1053766279354614 7947	12	False

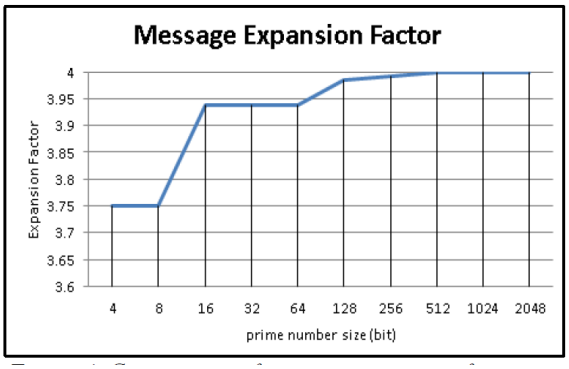
Tabel 2 menunjukan hasil dari tes dekripsi yang dilakukan pada cipherteks. Hasil dari dekripsi sesuai dengan pesan asli yang sudah dienkripsi sebelumnya, tetapi pada tes 4 memiliki nilai yang berbeda karena nilai $m \geq n$ (tidak memenuhi syarat). Tes tersebut menggunakan nilai *p* dan *q* yang sama pada tes sebelumnya dan memiliki nilai $n = 3287973779$.

Tabel 3. Hasil tes dekripsi. (sumber: : Shafa, Surya, & Fairuz.

Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm)

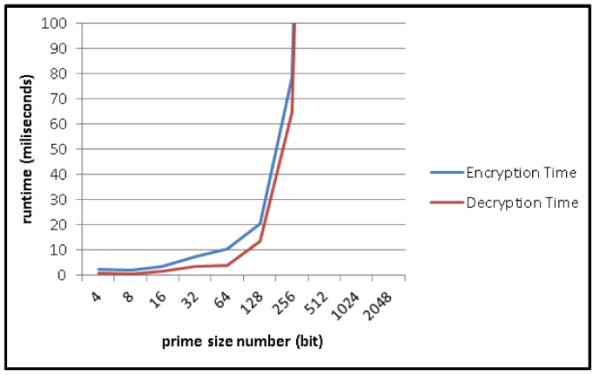
No	m1 + m2	Cipherte xt m_1 $m_2 \bmod n_2$	Decrypti on Result	Conclu- sion
1	20 + 40	8207684 3502096 35468	60	True
2	2560000 + 6534000 0	7364355 9180228 96602	9094000 0	True
3	3287973 779 + 121	2478900 2652316 43136	121	False

Tabel 3 merupakan hasil dari tes homomorpik yang dilakukan. Tes tersebut memiliki hasil yang mirip dengan tes dekripsi sebelumnya. Hasil akan benar ketika nilai kedua *m* kurang dari *n*, dan salah ketika *m* lebih besar sama dengan *n*. Dari hasil tersebut dibuktikan bahwa dapat dilakukan operasi pada pesan dengan tetap menghasilkan hasil dekripsi yang sesuai.



Gambar 6. Perbandingan perluasan faktor pada pesan. (sumber: Shafa, Surya, & Fairuz. *Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm*)

Gambar 6 merupakan hasil dari tes yang melalukan enkripsi dengan nilai bilangan prima yang berbeda untuk mengetahui perluasan faktor yang terjadi. Perluasan terjadi pada rentang 3.75 hingga 4, sehingga dapat disimpulkan bahwa cipherteks dapat memiliki ukuran 4 kali lipat dari bilangan prima yang digunakan.



Gambar 6. Hasil tes *runtime*. (sumber: Shafa, Surya, & Fairuz. *Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm*)

Pada gambar 6 dilakukan tes *runtime* untuk mengetahui berapa lama waktu yang diperlukan untuk proses enkripsi dan dekripsi. Dari grafik tersebut dapat dilihat terjadi peningkatan secara eksponensial yang cukup besar. Makin panjang ukuran bilangan prima, maka semakin lama pula waktu yang diperlukan dalam proses dan enkripsi.

A. Algoritma ECC

Tes yang dilakukan adalah membandingkan waktu enkripsi algoritma ECC dengan ECDH dan waktu enkripsi yang diperlukan algoritma ECC pada panjang pesan berbeda.

Tabel 4. Enkripsi menggunakan ECC, ECDH dan AES-128. (sumber: Tohari, Jiankun, & Song. An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography)

Encryption algorithm	Text length (byte)	Encryption time (ms)			
		160 bit	192 bit	224 bit	256 bit
ECC	6	292	341	395	470
ECDH / AES-128	60	5080	7671	111214	14999
Total		5362	8012	11609	15469

Waktu yang terdapat dalam tes enkripsi pada tabel 4 sudah termasuk waktu dalam membangkitkan kunci AES, enkripsi kunci AES dengan kunci privat ECC, dekripsi kunci AES dengan kunci privat ECC, dan enkripsi pesan menggunakan kunci AES. Pada algoritma ECC, makin panjang kunci yang digunakan pada pesan yang pendek tidak mengalami pertambahan yang terlalu signifikan.

Tabel 5. Enkripsi menggunakan ECC. (sumber: Tohari, Jiankun, & Song. An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography)

Encryption algorithm	Text length (byte)	Encryption time (ms)			
		160 bit	192 bit	224 bit	256 bit
ECC	6	292	341	395	470
ECC	60	1406	1741	2207	3097
Total		1688	2082	2602	3567

Pada tabel 5 dapat dilihat bahwa dengan panjang pesan yang

lebih besar, perbedaan panjang kunci juga tidak terlalu mempengaruhi waktu yang diperlukan dalam proses enkripsi pada algoritma ECC. Berbeda dengan ECDH dan AES-18 yang terdapat perbedaan cukup signifikan pada panjang kunci yang semakin besar. Waktu yang cenderung lebih cepat tersebut menjadikan algoritma ECC ini semakin tepat untuk digunakan pada sistem *e-voting* yang menggunakan *mobile phone.*

V. KESIMPULAN

Aplikasi *e-voting* memiliki peluang untuk menggantikan proses pemilahan yang konvensional. Masalah utama yang terdapat dalam penerapan sistem *e-voting* adalah soal kemanan. Pemanfaatan kriptografi dapat digunakan untuk menyelesaikan permasalahan ini. Terdapat berbagai algoritma kriptografi kunci publik yang dapat digunakan sesuai dengan jenis sistem *e-voting*. Algoritma Paillier dapat digunakan untuk sistem *e-voting* pada komputer yang terhubung ke internet. Properti Homomorfiknya dapat berguna untuk menghitung suara yang masuk dengan tetap menjaga kerahasiaan pilihan dari pemilih. Algoritma ECC memiliki panjang kunci yang kecil dan cocok digunakan dalam sistem *e-voting* pada *mobile phone* karena memerlukan kemampuan komputasi yang tidak terlalu besar dengan tetap menjaga keamanan seperti pada algoritma RSA. Dari hasil analisis yang dilakukan dapat disimpulkan bahwa penggunaan algoritma ECC mendapatkan peningkatan waktu yang tidak terlalu besar ketika panjang kuncinya ditambahkan. Algoritma Paillier tidak mengalami penambahan yang besar ketika panjang kuncinya kecil, tetapi ketika panjang kuncinya makin besar akan terjadi peningkatan secara eksponensial. Pemilihan penggunaan algoritma kriptografi perlu disesuaikan dengan kebutuhan pada tingkat kemanan dan jenis sistem yang akan digunakan.

VI. ACKNOWLEDGMENT

Puji syukur penulis ucapkan kepada Tuhan Yang Maha Esa atas nikmat-Nya yang sangat melimpah dan atas diberikannya kesempatan kepada saya untuk menyelesaikan makalah ini. Juga ucapan terima kasih sebesar – besarnya kepada dosen mata kuliah IF4020 Kriptografi, Bapak Dr. Ir. Rinaldi Munir, MT. atas ilmu dan bimbingannya selama 1 semester ini sehingga makalah ini dapat terselesaikan. Saya juga berterima kasih kepada orang tua dan keluarga terdekat yang tiada hentinya selalu mendoakan agar saya mendapatkan segala sesuatu yang terbaik dan yang telah memberi dukungan atas segala hal yang saya lakukan. Dan terakhir, tidak lupa berterima kasih kepada teman – teman saya yang selalu membantu dalam menghadapi berbagai permasalahan dan selalu ada dikala senang maupun duka.

REFERENCES

[1] Munir, Rinaldi. 2020. Bahan Kuliah IF4020 Kriptografi: Pengantar Kriptografi.

[2] Munir, Rinaldi. 2020. Bahan Kuliah IF4020 Kriptografi: Kriptografi Kunci-Publik.

[3] Munir, Rinaldi. 2020. Bahan Kuliah IF4020 Kriptografi: *Elliptic Curver Cryptography* (ECC) – Bagian 1 & 2.

[4] Wikipedia. *Paillier cryptosystem.* Diakses di https://en.wikipedia.org/wiki/Paillier_cryptosystem.

[5] Wikipedia. *Electronic voting.* Diakses di https://en.wikipedia.org/wiki/Electronic_voting.

[6] Anggriane, S. M., Surya, M.N, & Fairuz A. 2016. *Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm*. 2016 *International Conference on Informatics and Computing* (ICIC).

[7] Ahmad, T, Jiankun H, & Sung H. 2009. *An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography*. *2009 Third International Conference on Network and System Security*.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Desember 2020

Eka Sunandika - 13517130