Enkripsi Data Dengan Mengunakan Metode ECC (*Elliptic Curve Cryptography*)

Tutuk Indriyani[1], Panji Dinasti Airlangga[2], Fandi Jaka[3]
Institut Teknologi Adhi Tama Surabaya[1,2,3]
e-mail correspondent author: tutuk@itats.ac.id

ABSTRACT

In order to prevent undesirable things from happening, such as the manipulation of sales transaction report data by their own employees, the researchers created an encrypted data security system for their sales transaction reports. This sales data encryption is hoped to help solve the problem of sales transaction report data leakage experienced by shop owners. so that shop owners who carry out the transaction process do not need to worry about their sales transaction report data being accessible to unauthorized parties or Rohmat shop employees who want to cheat regarding sales transaction reports. The solution to overcome this was to create a cryptographic system. One cryptographic method that provides a solution to information security problems is the Elleptic Curve Cryptography (ECC) method. The Elleptic Curve Cryptography (ECC) method is a cryptographic method that provides free public key solutions. The results of testing this method showed that the method worked quite well because the results showed that from the 20 data that had been tested using the avalanche effect, the smallest value was 6.54%, the largest was 22% and the average Avalanche Effect value was also obtained at 11.283%. The higher the average value obtained, the better this method will be applied.

Keywords*: Cryptography, Encryption, Elleptic Curve Cryptography, Sales Data.*

ABSTRAK

Dalam mencegah hal-hal yang tidak diinginkan terjadi seperti termanipulasinya data laporan transaksi penjualan oleh karyawanya sendiri, sehingga peneliti membuat sistem keamanan data terenkripsi pada laporan transaksi penjualanya. Enkripsi data penjualan ini dengan harapan dapat membantu menyelesaikan masalah kebocoran data laporan transaksi penjualan yang dialami oleh pemilik toko. sehingga pemilik toko yang melakaukan proses transaksi tidak perlu khawatir terkait data laporan transaksi penjualannya yang dapat diakses oleh pihak yang tidak memiliki kepentinga atau karyawan toko rohmat yang ingin berbuat curang soal laporan transaksi penjualan. Solusi untuk mengatasi hal tersebut maka dibuatlah sebuah sistem kriptografi. salah satu metode kriptografi yang memberikan solusi untuk masalah keamanan informasi adalah metode *Elleptic Curve Crytptography* (ECC). Metode *Elleptic Curve Crytptography* (ECC) adalah metode kriptografi yang memberikan solusi kunci public secara bebas. Hasil dari pengujian metode ini mendapatkan metode berjalan dengan cukup baik karena hasil menunjukkan dari 20 data yang sudah di uji mengunakan *avalanche effect* nilai terkecil adalah 6,54%, terbesar adalah 22% dan di dapatkan juga nilai rata - rata Avalanche Efeect sebesar 11,283%. Semakin tinggi nilai rata-rata yang didapatkan akan semakin baik metode ini diterapkan.

Kata kunci: Kriptografi, Enkripsi, *Elleptic Curve Cryptography*, Data Penjualan.

PENDAHULUAN

Dalam penelitian ini akan memanfaatkan transaksi mengacu pada pertukaran barang atau jasa dengan uang. Data transaksional mencakup semua detail yang terkait dengan pertukaran ini, termasuk tanggal transaksi, jumlah, dan instrumen yang digunakan seseorang untuk menyelesaikan penjualan. Mempelajari lebih lanjut data transaksional dapat membantu Anda membuat keputusan bisnis yang lebih baik. Dalam artikel ini, kami menjawab pertanyaan "Apa itu data transaksional", menyoroti pentingnya data tersebut, menjelaskan siapa yang menggunakannya, membuat daftar jenisnya, mengeksplorasi tantangan dalam menggunakannya, dan berbagi praktik terbaik dalam menggunakannya[1]. Data laporan transaksi penjulanya atau kebocoran data pada laporan transaksi

penjualanya dan juga dikarenakan karyawan yang ada di toko rohmat ini lebih dari satu orang maka untuk mencegah hal yang tidak diinginkan terjadi seperti termanipulasinya data laporan transaksi penjualan oleh karyawan – karyawanya sendiri. Agar hal seperti itu tidak terjadi lagi di toko rohmat, peneliti akan membuat sistem keamanan data terenkripsi [2].

Solusi untuk mengatasi hal tersebut maka dibuatlah sebuah sistem kriptografi. salah satu metode kriptografi yang memberikan solusi untuk masalah keamanan informasi adalah metode *Elleptic Curve Crytptography* (ECC). Kriptografi Kurva Elliptic memiliki tingkat keamanan yang lebih baik. Sistem kriptografi kurva elips memberikan perlindungan yang lebih kuat dan lebih baik daripada algoritma enkripsi lainnya dalam mencegah serangan, membuat situs web dan infrastruktur lebih aman dibandingkan metode enkripsi tradisional, memungkinkan ECC memberikan jaminan yang lebih baik untuk keamanan Internet seluler. Kedua, kriptografi kurva elips lebih baik untuk Internet seluler. Kriptografi kurva elips memiliki kunci yang relatif pendek yaitu 256 bit[3].

Salah satu teknik Salah satu kelemahan utama kriptografi kunci publik adalah membutuhkan terlalu banyak komputasi dan menghabiskan terlalu banyak energi dan waktu, sehingga peningkatan akselerator sangat diperlukan untuk meningkatkan efisiensi enkripsi dan dekripsi kurva elips serta pembangkitan kunci Mahasiswa dalam dan luar negeri yang memiliki banyak pengalaman dalam kriptografi kurva elips berkomitmen untuk meneliti cara meningkatkan efisiensi dan secara bertahap menemukan akselerator yang lebih sesuai. untuk kriptografi kurva elips. Misalnya, metode ASIC dapat digunakan untuk merancang dan mengimplementasikan akselerator perangkat keras[2].

Dalam tahap pengujian untuk proses enkripsi dan deskripsi dalam penelitian ini, peneliti mendapatkan data dari keseluruhan prosesnya yaitu mengunkan *Avalanche Effect*. *Avalanch Effect* sendiri adalah sebuah cara agar bisa mengetahui tingkat keakuratan dalam algoritma kriptografi dengan mengunakan metode *Elliptic Curve Cryptography*. Dengan menggunakan sistem pengujian ini supaya dapat mengetahui bahwa metode ini memiliki akurasi yang baik [4].

TINJAUAN PUSTAKA

A. Pentingnya Data Transaksi

Kita semua telah melihat apa yang terjadi ketika perlindungan gagal. Logo target Corp. yang terkenal berwarna merah dan biru ketika penjahat dunia maya membobol data konsumen. Lebih dari 70 juta pelanggan terkena dampaknya, diikuti dengan penyelesaian gugatan class action senilai $10 juta. Ketidakpercayaan konsumen selanjutnya sangat beragam. Namun, ada banyak hal yang dapat dilakukan oleh bisnis. Meskipun perusahaan rintisan mungkin tidak memiliki volume data yang cukup untuk mendukung CRM di cloud, bisnis kecil yang sudah matang dan perusahaan skala menengah yang sedang tumbuh agresif memilikinya. Menurut Trackvia.com, teknologi CRM meningkatkan pendapatan sebesar 41 persen. Masuk akal mengapa perusahaan yang haus akan pertumbuhan mengandalkan CRM untuk membina hubungan pelanggan. Sebagai arsitek solusi Salesforce, kami melihat perusahaan memulai dengan sebuah mimpi ketika mimpi itu terwujud, data tumbuh secara eksponensial. Pertimbangkan ini mengakses informasi melalui komputer. Begitu juga dengan bank Anda, sekolah anak Anda, dan pengecer online favorit Anda. Semua data sensitif tersebut dikumpulkan dalam penyimpanan data besar lemari arsip virtual dengan aliran data dari berbagai sumber, kontrol akses, dan masalah kepatuhan keamanan data. Data CRM menuntut integritas, akurasi, dan keamanan. Nyawa dan penghidupan masyarakat menjadi taruhannya[5].

B. Kriptografi

Ketika informasi rahasia dikirim secara elektronik dari satu individu ke individu lain, suatu bentuk enkripsi harus digunakan untuk melindungi informasi dari pengintip. Karena teknologi internet

bergantung pada transmisi data melalui domain publik, enkripsi ini sangat penting untuk menjaga keamanan informasi yang dikirimkan secara elektronik. Enkripsi kunci publik, yang pertama kali dikembangkan pada tahun 1970an, secara bertahap mendominasi "pasar kriptologi" karena keunggulan inherennya dibandingkan metode kunci privat dalam mengenkripsi data; Berbeda dengan enkripsi kunci publik, enkripsi kunci publik tidak mengharuskan individu berbagi kunci rahasia[6]. Meskipun algoritma enkripsi kunci publik seperti RSA telah diterima secara universal di arena kriptologi modern, algoritma ini tetap rentan terhadap banyak potensi ancaman keamanan. Misalnya, karena enkripsi kunci publik melibatkan "penerima" yang menyediakan kunci publik kepada "pengirim" mana pun yang ingin mengiriminya informasi rahasia (penerima menggunakan kunci pribadi yang berbeda untuk mendekripsi data), hal ini sangat mungkin terjadi karena suatu alasan. individu untuk mengirim pesan terenkripsi kepada penerima yang tampaknya dikirim dari orang lain; lagi pula, kunci publik yang digunakan untuk mengenkripsi pesan ini tersedia sepenuhnya untuk semua orang. Dengan kata lain, sistem enkripsi publik seperti RSA pada dasarnya tidak melindungi terhadap identifikasi pengirim palsu[2]. Meskipun teknik penandatanganan digital ini secara teoritis dapat dilakukan, algoritma kunci publik yang mendasarinya umumnya terlalu tidak efisien dan memerlukan terlalu banyak komputasi untuk digunakan dalam implementasi praktis. Untuk menghemat waktu, protokol tanda tangan digital menggunakan "fungsi hashing satu arah" untuk menghasilkan tanda tangan pengirim untuk dokumen tertentu. Penerapan teknik ini cukup sederhana: pengirim pertama-tama membuat "hash satu arah" dari dokumen yang ingin dia kirim dan mengenkripsi hash ini dengan kunci pribadinya.

Pengirim kemudian mengenkripsi dokumen itu sendiri dengan kunci publik penerima dan mengirimkan dokumen tersebut, bersama dengan hash yang "ditandatangani", ke penerima. Penerima mendekripsi dokumen (dengan kunci pribadinya) dan menerapkan hash satu arah yang sama padanya. Terakhir, dia menerapkan kunci publik pengirim ke hash yang "ditandatangani" (hash yang dikirimkan kepadanya). Tanda tangan divalidasi jika hash yang dihasilkan penerima dari dokumen cocok dengan hash "ditandatangani" yang didekripsi yang dia terima dari pengirim. Teknik hashing satu arah untuk menghasilkan tanda tangan digital ini memiliki beberapa keunggulan dibandingkan teknik penandatanganan sederhana yang dijelaskan sebelumnya. Salah satu fitur penting dari hashing satu arah adalah memungkinkan pengirim untuk "menandatangani" hanya sebagian kecil dari dokumen asli, sehingga sangat mengurangi waktu yang dibutuhkan untuk "mempersiapkan" (mengenkripsi) dokumen untuk pengiriman. Manfaat lain dari protokol ini adalah tanda tangan digitalnya dapat disimpan terpisah dari dokumen aslinya [4].

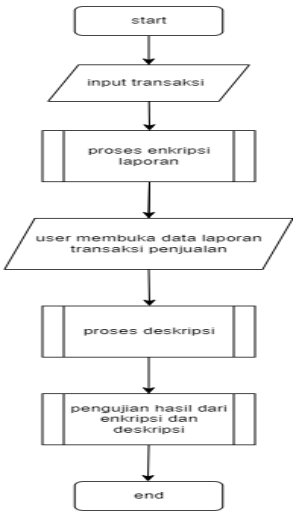
C. *Elliptic Curve Criptografy* (ECC)

Pertama, Kriptografi Kurva Elliptic memiliki tingkat keamanan yang lebih baik. Sistem kriptografi kurva elips memberikan perlindungan yang lebih kuat dan lebih baik daripada algoritma enkripsi lainnya dalam mencegah serangan, membuat situs web dan infrastruktur lebih aman dibandingkan metode enkripsi tradisional, memungkinkan ECC memberikan jaminan yang lebih baik untuk keamanan Internet seluler [4]. Kedua, kriptografi kurva elips lebih baik untuk Internet seluler. Kriptografi kurva elips memiliki kunci yang relatif pendek yaitu 256 bit, sehingga memakan lebih sedikit ruang penyimpanan. Karena semakin banyak pengguna menggunakan perangkat seluler untuk menyelesaikan berbagai aktivitas online, kriptografi kurva elips memberikan pengalaman pelanggan yang lebih baik untuk keamanan Internet seluler. Ketiga, Kriptografi Kurva Elliptik mempunyai sifat yang lebih baik. Kriptografi kurva elips dapat memberikan keamanan yang lebih baik dengan panjang kunci yang lebih pendek. Misalnya, kekuatan kunci kriptografi kurva elips 256-bit hampir sama dengan kekuatan kunci RSA 3072-bit (saat ini, panjang kunci RSA normal adalah 2048 bit). Menurut pengujian otoritas asing terkait, waktu respons server Web sepuluh kali lebih cepat dibandingkan RSA saat menggunakan algoritma ECC pada server Apache dan IIS [7].

Dikombinasikan dengan perkalian kompleks, metode kriptografi, mudah untuk menemukan kurva elips, tetapi untuk lebih memperkuat keamanan sistem kata sandi, kriptografi, kurva elips cenderung dihasilkan secara acak. Namun kurva elips yang dibutuhkan oleh kriptografi kurva elips harus memiliki orde yang sama, sehingga polarisasi keteraturan menjadi efek penting dalam menghasilkan kurva elips[8]. Pada tahun 1984, Schoof dengan algoritma waktu polinomial diusulkan untuk menghitung urutan metode kurva elips, namun kinerja sebenarnya dari algoritma tersebut sangat buruk, sehingga penulis tidak dapat memperoleh aplikasi praktis dalam kriptografi kurva elips. Kemudian, Elkie mengemukakan bilangan prima Elkie dan bilangan prima Atkins, kay dalam bidang berhingga memiliki konteks yang lebih besar, algoritma diusulkan, dan sangat meningkatkan efisiensi perhitungan tatanan kurva elips. Demikian pula Lecier mengusulkan metode penggunaan bentuk cara hitung efeknya, yang memiliki hasil serupa dengan . Kemudian, algoritma yang lebih efisien dikemukakan oleh Satoh, Harley dan juga memberikan promosi yang sama mengenai metode perhitungan yang sederhana dan efektif untuk menghitung efek yang lebih luar biasa. Sejauh ini, masalah ini telah diselesaikan dengan hampir sempurna oleh beberapa kriptografer dan ahli matematika[9]

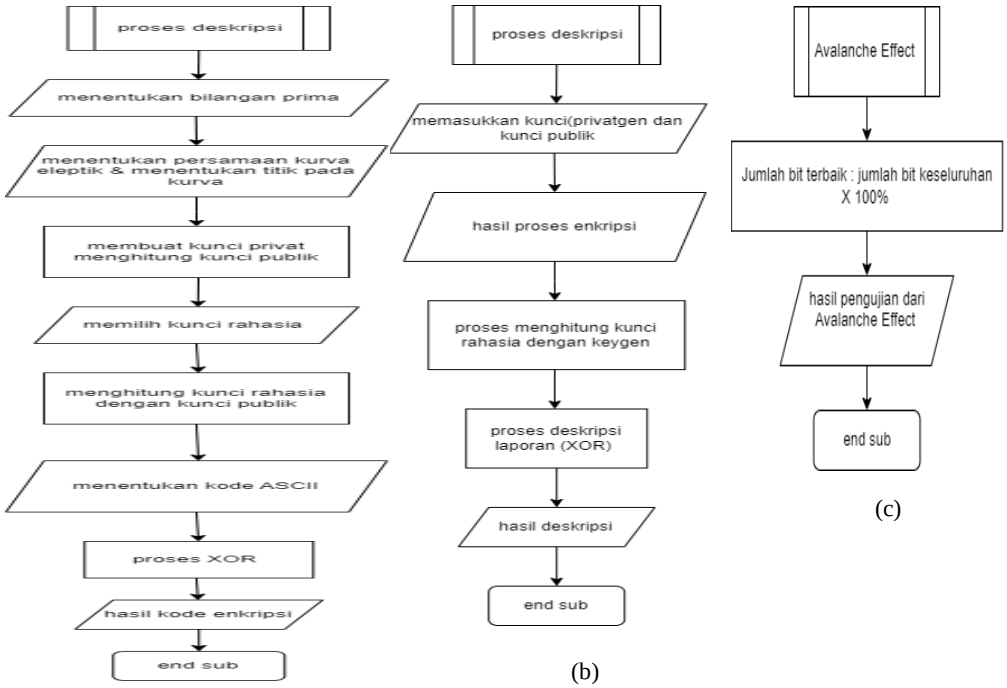
METODE

Pada proses ini pertama dilakukan input data transaksi, tahap kedua dilakukan proses enkripsi laporan, tahap ketiga dilakukan proses deskripsi dan proses terakhir dilakukan proses pengujian. Desain pada penelitihan ini ditunjukkan pada Gambar 1.



Gambar 1 Flowchart enkripsi dan deskripsi laporan transaksi penjualan

Dari gambar flowchart di atas dapat di jelaskan bahwa tahap pertama yaitu melakukan input transaksi jika ada sesorang yang mau membeli di toko rohmat. Input transaksinya sendiri berupa total harga yang customer beli.



Gambar 2 (a) Flowchart proses enkripsi (b) Flowchart proses dekripsi (c) Flowchart pengujian

Penjelasan Gambar 2 a. Proses *enkripsii* ini bekerja sesuai transaksi yang masuk, misalnya seseorang ingin membeli barang di toko rohmat dengan nilai total harga yang dibeli 500.000 ribu, maka ketika transaksi itu sudah masuk, maka sistem secara otomatis melakuan proses *enkripsi*, dengan demikian maka harga input yang aslinya 500.00 ribu berubah ketika ada di table database menjadi angka yang acak. Ketika ingin membuka data yang sudah *terenkripsi* tersebut maka user atau pengguan harus mendownloadnya agar yang tadinya angka yang acak dan tidak bisa dibaca Kembali terbuka dan bisa terbaca lagi.

Penjelasan pada Gambar 2 b. Proses *deskripsi* yaitu proses dimana user atau pengguna ingin membuka data yang sudah terenkripsi sebelumnya,caranya adalah user harus mendownload laporan transaksi penjualnya, ketika user mendownloadnya sistem akan otomatis melakukan proses *deskripsi* dan output dari *deskripsi* sendiri yaitu berupa file pdf yang nanti dapat dibaca dengan mudah oleh user mencakup total pembeli dan total keseluruhan yang didapat, yang awalnya angka acak *(enkripsi)* di tabel database akan bisa terbaca lagi oleh user setelah melakukan proses *deskripsi* tersebut.

Penjelasan pada Gambar 2 c. Pengujin sistem, setelah melakukan proses *enkripsi* maupun *deskripsi* akan dibuat suatu pengujian dimana pengujian ini bertujuan untuk mengetahui tingkat efektifitas dari sistem enkripsi atau deskripsi yang telat dibuat mengunakan metode *ECC(Elliptic Curve Cryptography)*, untuk melakukan pengujian ini yaitu mengunakan *avalanche effect*, dan akan dihitung secara manual sesuai jumlah data yang peneliti inginkn, pengujianya akan mengambil data yang sudaah dienkripsi di dalam table databse[10].

HASIL DAN PEMBAHASAN

Pada skenario ini akan mengunakan *Avalanche Effect* untuk proses enkripsi maupun deskripsi yang saya buat, untuk mendapatkan data dari keseluruhan prosesnya, dalam pengujian ini akan melakukan pengujian dari 20 item transaksi, untuk mengetahui tingkat efektifitas enkripsi pada aplikasi laporan transaksi penjualan dengan mengunakan algoritma kriptografi dengan mengunakan metode *Elleptic Curve Crytptography* (ECC). Karena nilai *Avalanche Effect* yang cukup tinggi akan membuktikan bahwa implementasi *Elleptic Curve Crytptography* (ECC) cocok digunakan untuk aplikasi enkripsi laporan transaksi penjualan ini.

Tabel 1. Hasil enkripsi laporan transaksi

Data ke-	Total transaksi	Enkripsi total transaksi	Enkripsi
1	Rp. 50.000	26*^|9*^|12*^|12*^|12*^|12*^|12	Berhasil *dienkripsi*
2	Rp. 150.000	26*^|8*^|12*^|12*^|12*^|12	Berhasil *dienkripsi*
3	Rp. 50.000	26*^|9*^|12*^|12*^|12*^|12	Berhasil *dienkripsi*
4	Rp. 120.000	26*^|13*^|9*^|12*^|12*^|12*^|12	Berhasil *dienkripsi*
5	Rp. 40.000	26*^|13*^|12*^|12*^|12*^|12*^|12	Berhasil *dienkripsi*
6	Rp. 40.000	26*^|11*^|10*^|9*^|12*^|12	Berhasil *dienkripsi*
7	Rp. 1.500.000	26*^|13*^|12*^|11*^|14*^|12*^|12	Berhasil *dienkripsi*
8	Rp. 500.000	26*^|13*^|15*^|9*^|15*^|12*^|12	Berhasil *dienkripsi*
9	Rp. 500.000	26*^|15*^|4*^|9*^|12*^|12*^|12	Berhasil *dienkripsi*
10	Rp. 5.000.000	26*^|9*^|15*^|11*^|9*^|12*^|12	Berhasil *dienkripsi*
11	Rp. 100.000	26*^|5*^|13*^|13*^|12*^|12	Berhasil *dienkripsi*
12	Rp. 100.000	26*^|8*^|12*^|11*^|8*^|12*^|12	Berhasil *dienkripsi*
13	Rp. 50.000	26*^|10*^|15*^|9*^|15*^|12*^|12	Berhasil *dienkripsi*
14	Rp. 50.000	26*^|9*^|8*^|9*^|12*^|12*^|12	Berhasil *dienkripsi*
15	Rp. 1.500	26*^|13*^|12*^|15*^|5*^|12*^|12*^|12	Berhasil *dienkripsi*
16	Rp. 12.000	26*^|13*^|4*^|4*^|5*^|12*^|12	Berhasil *dienkripsi*
17	Rp. 107.200	26*^|13*^|13*^|15*^|9*^|15*^|12*^|12	Berhasil *dienkripsi*
18	Rp. 107.200	26*^|8*^|15*^|10*^|9*^|12*^|12	Berhasil *dienkripsi*
19	Rp. 112.500	26*^|5*^|14*^|9*^|12*^|12*^|12	Berhasil *dienkripsi*
20	Rp. 112.500	26*^|13*^|4*^|4*^|9*^|12*^|12*^|12	Berhasil *dienkripsi*

Tabel 1 menjelaskan ketika ada pembeli dan akan melakukan sebuah transaksi maka setelah melakukan pembayaran otomatis sistem akan melakukan proses *enkripsi* transaksi tersebut kedalam database dan tersimpan, dengan contoh data transaksi misalnya “500000” dan data tersebut sebagai *plaintext* maka setelah transaksi tersebut berhasil dilakukan dan masuk kedalam database yang awalnya 500000 akan menjadi angka acak seperti ini (**26*^|9*^|12*^|12*^|12*^|12*^|12**) dan angka acak tersebut dinamakan *chipertext, b*egitupun seterusnya sampai ada transaksi-transaksi selanjutnya. Pada Tabel 1 menunjukkan tabel dari database sistem yang juga menunjukkan keberhasilan enkripsi atau terbukti kalau sistem melakukan enkripsi sesuai dengan alur yang peneliti rancang. Hal ini akan membuat aplikasi lebih aman dari pengambilandata secara langsung oleh pihak yang tidak mempunyai wewenang atau biasa disebut hacker. Untuk prose hasil dekripsi dapat dilihat pada Tabel 2.

Tabel 2. Hasil deskripsi laporan tansaksi

Data ke-	Kategori	Produk	Tanggal	Ter jual	Total
1	Bahan bangunan	Semen 50kg	01 February 2023	1	Rp. 50.000
2	Bahan bangunan	Semen 50kg	06 February 2023	3	Rp. 150.000
3	Bahan bangunan	Semen 50kg	14 February 2023	1	Rp. 50.000
4	Bahan bangunan	Keramik 40x40	01 February 2023	3	Rp. 120.000
5	Bahan bangunan	Keramik 40x40	06 February 2023	1	Rp. 40.000
6	Bahan bangunan	Keramik 40x40	14 February 2023	1	Rp. 40.000
7	Bahan bangunan	Cat Nippon paint 20kg	01 February 2023	3	Rp. 1.500.000
8	Bahan bangunan	Cat nippon paint 20kg	06 February 2023	1	Rp. 500.000
9	Bahan bangunan	Cat nippon paint 20kg	12 February 2023	1	Rp. 500.000
10	Bahan bangunan	Cat nippon paint 20kg	14 February 2023	10	Rp. 5.000.000
11	Bahan bangunan	Triplek 3mm	01 February 2023	2	Rp. 100.000
12	Bahan bangunan	Triplek 3mm	06 February 2023	2	Rp. 100.000
13	Bahan bangunan	Pipa pvc 2inci	01 February 2023	1	Rp. 50.000
14	Bahan bangunan	Pipa pvc 2inci	06 February 2023	1	Rp. 50.000
15	Bahan bangunan	Batu bata merah (20 x 10 x 5cm)	12 February 2023	1	Rp. 1.500
16	Bahan bangunan	Batu bata merah (20 x 10 x 5cm)	14 February 2023	8	Rp. 12.000
17	Bahan bangunan	Besi beton 10 SRB SNI	12 February 2023	2	Rp. 107.200
18	Bahan bangunan	Besi beton 10 SRB SNI	14 February 2023	2	Rp. 107.200
19	Bahan bangunan	Asbes harvlex	12 February 2023	3	Rp. 112.500
20	Bahan bangunan	Asbes harvlex	14 February 2023	3	Rp. 112.500

Pada Tabel 2. proses *deskripsi* yang dilakukan oleh system secara otomatis ketika melakukan download laporan. Yang dimaksud dari bagian proses *deskripsi* di sini adalah pada saat akan di tampilkan atau mendownload laporan otomatis data akan *terdekripsi* dari sistem, dan untuk outputnya yaitu berupa file dengan format "pdf", karena hasil total pembelian ada pembeli yang melakukan transaksi produk yang berbeda-beda maka hasil total deskripsinya ada yang sama seperti enkripsi di atas ada juga yang berbeda. Meskipun begitu di *database* nya setiap produk akan di enkripsi biar tetap aman bukan hanya total produk pembelian saja, hal ini biar aman dari orang yang ingin memanipulasi data laporan tersebut, karena laporan dari transaksi penjualan ini penting bagi keberlangsungan Toko rohmat.

Dari 20 data yang sudah di selesaikan atau sudah di hitung sesuai rumus *avalanche effect* maka dibuatlah tabel seperti dibawah ini untuk mengetahui keseluruhan hasil pengujian tersebut.

Tabel 3. Hasil keseluruhan Pengujian *avalanche effect*

Data ke-	Jumlah keseluruhan *chipertext*	Jumlah bit yang terbalik	*Avalanche Effect (%)*
1	88	7	12,57%
2	72	6	12%
3	72	6	12%
4	88	7	12,57%
5	96	6	16%

Data ke-	**Jumlah keseluruhan *chipertext***	**Jumlah bit yang terbalik**	***Avalanche Effect (%)***
6	72	8	9%
7	96	6	16%
8	88	4	22%
9	80	8	10%
10	80	7	11,42%
11	72	6	12%
12	80	9	8,88%
13	80	11	8%
14	72	9	8%
15	104	11	9,45%
16	72	11	6,54%
17	104	9	11,55%
18	80	8	10%
19	80	9	8,88%
20	80	10	8,8%
	Rata - Rata		**11,283%**

Tabel 3. di atas dapat dijelaskan dari hasil pengujian di didapatkan nilai Avalanche Effect terkecil adalah 6,54%, Avalanche Effect terbesar adalah 22% dan di dapatkan juga nilai rata - rata Avalanche Efeect sebesar 11,283%. Untuk nilai rata - rata Avalanche Effect yang presentasenya atau nilainya cukup besar akan membuktikan bahwa aplikasi enkripsi laporan transaksi penjualan mengunakan algoritma kriptografi dengan metode *Elleptic Curve Crytptography* (ECC) berjalan dengan baik, karena semakin besar presentase yang didapatkan maka akan semakin baik aplikasi ini berjalan, untuk nilai rata-rata bisa bertambah dan juga menurun tergantung jumlah transaksi yang akan di dapat setiap harinya atau setiap bulannya, karena setiap pembeli mempunyai nilai transaksi yang berbeda-beda. Dan dapat disimpulkan bahwa metode *Elleptic Curve Crytptography* (ECC) cukup efektif untuk menyelesaikan enkripsi dan deskripsi laporan transaksi penjualan tersebut, karena nilai dari rata-rata tersebut bisa bertambah atau juga bisa turun tergantung pembeli melakukan sebuah transaksi di toko rohmat, karena disini yang sebagai plaintext atau yang di enkripsi adalah total harga dari pembelian yang masuk.

KESIMPULAN

Pembuatan aplikasi *enkripsi* dan *deskripsi* laporan transaksi penjualan mengunakan algoritma kriptografi dengan metode yang digunakan *ECC (Elleptic Curve Cryptography)* telah berhasil dikembangkan sesuai dengan alur yang sudah ditetapkan dari awal hingga akhir, mulai dari perhitungan manual *enkripsi* juga sampai di terapkan ke dalam aplikasi ini dan yang terakhir telah berhasil dilakukanya pengujian hasil enkripsinya mengunakan *avalanche effect*, dengan ketentuan rumus *avalanche effect.* Hasil dari pengujian aplikasi ini menandakan aplikasi berjalan dengan cukup baik karena hasil menunjukkan dari 20 data yang sudah di uji mengunakan *avalanche effect* nilai terkecil adalah 6,54%, terbesar adalah 22% dan di dapatkan juga nilai rata - rata Avalanche Efeect sebesar 11,283%.

DAFTAR PUSTAKA

[1] T. Indriyani, S. Nurmuslimah, A. Taufiqurrahman, R. K. Hapsari, C. N. Prabiantissa, and A. Rachmad, "Steganography on Color Images Using Least Significant Bit (LSB) Method," 2023, pp. 39–48. doi: 10.2991/978-94-6463-174-6_5.

[2] M. Reqica, D. Berisha, A. Jusufi, and M. Reqica, "Exploitation of exponential and logarithmic functions for data encryption and decryption," in *IFAC-PapersOnLine*, Elsevier B.V., Oct. 2022, pp. 286–291. doi: 10.1016/j.ifacol.2022.12.036.

[3] H. Abdulkudhur Mohammed and N. F. Hameed Al Saffar, "LSB based image steganography using McEliece cryptosystem," *Mater Today Proc*, Jul. 2021, doi: 10.1016/j.matpr.2021.07.182.

[4] O. Abolade *et al.*, "Overhead effects of data encryption on TCP throughput across IPSEC secured network," *Sci Afr*, vol. 13, Sep. 2021, doi: 10.1016/j.sciaf.2021.e00855.

[5] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Opt Lasers Eng*, vol. 124, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105837.

[6] K. Dhal, S. C. Rai, and P. K. Pattnaik, "LIKC: A liberty of encryption and decryption through imploration from K-cloud servers," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 2383–2390, Jun. 2022, doi: 10.1016/j.jksuci.2020.01.011.

[7] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos Solitons Fractals*, vol. 152, Nov. 2021, doi: 10.1016/j.chaos.2021.111318.

[8] X. Ma, B. Song, W. Lin, J. Wu, W. Huang, and B. Liu, "High-fidelity decryption technology of Visual Cryptography based on optical coherence operation," *Results Phys*, vol. 43, Dec. 2022, doi: 10.1016/j.rinp.2022.106065.

[9] D. Kumar, A. B. Joshi, and S. Singh, "A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system," *Results in Optics*, vol. 5, Dec. 2021, doi: 10.1016/j.rio.2021.100146.

[10] T. Indriyani, M. I. Utoyo, and R. Rulaningtyas, "A New Watershed Algorithm for Pothole Image Segmentation," *Studies in Informatics and Control*, vol. 30, no. 3, pp. 131–139, 2021, doi: 10.24846/v30i3y202112.