KOMPUTASI: Jurnal Ilmiah Ilmu Komputer dan Matematika
Vol.18, No.1, Januari 2021, Hal. 22– 28
P-ISSN: 1693-7554, E-ISSN: 2654-3990
https://journal.unpak.ac.id/index.php/komputasi

IMPLEMENTASI ALGORITMA TANDA TANGAN DIGITAL BERBASIS KRIPTOGRAFI KURVA ELIPTIK DIFFIE-HELLMAN

Asep Saepulrohman[1)], Teguh Puja Negara[2)]
[1,2)]Program Studi Ilmu Komputer FMIPA, Universitas Pakuan
Jalan Pakuan Po.Box 452 Bogor 16143 Jawa Barat Indonesia

Corresponding Author: asepspl@unpak.ac.id

Abstrak

Tanda tangan digital (digital signature) merupakan salah satu bentuk layanan tanda tangan elektronik sebuah data yang dikirim dan diverifikasi secara elektron. Keamanan dan authentikasi data dilakukan menggunakan algoritma tanda tangan digital yang dinamakan Elliptic Curve Digital Signature Algorithm (ECDSA) yang dinilai tahan terhadap tipe serangan. Tanda tangan digital dibuat dengan memanfaatkan sistem kriptografi kunci publik. Kriptografi kurva eliptik termasuk sistem kriptografi kunci publik yang didasarkan pada permasalahan matematika logaritma diskrit. Skema yang ditunjukkan secara matematis untuk membuktikan keaslian data atau dokumen elektronikl terdiri dari deret fungsi hash yang dihasilkan dari proses algoritme fungsi hash tertentu yang kemudian disandikan (dienkripsi) dengan algoritme kriftografi kunci asimetris. Representasi tentang tanda tangan elektronik diterapkan pada citra (image) menggunakan kriptografi kurva eliptik dengan pemrograman JavaScript ECDH untuk proses otentikasi, integritas dan, verifikasi data.

Kata kunci*: Tanda tangan digital; kriptografi; ECDSA; enkripsi; dekripsi*

Abstract

Digital signature (digital signature) is a form of electronic signature service where data is sent and verified electronically. Data security and authentication are carried out using a digital signature algorithm called the Elliptic Curve Digital Signature Algorithm (ECDSA) which is considered resistant to this type of attack. Digital signatures are created using a public key cryptography system. Elliptic curve cryptography is a public key cryptography system based on the mathematical problems of discrete logarithms. The scheme shown mathematically to prove the authenticity of an electronic data or document consists of a series of hash functions generated from a specific hash function algorithm which is then encoded (encrypted) by an asymmetric key cryptographic algorithm. The representation of the electronic signature is applied to the image using elliptic curve cryptography with JavaScript ECDH programming for authentication, integrity and data verification processes.

Keywords: *Digital signature; cryptography; ECDSA; encryption; decryption*

1. Pendahuluan

Pemberlakuan masa darurat Covid-19 pada tanggal 16 Maret 2020, hampir seluruh sektor di Indonesia bahkan di seluruh dunia mengambil kebijakan terkait melakukan sebuah pekerjaan dilakukan via daring. Dengan adanya hal tersebut, terkadang diperlukan proses pertukaran dokumen elektronis (*file*) oleh karena itu diperlukan adanya suatu mekanisme untuk menjamin keaslian (*otentikasi*) dokumen elektronis salah satunya dengan menggunakan tanda tangan digital. Dalam penelitian ini bertujuan bagaimana untuk mengatasi permasalahan di atas dengan menggunakan pendekatan konsep kriptografi asimetris. Kriptografi asimetris atau sering disebut kriptografi kunci publik salah satu sistem pengamanan dalam data yang pertama kali dikemukakan oleh Diffe dan Hellman pada tahun 1976. Elliptic-Curve Diffie-Hellman (ECDH) membangun rahasia bersama yang digunakan sebagai kunci antara dua pihak dengan membuat protokol perjanjian kunci publik dan privat berdasar kurva eliptik pada saluran yang tidak aman. Kunci tersebut kemudian dapat digunakan untuk mengenkripsi komunikasi yang kemudian

menggunakan sandi kunci simetris. Ini adalah varian dari protokol Diffie-Hellman yang menggunakan kriptografi kurva eliptik. Pertukaran kunci yang diterapkan dalam bidang kriptografi untuk enkripsi P_e disebut kunci publik yang dapat didistribusikan secara bebas di saluran yang tidak aman, sedangkan kunci dekripsi P_d disebut kunci privat yang bersifat rahasia dan harus dijaga kerahasiaannya [1], [2], [3].

ECDH memiliki banyak aplikasi dalam kriptografi dan keamanan data, seperti penelitian terbaru yang mengerjakan aplikasi kriptografi di berbagai bidang ilmu dan pengembangan keamanan informasi [4] dengan penerapan kriptografi kurva eliptik dalam penelitian lapangan biner, analisis algoritma pertukaran kunci Diffie-Hellman dengan algoritma pertukaran kunci yang diusulkan [5], implementasi kurva eliptik diffie-hellman (ECDH) untuk pengkodean pesan menjadi titik pada GF(p) [6] dan lain-lain. Pemodelan terkait skema enkripsi kunci publik akan dijelaskan dalam hal operasi enkripsi, dekripsi dan pengaturan terkait dengan prosedur penyebaran kunci. Karya ini melaporkan sifat khusus dari kurva elips yang menarik kriptografer, salah satunya mendekati jumlah dua titik dalam kurva elips [7]. Analisis rinci telah dilakukan pada ECDH dengan bantuan plot fase, tabel jumlah poin. Kemudian dalam penelitian [8] dengan membahas tentang kriptografi Kurva Elliptic dan aplikasinya .

Kriptografi kurva eliptik menawarkan tingkat keamanan yang sama dengan algoritme kriptografi kunci publik konvensional, tetapi dengan ukuran kunci yang lebih pendek dan menunjukkan daya tarik yang tersembunyi. Perbandingan *eliptic curve cryptography* (ECC) dengan RSA, panjang kunci ECC lebih pendek dari RSA, misalnya kunci ECC 160 bit memberikan keamanan yang sama dengan RSA 1024 bit kunci. Operasi aritmatika pada kriptografi kriptografi yang berdasarkan kurva eilptic tidak menggunakan bilangan real, tetapi kriptografi beroperasi pada ranah bilangan bulat. Dalam kriptografi teks biasa, teks tersandi, dan kunci dinyatakan sebagai bilangan bulat. Oleh karena itu, untuk kurva eliptik yang akan digunakan dalam sistem keamanan data, kurva eliptik didefinisikan dalam bidang hingga atau Galois Field $GF(p)$ atau $GF(2^m)$. Bentuk umum dari kurva eliptik di $GF(p)$ atau $GF(2^m)$ adalah $y^2 = x^3 + ax + b \bmod$ p dengan p adalah bidang berhingga dan unsur-unsur dalam bidang galois adalah {0, 1,2, ..., p-1} dimana operasi penjumlahan dan perkalian dilakukan dengan modulus p. Dalam kriptografi [9] menunjukkan kurva eliptik E yang telah dimodelkan menjadi persamaan matematis dalam grafik suatu persamaan bentuk $E: y^2 = x^3 + ax + b$ dengan a, b adalah konstanta dengan batasan bahwa $4a3 + 27b^2 \neq 0$ yang memenuhi sifat non-singular dari pasangan $(x, y) \in R \times R$ bersama dengan titik khusus $\mathcal{O}$ disebut titik tak terhingga yang disebut persamaan Weierstrass untuk kurva elips. Karena setiap kurva eliptik ditentukan oleh persamaan kubik, teorema Bezout menjelaskan bahwa setiap garis memotong kurva tepat pada tiga titik, diambil dengan kelipatan. Hukum grup dengan mensyaratkan bahwa tiga titik co-linear berjumlah nol. Operasi penjumlahan pada kurva elips pada GF(p) memiliki aturan yang sama dengan bilangan real. Kasus pertama jika if $x_1 \neq x_2$ maka operasi penjumlahan $P + Q = R$. Penjumlahan $R = (x_3, y_3)$ dicari dengan menentukan garis l melalui P dan Q yang berpotongan di $-R$, di mana $-R$ adalah hasil refleksi R pada sumbu x. Koordinat titik R dapat ditentukan dengan Persamaan 1

$$x_3 = \lambda^2 - x_1 - x_2 \text{ dan } y_3 = \lambda(x_1 - x_3) - y_1 \quad (1)$$

dengan $\lambda = (3{x_2}^2 + a)/2y_1$. Kasus kedua, titik P dan Q titik yang sama $x_1 = x_2$ kemudian dapat ditulis $P + P = R$. R ditemukan dengan menentukan garis l yang bersinggungan dengan kurva elips di titik P, maka perpotongan garis l dengan kurva elips adalah -R yang merupakan refleksi dari sumbu x. Kasus terakhir jika $x_1 = x_2$ dan $y_1 = -y_2$, dalam hal ini $Q = -P$ dimana garis l melalui P dan Q tidak berpotongan dengan kurva elips sehingga dikatakan memiliki titik tak terhingga yang ditulis $P + Q + P + (-P) = \mathcal{O}$.

2. Metode Penelitian

Metode yang digunakan dalam pertukaran kunci bersama Diffie-Hellman untuk kriptografi kurva eliptik yang dianalisis dan digunakan dalam penelitian ini diambil dari https://asecuritysite.com/encryption/js08. Sebelum dijelaskan lebih lanjut, misalkan Alice ingin membuat menyampaikan kunci sama Bob pada saluran yang tidak aman maka langkah-langkahnya sebagai berikut:

Pilih parameter domain yang kuat secara kriptografi yaitu, , (p, a, b, G, n, h) dalam kasus utama case $(m, f\ (x), a, b, G, n, h)$ dalam kasus biner harus disepakati. Parameter sistem harus dipertukarkan secara otentik antara pihak-pihak yang terlibat dalam komunikasi.

Kesepakatan kunci

Perjanjian kunci juga harus diamankan dengan otentikasi yang kuat. dengan prosedur sebagai berikut:

1. Setiap pihak harus memiliki pasangan kunci yang sesuai untuk kriptografi kurva eliptik, yang terdiri dari kunci pribadi d (bilangan bulat dipilih secara acak dalam interval $[1, n-1]$ dan kunci publik yang diwakili oleh titik Q (di mana $Q = d.Q$), yaitu, hasil penambahan G ke waktu itu sendiri).
2. Izinkan pasangan kunci Alice (d_A, Q_A) pasangan kunci Bob menjadi (d_B, Q_B) di mana setiap pihak harus mengetahui kunci publik pihak lain sebelum menjalankan protocol.
3. Alice menghitung poin $(x_k, y_k) = d_A.Q_B$ dan Bob menghitung poin points $(x_k, y_k) = d_B.Q_A$ dimana rahasia bersama adalah x_k (koordinat x poin). Kebanyakan protokol standar berdasarkan ECDH berasal dari kunci x_ksymmetric menggunakan beberapa fungsi derivasi kunci berbasis hash.
4. Rahasia bersama yang dihitung oleh kedua belah pihak adalah sama, karena $d_A Q_B = d_A.d_B.G = d_B.d_A.G = d_B Q_A$.

Algoritme penghasil kunci ECDH

Domain parameter kurva eliptik di atas F_p didefinisikan sebagai persamaan $T(p, a, b, G, n, h)$, di mana p adalah bidang yang didefinisikan kurva, , a, b koefisien persamaan kurva elips, G generator titik adalah elemen pembangun kelompok, n adalah orde utama dari G yaitu bilangan bulat positif terkecil adalah $nG = 0$, dan h kofaktor, banyaknya titik dalam kelompok eliptik $E_p(a, b)$ dibagi n

Algoritma 1	Algoritma penghasil kunci ECDH
Input:	Parameter domain (p, a, b, G, n, h)
Output:	Kunci private: d_A, d_B dan Kunci publik: Q_A, Q_B
1.	Pilih bilangan bulat $d_A, d_B \in [1, n-1]$
2.	User A menghitung $Q_A = d_A.G$ send to User B
3.	User B menghitung $Q_B = d_B.G$ send to User A
4.	User A menghitung $K = d_A.Q_B = d_A(d_B.G)$
5.	User B menghitung $K' = d_B.Q_A = d_B(d_A.G)$

Kemudian proses selanjutnya adalah proses enkripsi pesan dengan ECDH yang merupakan varian dari algoritma Diffie-Hellman untuk kurva elips. Masalah yang dia selesaikan adalah sebagai berikut: dua pihak (biasanya Alice dan Bob) ingin bertukar informasi dengan aman, sehingga pihak ketiga tidak dapat menguraikan kode mereka. Selanjutnya adalah proses enkripsi ECDH pada Algoritma 2.

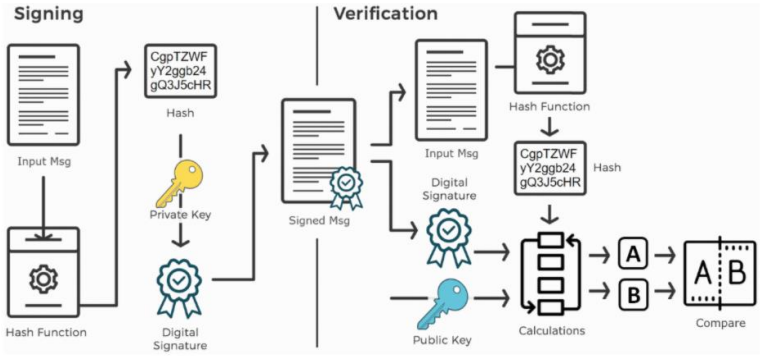
Algoritma 2	Algorimta enkripsi ECDH
Input:	Parameter domain (p, a, b, G, n, h)
	Kunci privat: x, y dan kunci publik: P_A, P_B, plaintext M
Output:	Chipertext: C
1.	Hitung $S = yP_A = x.P_B$
2.	Hitung C= $M + S$

Dalam desain sistem dekripsi ini, akan mengembalikan pesan terenkripsi ke pesan asli lagi. Proses dekripsi kemudian dilakukan dengan cara mereduksi pesan rahasia pada Algoritma 3.

Algoritma 3	Algorimta dekrispsi ECDH
Input:	Parameter (p, a, b, G, n, h), kunci rahasia bersama S, chipertext C
Output:	Plaintext M
1.	Hitung $M = C - S$
2.	Plaintext $M = C - S$

3. Hasil dan Pembahasan

Tanda tangan digital (*digital signature*) bekerja hampir sama dengan cara kerja tanda tangan dokumen biasa. Dalam tanda tangan digital sistem kerja yang dilakukan dengan dua algoritma, yaitu algoritma *sign* untuk menandatangani sebuah dokumen M dan menghasilkan sebuah tanda tangan (*sign*) ρ, dan algoritma *verify* yang mengembalikan nilai true bila tanda tangan ρ asli dari pemilik penandatangan untuk dokumen M. Sistem digital signature menggunakan kunci asimetris dengan algoritma *sign* menggunakan kunci privat dan algoritma *verify* menggunakan kunci publik. Proses tanda tangan digital (*digital signature*) dengan kunci asimetris dapat dilihat pada Gambar 3.1 [21]



Gambar 3.1 Skema pembentukan dan validasi tanda tangan digital

Skema penandatanganan dilakukan dengan pesan di hash, kemudian dilakukan proses komputasi berdasarkan kurva eliptik, logaritma diskrit atau primitif kriptografi lainnya, dan tahap berikutnya menghitung tanda tangan digital. Pesan bertanda tangan yang dihasilkan terdiri dari pesan asli dan tanda tangan terhitung. Pada verifikasi tanda tangan, pesan untuk verifikasi di-hash dan beberapa perhitungan dilakukan antara hash pesan, tanda tangan digital dan kunci publik, dan akhirnya perbandingan memutuskan apakah tanda tangan itu valid atau tidak.

ECDSA adalah adaptasi dari algoritma DSA klasik, yang diturunkan dari skema tanda tangan ElGamal. Lebih tepatnya, algoritme ECDSA adalah varian dari tanda tangan ElGamal, dengan beberapa perubahan dan pengoptimalan untuk menangani representasi elemen grup (titik-titik kurva eliptik). Seperti algoritme kripto kurva eliptik lainnya, ECDSA menggunakan kurva eliptik (seperti secp256r1), kunci pribadi (bilangan bulat acak dalam panjang kunci kurva-untuk menandatangani pesan) dan kunci publik (titik EC, dihitung dari kunci privat dengan mengalikannya menjadi titik generator kurva untuk memverifikasi tanda tangan). Proses tanda /verifikasi ECDSA bekerja sebagai berikut:

Untuk proses kriptografi, kita bekerja di F_q dengan $q = p^n$ adalah pangkat utama $p \neq 2, 3$ dan kurver eliptik E/F_qadalah kurver nonsingular yang memenuhi persamaan $y^2 = x^3 + ax + b$. Himpunan titik pada E terletak pada F_q ditambah titik tak terhingga berubah menjadi suatu kelompok, dilambangkan $E(F_q)$. Dalam pekerjaan ini, Elliptic Curve Diffie Hellman (ECDH) digunakan untuk menghasilkan kunci bersama. Implementasi ini menggunakan Elliptic Curve Cryptography (ECC) yang diberikan oleh dinamika berikut: Dalam contoh ini kami menggunakan secp224r1 untuk menghasilkan titik pada kurva. Formatnya adalah: Kami menguji validasi kurva

di secp224r1 dengan menggunakan a pada kurva curve $y^2 = x^3 + ax + b$ Koordinat generator adalah

Method	**secp224r1**
p (medan)	115792089210356248762697446949407573530086143 415290314195533631308867097853951
a dari $y^2 = x^3 + ax + b$	115792089210356248762697446949407573530086143 415290314195533631308867097853948
b dari $y^2 = x^3 + ax + b$	410583637251521421293261297800472684091144410 159937255548352563140394674012 91
G_x, G_y-titik dasar yang merupakan (x, y) titik pada kurva eliptik	484395612939064517590525852527979142027629 4 952604174799584408071708240463528 6 361342509567497957985851279195878819566111 0667298501507187719825356841440510 9
(menciptakan medan hingga 0 sampai N − 1). Semua operasi selesai (mod N)	115792089210356248762697446949407573529996955 224135760342422259061068512044369

Berikut ini contoh [20] perhitungan proses pengamanan tanda tangan digital dengan JavaScript menggunakan kunci ECC dan ECDH:

Langkah 1. Komunikasi terenkripsi yang aman antara dua pihak mengharuskan mereka bertukar kunci terlebih dahulu secara fisik yang aman, seperti daftar kunci kertas yang dibawa oleh kurir tepercaya. Metode pertukaran kunci Diffie-Hellman memungkinkan dua pihak yang tidak memiliki pengetahuan sebelumnya satu sama lain untuk bersama-sama membangun kunci rahasia bersama melalui saluran yang tidak aman.

a. **Nilai pribadi Alice (a):**
   55351826471957705962817146026270180827124176211142850770529849242510895012083
b. **Nilai pribadi Bob's (b):**
   26869739350039700103220091651548837834466042671903266250677849251629126350832

Langkah 2. Kunci publik diwakili oleh titik Q (di mana Q = d.G), yaitu, hasil penambahan G ke dirinya sendiri d waktu dengan pasangan Alice ke $(d_A, Q_A) = (X, Y)$ dan pasangan kunci Bob $(d_B, Q_B) = (X, Y)$

a. **Alice's public point** $(\boldsymbol{Q} = \boldsymbol{d}.\boldsymbol{G})$ $(\boldsymbol{X}, \boldsymbol{Y})$

   61368183515432999791942231510419692409473533315735053019205557541828036827997
   29017125600637541663330393347717447521906557369219427507668092462875498193601
b. **Bob's public point** $(\boldsymbol{Q} = \boldsymbol{d}.\boldsymbol{G})$ $(\boldsymbol{X}, \boldsymbol{Y})$
   95677274946659838963303419671813122727966191708115920103532320706843258977851
   17208849337173536564769101530105675071932516819394197019341837952228969100849

Step 3. Langkah penghitungan, Alice menghitung poin $d_A Q_B$ serta Bob menghitung poin $d_B Q_A$dimana rahasia bersama adalah xk (koordinat x poin) dan sebagian besar protokol standar didasarkan pada ECDH yang diturunkan dari kunci simetris xk menggunakan beberapa fungsi derivasi kunci berbasis hash

a. **Alice's secret key** $\boldsymbol{S} = \boldsymbol{d_A Q_B} = \boldsymbol{d_A}.\boldsymbol{d_B}.\boldsymbol{G}$ $(\boldsymbol{X}, \boldsymbol{Y})$:
   43162763789784827943093991953088973222325560789113850755924705569579541548738

217791790862033704544831759148402254618407774696035971901197602613525
5900396

b. Bob's secret key $S = d_B Q_A = d_B . d_A . G\ (X, Y)$:
43162763789784827943093991953088973222325560789113850755924705569579541548738
217791790862033704544831759148402254618407774696035971901197602613525
5900396

4. Kesimpulan

Dalam pekerjaan ini, kami memperkenalkan sistem keamanan data di bidang yang terbatas. Sistem yang diusulkan memiliki dinamika yang kaya sebagaimana yang dikonfirmasi oleh perangkat lunak yang mengimplementasikan algoritma pertukaran kunci ECDH dan algoritma dekripsi-enkripsi telah berhasil dibangun. Perangkat lunak ini dapat mengirim pesan sms (kunci atau teks sandi) dan menerima data dengan baik. Kami juga menunjukkan contoh proses enkripsi dan dekripsi dengan algoritme yang tidak akan mungkin dilakukan tanpa kunci yang dihasilkan dari proses pertukaran kunci menggunakan algoritme ECDH. Penelitian lebih lanjut dapat dilakukan untuk menemukan aplikasi potensial dalam rekayasa komunikasi dan kriptosistem untuk algoritma kriptografi pasca-kuantum yang digunakan untuk membangun kunci rahasia antara dua pihak melalui saluran komunikasi yang tidak aman.

Referensi

[1] Shamir, A. "New directions in croptography." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2162*, 159. https://doi.org/10.1007/3-540-44709-1_14, 2001.

[2] Kumar, R., Ravindranath, C. C. "Analysis of Diffie-Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm." *International Journal of Emerging Trends Technology in Computer Science (IJETTCS),* vol. no. 1, p. 40-43, 2015.

[3] Nagaraj, S., Raju, G. S. V. P., Srinadth, V. "Data encryption and authetication using public key approach." *Procedia Computer Science*, vol 48, p.126-132. https://doi.org/10.1016/j.procs.2015.04.161, 2015.

[4] Susanto, D. R., Muchtadi-Alamsyah, I , (2016), "Implementation of Elliptic Curve Cryptography in Binary Field." Journal of Physics: Conference Series, vol.710, no. 1, https://doi.org/10.1088/1742-6596/710/1/012022.

[5] Kumar, R., Ravindranath, C. C., (2015), "Analysis of Diffie-Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm." International Journal of Emerging Trends Technology in Computer Science (IJETTCS), vol. no. 1, p. 40-43.

[6] Saepulrohman A., Negara, T.P. "Implementation of Elliptic Curve Diffie-Hellman (ECDH) for Encoding Messeges Becomes a Point on the GF(p)." *International Journal of Advanced Science and Technology* , 29(6), p. 3264-3273, 2020.

[7] Saepulrohman, A., Guritman, S., Silalahi, B. P. "Dekoding Sindrom Kode Gilbert-Varshamov Biner Berjarak Minimum Rendah." *Journal of Mathematics and Its Applications,* vol 14, no.1, p. 41-54 https://doi.org/10.29244/jmap.14.1.41-54 , 2015.

[8] Sonnino, A., & Sonnino, G. "Elliptic-Curves Cryptography on High- Dimensional Surfaces." *International Journal of Advanced Engineering Research and Science (IJAERS),* vol. 4, no. 2. https://dx.doi.org/10.22161/ijaers.4.2.28, 2017.

[9] Saudy, N. F., Ali, I. A., Barkouky, R. Al. "Error analysis and detection procedures for elliptic curve cryptography." *Ain Shams Engineering Journal*, vol. 10, no. 3, p. 587-597. https://doi.org/10.1016/j.asej.2018.11.007, 2019.

[10] Weng, J., Dou, Y., Ma, C. “Research on attacking a special elliptic curve discrete logarithm problem.“ *Mathematica. Problems in Engineering*, https://doi.org/10.1155/2016/5361695, 2016.

[11] Myasnikov, A. G., Roman Kov, V. “Verbally closed subgroups of free groups.” *Journal of Group Theory* vol. 17, no. 1, p. 29-40. https://doi.org/10.1515/jgt-2013-0034, 2014.

[12] Susantio, D. R., Muchtadi-Alamsyah, I. “Implementation of Elliptic Curve Cryptography in Binary Field.” *Journal of Physics: Conference Series*, vol.710, no. 1, https://doi.org/10.1088/1742-6596/710/1/012022, 2016.

[13] Johnson, D., Menezes, A., & Vanstone, S. *The Elliptic Curve Digital Signature Algorithm Validation System (ECDSAVS)*. 56. http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf, 2004.

[14] Verma, S. K., Ojha, D. B. “A Discussion on Elliptic Curve Cryptography and Its Applications.” *International Journal of Computer Science Issues 2012*, vol. 9, no. , p. 74-77. 2012.

[15] Bisson, G., Sutherland, A. V. “Computing the endomorphism ring of an ordinary elliptic curve over a finite field.” *Journal of Number Theory*, vol. 131, no.5, p. 815-831. https://doi.org/10.1016/j.jnt.2009.11.00, 2011.

[16] Kefa R. “Elliptic Curve Cryptography over Binary Finite Field GF(2^m).” *Information Technology Journal,* vol. 5, no.1, p. 204-229. 2006.

[17] Lopez, J., Dahab, R. “Fast multiplication on elliptic curves over GF(2^m) without precomputation.” *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Articial Intelligence and Lecture Notes in Bioinformatics),* 1717(107), p. 316-327. https://doi.org/10.1007/3-540-48059-527, 1999.

[18] King, B. “An improved implementation of elliptic curves over gf(2^n) when using projective point arithmetic.” *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Arti_cial Intelligence and Lecture Notes in Bioinformatics)*, 2259(1), p. 134-150. https://doi.org/10.1007/3-540-45537-x11, 2001.

[19] Saepulrohman A., Negara, T.P. “Elliptic Curve Diffie-Hellman Cryptosystem for Public Exchange Process.” *Proceedings of the 5th NA International Conference on Industrial Engineering and Operations Management,* Detroit, Michigan, USA, August 10 - 14, 2020

[20] --------.“JavaScript ECDH Key Exchange Demo", http://www-cs-students.stanford.edu/~tjw/jsbn/ecdh.html.Diakses 04 Januari 2020.

[21] --------.“Digital Signature, ECDSA, and EdDSA", https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/content/digital-signatures.html. Diakses 04 Januari 2020.