

Rancang Bangun Aplikasi Keamanan Data Penjualan Menggunakan Metode Elgamal Berbasis Web Pada PT. Pixelindo

Design and Development of Sales Data Security Applications Using the Web-Based Elgamal Method at PT. Pixelindo

Sudarman Ramadhani^{a,1}, Lili Tanti^{b,2}

^aProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^bProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

E-mail: sudarmanramadhani2811@gmail.com¹, lilitanti@gmail.com²

ABSTRAK

PT. Pixelindo memiliki jumlah transaksi penjualan begitu banyak dan memiliki jumlah pelanggan yang banyak dimana data tersebut input ke dalam *Microsoft Word* sehingga data-data tersebut harus tersimpan sehingga tidak ada nya kehilangan atau pencurian data-data transaksi yang mengakibatkan data-data tersebut di salah gunakan oleh pihak yang tidak berwajib. PT. Pixelindo belum memiliki sistem keamanan yang mampu mengamankan data penjualan sehingga data itu tidak hilang ataupun dicuri untuk kepentingan seseorang dan juga menjaga privasi pelanggan itu sendiri, dan terkadang pencurian data ini terjadi karena beberapa pihak ingin mengetahui proses penjualan dan ingin memiliki data pribadi pelanggan. Berdasarkan permasalahan diatas, penulis membuat sebuah aplikasi keamanan yang di mana menggunakan proses proses enkripsi dan dekripsi dalam sebuah data penjualan pada PT. Pixelindo. Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (chipertext) dan proses dekripsi merupakan proses mengubah pesan rahasia (ciphertext) menjadi pesan asli (plaintext) (Alfiah et al. 2020). Sistem yang dirancang menerapkan metode El-Gamal yang merupakan sistem enkripsi kunci asimetris yang ditemukan Taher El-Gamal pada tahun 1985 yang memiliki keunggulan teknologi pesan teks yang sama menghasilkan pesan teks rahasia yang berbeda setiap saat jika dienkripsi (Siambaton 2023). Hal ini dapat membantu pengamanan data penjualan yang berisi data pelanggan dan data transaksi pelanggan pada PT. Pixelindo, sehingga dapat memberikan perlindungan keamanan data penjualan yang lebih tinggi.

Kata Kunci : Printer, PT. Pixelindo, Keamanan Data, Penjualan

ABSTRACT

PT. Pixelindo has a large number of sales transactions and has a large number of customers where the data is input into *Microsoft Word* so that the data must be stored so that there is no loss or theft of transaction data which results in the data being misused by unauthorized parties. PT. Pixelindo does not yet have a security system that is able to secure sales data so that the data is not lost or stolen for someone's benefit and also maintains the privacy of the customer itself, and sometimes this data theft occurs because some parties want to know the sales process and want to have the customer's personal data. Based on the problems above, the author created a security application that uses encryption and decryption processes in sales data at PT. Pixelindo. The encryption process is the process of changing the original message (plaintext) into a secret message (ciphertext) and the decryption process is the process of changing the secret message (ciphertext) into the original message (plaintext) (Alfiah et al. 2020). The system designed applies the El-Gamal method which is an asymmetric key encryption system discovered by Taher El-Gamal in 1985 which has the advantage of the same text message technology producing different secret text messages every time if encrypted (Siambaton 2023). This can help secure sales data containing customer data and customer transaction data at PT. Pixelindo, so that it can provide higher sales data security protection.

Keywords : Printing, PT. Pixelindo, Data Security, Sales

Disubmit: 15 Agustus 2024

Direview: 25 September 2024

Diterima : 12 Oktober 2024

Copyright © 2024 – senadimu. All rights reserved

1. PENDAHULUAN

Perkembangan teknologi komputer saat ini telah mengalami tahapan kemajuan yang sangat pesat dan sudah menjadi suatu kebutuhan. Semakin tinggi tingkat teknologi komputer, semakin tinggi ancaman yang mengancam keamanan pengguna komputer. Salah satu dampak negatif dalam perkembangan teknologi adalah adanya pencurian data maka aspek yang di takuti oleh para pengguna jaringan komunikasi. Dengan adanya pencurian data maka aspek keamanan data dalam pertukaran informasi serta penyimpanan data sangatlah penting. Karena suatu komunikasi data jarak jauh, belum tentu aman dari pencurian sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri (Alfiah, Sudarji, and Al Fatah 2020).

Keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapatkan perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. (Yudistira 2022).

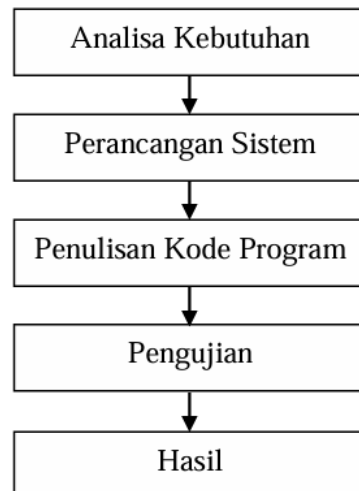
Pixelindo berdiri pada tahun 2002 dengan cabang pertama di Medan. Didirikan untuk memenuhi kebutuhan akan jasa refill toner, penjualan berbagai macam jenis printer inkjet & laser, sparepart inkjet & laser, sparepart toner, cartridge remanufaktur, servis printer inkjet & laser, pasang infus, tinta inkjet, dye, pigment & sublimation ink (pixelindo.com).

PT. Pixelindo memiliki jumlah transaksi penjualan begitu banyak dan memiliki jumlah pelanggan yang banyak dimana data tersebut input ke dalam *Microsoft Word* sehingga data-data tersebut harus tersimpan sehingga tidak ada nya kehilangan atau pencurian data-data transaksi yang mengakibatkan data-data tersebut di salah gunakan oleh pihak yang tidak berwajib. PT. Pixelindo belum memiliki sistem keamanan yang mampu mengamankan data penjualan sehingga data itu tidak hilang ataupun dicuri untuk kepentingan seseorang dan juga menjaga privasi pelanggan itu sendiri, dan terkadang pencurian data ini terjadi karena beberapa pihak ingin mengetahui proses penjualan dan ingin memiliki data pribadi pelanggan. Untuk menjaga keamanan suatu data dari ancaman yang dijelaskan diatas, maka diperlukan suatu aplikasi pengamanan data agar terhindar dari gangguan pelaku yang tidak bertanggung jawab. Sehingga pelaku yang tidak bertanggungjawab tidak dapat mengetahui isi dari data penjualan tersebut. Dalam penelitian ini sistem yang akan dibangun adalah mengubah data penjualan yang terdapat di dalam sebuah *File* dokumen kedalam bentuk yang tidak dapat dikenali agar kerahasiaannya dapat terjaga.

Berdasarkan permasalahan diatas, penulis membuat sebuah aplikasi keamanan yang di mana menggunakan proses enkripsi dan dekripsi dalam sebuah data penjualan pada PT. Pixelindo. Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (ciphertext) dan proses dekripsi merupakan proses mengubah pesan rahasia (ciphertext) menjadi pesan asli (plaintext) (Alfiah et al. 2020). Sistem yang dirancang menerapkan metode El-Gamal yang merupakan sistem enkripsi kunci asimetris yang ditemukan Taher El-Gamal pada tahun 1985 yang memiliki keunggulan teknologi pesan teks yang sama menghasilkan pesan teks rahasia yang berbeda setiap saat jika dienkripsi (Siambaton 2023). Hal ini dapat membantu pengamanan data penjualan yang berisi data pelanggan dan data transaksi pelanggan pada PT. Pixelindo, sehingga dapat memberikan perlindungan keamanan data penjualan yang lebih tinggi.

2. METODE

Tahapan dalam penelitian ini dapat di modelkan pada bgan alur penelitian. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar 1. Bagan Alur Penelitian

Keterangan dari bagan alur diatas adalah Menganalisa kebutuhan sistem yang sudah ada dan menambahkan sistem yang baru dalam perancangan bila ternyata dibutuhkan. Data yang diperlukan dalam analisa ini adalah data penjualan yang berisi data pelanggan, data produk dan data transaksi pelanggan. Penulisan kode program merupakan penerjemahan desain dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh programmer yang akan menterjemahkan transaksi yang diminta oleh user. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan dimaksimalkan dalam tahapan ini. Setelah pengkodean selesai maka akan dilakukan testing terhadap sistem yang telah dibuat tadi. Tujuan testing adalah menemukan kesalahan-kesalahan terhadap sistem tersebut dan kemudian bisa diperbaiki. Pada tahap ini dilakukan pengujian sistem secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian yang dilakukan yaitu pengujian perangkat lunak yang tes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi atau struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan, pengujian tersebut untuk masing-masing peralatan yang dirancang. Pada tahap ini program akan diterapkan untuk Rancang Bangun Aplikasi Keamanan Data Penjualan Menggunakan Metode Elgamal Berbasis Web Pada PT. Pixelindo dapat melakukan keamanan data penjualan sehingga tidak dapat dicuri dan tidak disalah gunakan oleh pihak lain.

3. HASIL DAN PEMBAHASAN

A. Penerapan Metode Elgamal

1. Algoritma Generate Key

Algoritma Elgamal merupakan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan dua buah bilangan acak (random) g dan x , dengan syarat bahwa nilai g dan x lebih kecil dari p yang memenuhi persamaan.

$$Y = g^x \bmod p \dots\dots\dots (2.1)$$

Dari persamaan II.1 nilai y, g dan p merupakan kunci public, sedangkan x, p merupakan pasangan kunci pribadi. Besaran-besaran digunakan dalam algoritma kriptografi Elgamal adalah:

- 1) P adalah bilangan prima dengan syarat $P > 255$
- 2) G adalah bilangan acak, dengan syarat G
- 3) X adalah bilangan acak, dengan syarat $X < P$
- 4) Y adalah hasil perhitungan dari $Y = G^x \text{ mod } P$
- 5) Lalu dihasilkan public key = y, g, p , dan private key = x, p

2. Algoritma Proses Enkripsi

Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (ciphertext). Pada proses ini digunakan public key (p, g, y). Langkah-langkah dalam mendekripsi pesan adalah sebagai berikut.

$$a = g^k \text{ mod } p \dots\dots\dots (2.2)$$

$$b = y^k \cdot m \text{ mod } p \dots\dots\dots (2.3)$$

- 1) Potong plaintext menjadi blok-blok m_1, m_2
- 2) Ubah nilai blok pesan ke dalam nilai ASCII
- 3) Pilih bilangan acak k , dengan syarat $1 \leq k \leq p-2$. Nilai k digunakan untuk menghitung nilai a dan b .
- 4) Setiap blok m dienkripsi dengan rumus sebagai berikut:

Nilai a (Gamma) = $g^k \text{ mod } p$

Nilai b (Delta) = $y^k \cdot m \text{ mod } p$

- 5) Susun ciphertext dengan urutan $a_1, b_1, a_2, b_2, \dots, a_N, b_N$

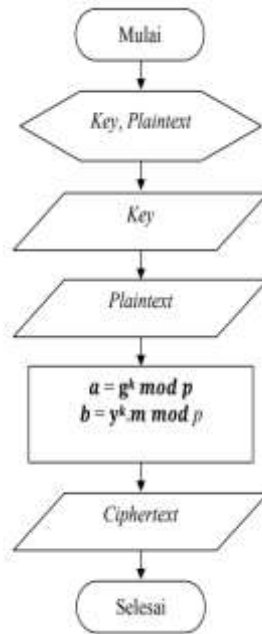
3. Algoritma Proses Dekripsi

Proses Dekripsi Merupakan proses mengubah pesan rahasia (ciphertext) menjadi pesan asli (plaintext). Proses dekripsi menggunakan kunci pribadi x dan p untuk mendekripsi a dan b menjadi plaintext (m) dengan persamaan:

$$M = b \cdot a^{(p-1-x)} \text{ mod } p \dots\dots\dots (II.4)$$

- 1) Penentuan nilai Gama dan Delta. Nilai Gamma(a) diperoleh dari ciphertext dengan urutan ganjil, sedangkan Delta(b) diperoleh urutan genap.
- 2) Hitung plaintext m dengan persamaan rumus tersebut.
- 3) Ubah nilai m yang didapat ke dalam nilai ASCII
- 4) Susun plaintext dengan urutan $m_1, m_2, \dots, m_N$ (Alfiah et al. 2020).

Flowchart enkripsi metode Elgamal dapat dilihat sebagai berikut :



Gambar 2. Flowchart Enkripsi Metode Elgamal.

Contoh proses enkripsi dari data konsumen :

A. Proses Enkripsi:

Langkah-langkah penyelesaian proses enkripsi data konsumen adalah sebagai berikut :

Diketahui:

Plaintext:

Tabel 1. Data Plaintext

Nama Pelanggan	Barang	Jumlah	Harga	Total
RAMA	Printer	2	2500000	5000000

Dalam plainteks sebelum melakukan proses enkripsi, ubah terlebih dahulu ke ASCII dari setiap huruf, Adapun nilai numeric sebagai berikut

Tabel 2. Data Plaintext

	Nama Pelanggan	Barang	Jumlah	Harga	Total
Plaintext	RAMA	PRINTER	2	2500000	5000000
Numeric (ASCII)	82,65,77,65	80,82,73,78,84,69,82	50	50,53,48,48,48,48,48	53,48,48,48,48,48,48

Nilai $p = 257$, $g = 7$ dan $x = 2$

Hitung $y = g^x \mod p$

$$y = 7^2 \mod 257$$

$$y = 49 \mod 257$$

$$y = 49$$

Berdasarkan proses pembangkit kunci, maka diperoleh:

Kunci PRIVATE = (x,y) Kpublic = (2, 257)

Kunci PUBLIC = (p,g,y) Kpublic = (257,7,49)

Nilai k yang dipilih harus berada dalam himpunan $1 \leq k \leq p-2$.

Berikut data dari nama pelanggan yaitu RAMA

Nilai k untuk P1 = 4

$$(R) = 82$$

$$a = g^k \bmod p$$

$$a = 7^4 \bmod 257$$

$$a = 2401 \bmod 257 = 88$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^4 \bmod P_1) \bmod 257$$

$$= 5764801 * 82 \bmod 257$$

$$= 472713682 \bmod 257$$

$$= 218$$

Nilai k untuk P2 = 3

$$(A) = 65$$

$$a = g^k \bmod p$$

$$a = 7^3 \bmod 257$$

$$a = 343 \bmod 257 = 86$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^3 \bmod P_3) \bmod 257$$

$$= 117649 * 65 \bmod 257$$

$$= 7647185 \bmod 257$$

$$= 150$$

Nilai k untuk P3 = 2

$$(R) = 77$$

$$a = g^k \bmod p$$

$$a = 7^2 \bmod 257$$

$$a = 49 \bmod 257 = 49$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^2 \bmod P_3) \bmod 257$$

$$= 2401 * 77 \bmod 257$$

$$= 184877 \bmod 257$$

$$= 94$$

Nilai k untuk P4 = 3

$$(A) = 65$$

$$a = g^k \bmod p$$

$$a = 7^3 \bmod 257$$

$$a = 373 \bmod 257 = 86$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^3 \bmod P_4) \bmod 257$$

$$= 117649 * 65 \bmod 257$$

$$= 7647185 \bmod 257$$

$$= 150$$

Tabel 3. Hasil Plaintext RAMA

Plainteks	Char	DEC	K	$a=(g^k) \bmod p$	$b=((y^k)*M) \bmod p$	(a,b)
P1	R	82	4	88	218	(88,218)
P2	A	65	3	86	150	(86,150)
P3	M	77	2	49	94	(49,94)
P4	A	65	3	86	154	(86,150)

Berikut data barang yaitu PRINTER

Nilai k untuk P1 = 4

$$(P) = 80$$

$$a = g^k \bmod p$$

$$a = 7^4 \bmod 257$$

$$a = 2401 \bmod 257 = 88$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^4 \bmod P_1) \bmod 257$$

$$= 5764801 * 80 \bmod 257$$

$$\begin{aligned} &= 461184080 \bmod 257 \\ &= 150 \\ \text{Nilai } k \text{ untuk } P2 &= 4 \\ (R) &= 82 \\ a &= g^k \bmod p & a &= 7^4 \bmod 257 \\ & & a &= 2401 \bmod 257 = 88 \\ b &= (y^k \bmod P_i) \bmod p \\ b &= (49^4 \bmod P1) \bmod 257 \\ &= 5764801 * 82 \bmod 257 \\ &= 472713682 \bmod 257 \\ &= 218 \\ \text{Nilai } k \text{ untuk } P3 &= 2 \\ (I) &= 73 \\ a &= g^k \bmod p & a &= 7^2 \bmod 257 \\ & & a &= 49 \bmod 257 = 49 \\ b &= (y^k \bmod P_i) \bmod p \\ b &= (49^2 \bmod P3) \bmod 257 \\ &= 2401 * 73 \bmod 257 \\ &= 175273 \bmod 257 \\ &= 256 \\ \text{Nilai } k \text{ untuk } P4 &= 4 \\ (N) &= 78 \\ a &= g^k \bmod p & a &= 7^4 \bmod 257 \\ & & a &= 2401 \bmod 257 = 88 \\ b &= (y^k \bmod P_i) \bmod p \\ b &= (49^4 \bmod P4) \bmod 257 \\ &= 5764801 * 78 \bmod 257 \\ &= 449654478 \bmod 257 \\ &= 82 \\ \text{Nilai } k \text{ untuk } P5 &= 2 \\ (T) &= 84 \\ a &= g^k \bmod p & a &= 7^2 \bmod 257 \\ & & a &= 49 \bmod 257 = 49 \\ b &= (y^k \bmod P_i) \bmod p \\ b &= (49^2 \bmod P5) \bmod 257 \\ &= 2401 * 84 \bmod 257 \\ &= 201684 \bmod 257 \\ &= 196 \\ \text{Nilai } k \text{ untuk } P6 &= 3 \\ (E) &= 69 \\ a &= g^k \bmod p & a &= 7^3 \bmod 257 \\ & & a &= 373 \bmod 257 = 86 \\ b &= (y^k \bmod P_i) \bmod p \\ b &= (49^3 \bmod P3) \bmod 257 \\ &= 117649 * 69 \bmod 257 \\ &= 8117781 \bmod 257 \\ &= 179 \\ \text{Nilai } k \text{ untuk } P7 &= 4 \\ (R) &= 82 \\ a &= g^k \bmod p & a &= 7^4 \bmod 257 \\ & & a &= 2401 \bmod 257 = 88 \end{aligned}$$

$$\begin{aligned}
 b &= (y^k \bmod P_i) \bmod p \\
 b &= (49^4 \bmod P_1) \bmod 257 \\
 &= 5764801 * 82 \bmod 257 \\
 &= 23162970418 \bmod 257 \\
 &= 145
 \end{aligned}$$

Tabel 4. Plaintext Hasil PRINTER

Plainteks	Char	DEC	K	$a=(g^k) \bmod p$	$b=((y^k)*M) \bmod p$	(a,b)
P1	P	80	4	88	150	(88,150)
P2	R	82	4	88	218	(88,218)
P3	I	73	2	49	256	(49,256)
P4	N	78	4	88	154	(88,82)
P5	T	84	2	49	196	49,196
P6	E	69	3	86	179	86,179
P7	R	82	4	88	145	88,145

Berikut data jumlah pembelian yaitu 2

Nilai k untuk P1 = 3

(P) = 50

$$a = g^k \bmod p$$

$$a = 7^3 \bmod 257$$

$$a = 343 \bmod 257 = 86$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^3 \bmod P_1) \bmod 257$$

$$= 117649 * 50 \bmod 257$$

$$= 5882459 \bmod 257$$

$$= 150$$

Tabel 5. Plaintext Hasil "2"

Plainteks	Char	DEC	K	$a=(g^k) \bmod p$	$b=((y^k)*M) \bmod p$	(a,b)
P1	2	50	3	86	243	(88,243)

Berikut data jumlah pembelian yaitu 2500000

Nilai k untuk P1 = 4

(P) = 50

$$a = g^k \bmod p$$

$$a = 7^4 \bmod 257$$

$$a = 2401 \bmod 257 = 88$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^4 \bmod P_1) \bmod 257$$

$$= 5764801 * 50 \bmod 257$$

$$= 288249959 \bmod 257$$

$$= 44$$

Nilai k untuk P2 = 2

(P) = 53

$$a = g^k \bmod p$$

$$a = 7^2 \bmod 257$$

$$a = 49 \bmod 257 = 49$$

$$b = (y^k \bmod P_i) \bmod p$$

$$b = (49^2 \bmod P_2) \bmod 257$$

$$= 2401 * 53 \bmod 257$$

$$= 127253 \bmod 257$$

$$= 38$$

Nilai k untuk P3 = 3

(P) = 48

$a = g^k \mod p$

$a = 7^3 \mod 257$

$a = 343 \mod 257 = 86$

$b = (y^k \mod P_i) \mod p$

$b = (49^3 \mod P3) \mod 257$

$= 117649 * 53 \mod 257$

$= 6235397 \mod 257$

$= 63$

Nilai k untuk P4 = 4

(P) = 48

$a = g^k \mod p$

$a = 7^4 \mod 257$

$a = 2401 \mod 257 = 88$

$b = (y^k \mod P_i) \mod p$

$b = (49^4 \mod P4) \mod 257$

$= 5764801 * 48 \mod 257$

$= 276710448 \mod 257$

$= 90$

Nilai k untuk P5 = 2

(P) = 48

$a = g^k \mod p$

$a = 7^2 \mod 257$

$a = 49 \mod 257 = 49$

$b = (y^k \mod P_i) \mod p$

$b = (49^2 \mod P5) \mod 257$

$= 2401 * 48 \mod 257$

$= 115248 \mod 257$

$= 150$

Nilai k untuk P6 = 3

(P) = 48

$a = g^k \mod p$

$a = 7^3 \mod 257$

$a = 343 \mod 257 = 86$

$b = (y^k \mod P_i) \mod p$

$b = (49^3 \mod P6) \mod 257$

$= 117649 * 48 \mod 257$

$= 564912 \mod 257$

$= 26$

Nilai k untuk P7 = 5

(P) = 48

$a = g^k \mod p$

$a = 7^5 \mod 257$

$a = 16807 \mod 257 = 102$

$b = (y^k \mod P_i) \mod p$

$b = (49^5 \mod P7) \mod 257$

$= 117649 * 50 \mod 257$

$= 5882459 \mod 257$

$= 150$

Tabel 6. Plaintext Hasil "2500000"

Plainteks	Char	DEC	K	$a=(g^k)\mod p$	$b=((y^k)*M)\mod p$	(a,b)
P1	2	50	4	88	44	(88,44)
P2	5	53	2	49	38	(49,38)

P3	0	48	3	86	63	(86,63)
P4	0	48	4	88	90	(88,90)
P5	0	48	2	49	150	(49,150)
P6	0	48	3	86	26	(86,26)
P7	0	48	5	102	150	(102,150)

Berikut data jumlah pembelian yaitu 2500000

Nilai k untuk P1 = 2

(P) = 53

$a = g^k \bmod p$

$$a = 7^2 \bmod 257$$

$$a = 49 \bmod 257 = 49$$

$b = (y^k \bmod P_i) \bmod p$

$$b = (49^2 \bmod P_1) \bmod 257$$

$$= 2401 * 53 \bmod 257$$

$$= 127253 \bmod 257$$

$$= 38$$

Nilai k untuk P2 = 3

(P) = 48

$a = g^k \bmod p$

$$a = 7^3 \bmod 257$$

$$a = 343 \bmod 257 = 86$$

$b = (y^k \bmod P_i) \bmod p$

$$b = (49^3 \bmod P_2) \bmod 257$$

$$= 117649 * 53 \bmod 257$$

$$= 6235397 \bmod 257$$

$$= 63$$

Nilai k untuk P3 = 4

(P) = 48

$a = g^k \bmod p$

$$a = 7^4 \bmod 257$$

$$a = 2401 \bmod 257 = 86$$

$b = (y^k \bmod P_i) \bmod p$

$$b = (49^4 \bmod P_3) \bmod 257$$

$$= 5764801 * 48 \bmod 257$$

$$= 276710448 \bmod 257$$

$$= 90$$

Nilai k untuk P4 = 5

(P) = 48

$a = g^k \bmod p$

$$a = 7^5 \bmod 257$$

$$a = 16807 \bmod 257 = 102$$

$b = (y^k \bmod P_i) \bmod p$

$$b = (49^5 \bmod P_4) \bmod 257$$

$$= 117649 * 50 \bmod 257$$

$$= 5882459 \bmod 257$$

$$= 150$$

Nilai k untuk P5 = 2

(P) = 48

$a = g^k \bmod p$

$$a = 7^2 \bmod 257$$

$$a = 49 \bmod 257 = 49$$

$b = (y^k \bmod P_i) \bmod p$

$$b = (49^2 \bmod P_5) \bmod 257$$

$$= 2401 * 48 \bmod 257$$

$$= 115248 \bmod 257$$

$$= 150$$

Nilai k untuk P6 = 3

$$(P) = 48$$

$$a = g^k \text{ mod } p \quad a = 7^3 \text{ mod } 257$$

$$a = 343 \text{ mod } 257 = 86$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^3 \text{ mod } P_6) \text{ mod } 257$$

$$= 117649 * 48 \text{ mod } 257$$

$$= 564912 \text{ mod } 257$$

$$= 26$$

Nilai k untuk P7 = 5

$$(P) = 48$$

$$a = g^k \text{ mod } p \quad a = 7^5 \text{ mod } 257$$

$$a = 16807 \text{ mod } 257 = 102$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^5 \text{ mod } P_7) \text{ mod } 257$$

$$= 117649 * 50 \text{ mod } 257$$

$$= 5882459 \text{ mod } 257$$

$$= 150$$

Tabel 7. Plaintext Hasil “500000”

Plainteks	Char	DEC	K	$a=(g^k)\text{mod } p$	$b=((y^k)*M) \text{ mod } p$	(a,b)
P1	5	53	2	49	38	(49,38)
P2	0	48	3	86	63	(86,63)
P3	0	48	4	88	90	(88,90)
P4	0	48	5	102	150	(102,150)
P5	0	48	2	49	150	(49,150)
P6	0	48	3	86	26	(86,26)
P7	0	48	5	102	150	(102,150)

Hasil enkripsi dari Plaintek “RAMA” adalah = (88,218), (86,150), (49, 94), (86,150). Dekripsi Metode Elgamal

Chiperteks:

(88,218), (86,150), (49, 94), (86,150)

Kunci : $x = 4$, $p = 257$

Mencari Plainteks P1:

$$s = a^x \text{ mod } p \quad P1 = b * S (p-x) \text{ mod } p$$

$$s = 88^2 \text{ mod } 257 \quad P1 = 218 * 34 (257-2) \text{ mod } 257$$

$$s = 7744 \text{ mod } 257 \quad P1 = 218 * 34 * 255 \text{ mod } 257$$

$$s = 34 \quad P1 = 82 = R$$

Mencari Plainteks P2:

$$s = a^x \text{ mod } p \quad P2 = b * S (p-x) \text{ mod } p$$

$$s = 86^2 \text{ mod } 257 \quad P2 = 150 * 200 (257-2) \text{ mod } 257$$

$$s = 7396 \text{ mod } 257 \quad P2 = (150 * 200 * 255) \text{ mod } 257$$

$$s = 200 \quad P2 = 65 = A$$

Mencari Plainteks P3:

$$s = a^x \text{ mod } p \quad P3 = b * S (p-x) \text{ mod } p$$

$$s = 49^2 \text{ mod } 257 \quad P3 = 94 * 88 (257-2) \text{ mod } 257$$

$$s = 2401 \text{ mod } 257 \quad P3 = (94 * 88 * 255) \text{ mod } 257$$

$$s = 88$$

$$P3 = 77 = M$$

Mencari Plainteks P4:

$$s = a^x \bmod p$$

$$s = 88^2 \bmod 257$$

$$s = 7744 \bmod 257$$

$$s = 34$$

$$P4 = b * S(p-x) \bmod p$$

$$P4 = 154 * 34 (255-2) \bmod 257$$

$$P4 = (154 * 34 * 255) \bmod 257$$

$$P4 = 65 = A$$

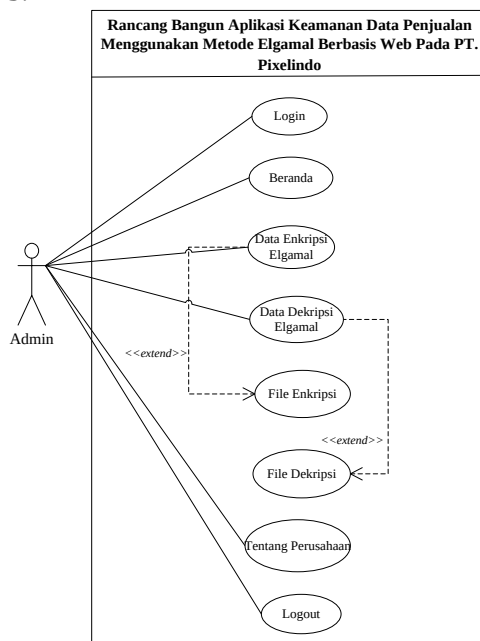
Maka hasil cipherteks yang didapat akan diproses kembali menjadi teks aslinya.yaitu: 88, 86, 49, 86 menjadi RAMA.

Tabel 8. Hasil Plaintext RAMA

Chipertext	Char	a	b	$s=a^x \bmod p$	$P=b*S(p-x) \bmod 257$
P1	88,218	88	218	34	82 = R
P2	86,150	86	150	200	65 = A
P3	49, 94	49	94	88	77 = M
P4	86,150	86	150	34	65 = A

B. Desain aplikasi

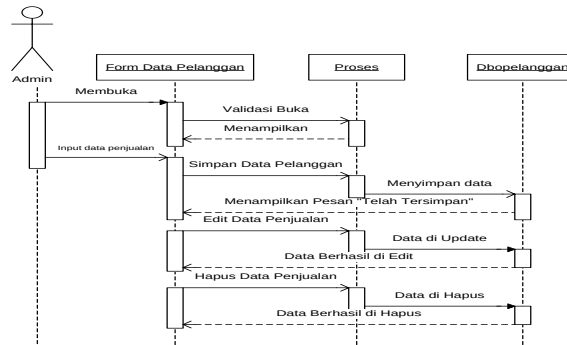
Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram UML *use case*, dapat dilihat pada gambar 3:



Gambar 3. Use Case Diagram

1. Sequence Diagram Data Dekripsi Elgamal

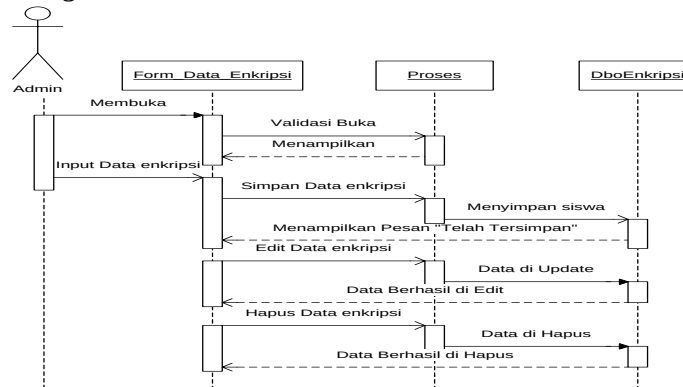
Pada *Sequence Diagram form enkripsi* menjelaskan admin melakukan enkripsi data dan dapat dilihat pada Gambar 4 sebagai berikut:



Gambar 4. Sequence Diagram Form Data Enkripsi Elgamal

2. Sequence Diagram File Enkripsi

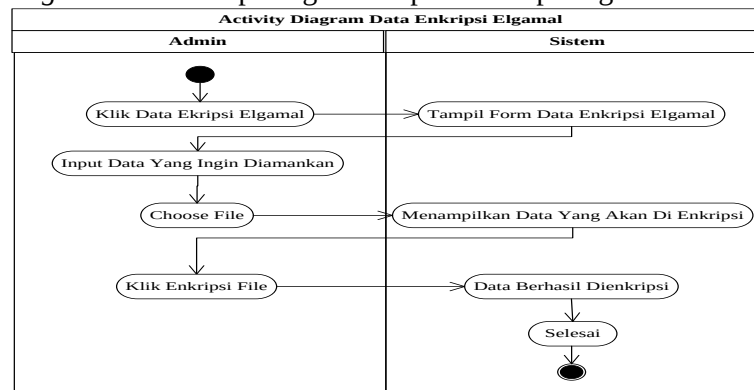
Pada *Sequence Diagram form enkripsi* menjelaskan admin melakukan enkripsi data dan dapat dilihat pada Gambar 5. sebagai berikut:



Gambar 5. Sequence Diagram Form File Enkripsi

3. Activity Diagram Data Enkripsi Elgamal

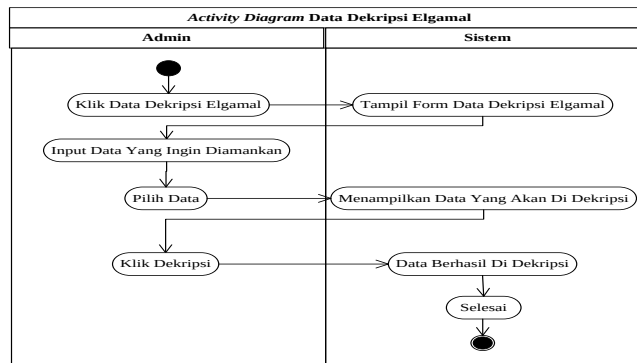
Activity Diagram Data Enkripsi Elgamal dapat dilihat pada gambar 6 berikut:



Gambar 6 Activity Diagram Data Enkripsi Elgamal

4. Activity Diagram Data Dekripsi Elgamal

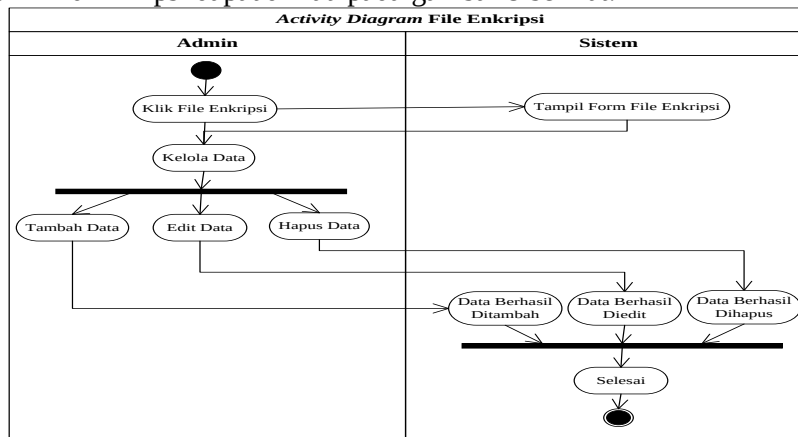
Activity Diagram Data Dekripsi Elgamal dapat dilihat pada gambar 7 berikut:



Gambar 7. Activity Diagram Data Dekripsi Elgamal

5. Activity Diagram File Enkripsi

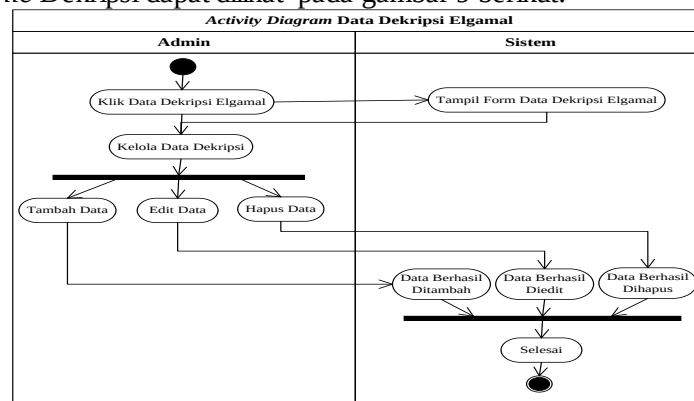
Activity Diagram File Enkripsi dapat dilihat pada gambar 8 berikut:



Gambar 8 Activity Diagram File Enkripsi

6. Activity Diagram File Dekripsi

Activity Diagram File Dekripsi dapat dilihat pada gambar 9 berikut:



Gambar 9 Activity Diagram Proses Dekripsi

C. Implementasi

1. Tampilan Data Enkripsi data

Tampilan ini merupakan halaman *enkripsi*. Halaman ini berisi *File enkripsi* yang akan dienkripsi oleh *admin*. Halaman ini dapat dilihat pada gambar 10 berikut ini:



Gambar 10. Tampilan Halaman *Data Enkripsi data*

2. Tampilan *Data Deskripsi*

Tampilan ini merupakan halaman *Deskripsi*. Halaman ini merupakan tampilan *deskripsi* yang ada diisi oleh admin. Halaman ini dapat dilihat pada gambar 11 berikut ini:



Gambar 11. Tampilan *Data Deskripsi*

3. Tampilan Halaman *Data File* enkripsi

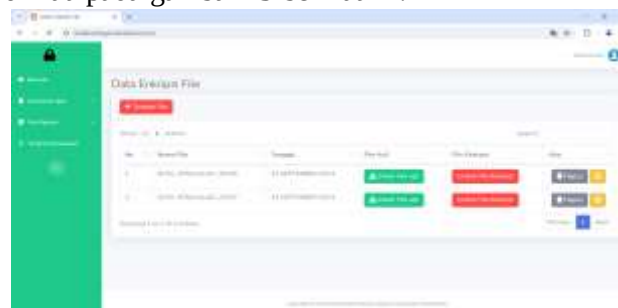
Tampilan ini merupakan halaman data *Data File* enkripsi. Halaman ini admin bisa mendownload data dan perhitungan enkripsi data elgamal. Halaman ini dapat dilihat pada gambar 12 berikut ini:



Gambar 12. Tampilan Halaman *Data File* enkripsi

4. Tampilan Halaman *Data File* deskripsi

Tampilan ini merupakan halaman data *Data File* deskripsi. Halaman ini berisi data deskripsi. Halaman ini dapat dilihat pada gambar 13 berikut ini:



Gambar 13. Tampilan Halaman *Data deskripsi*

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama Merancang Aplikasi Keamanan Data Penjualan Menggunakan Metode Elgamal Berbasis Web Pada PT. Pixelindo dapat ditarik kesimpulan sebagai berikut Dengan adanya aplikasi kriptografi dengan algoritma elgamal dapat meningkatkan keamanan data penjualan pada PT. Pixelindo. Dengan adanya aplikasi kriptografi dengan menerapkan algoritma elgamal pada PT. Pixelindo memudahkan proses pengamanan data penjualan lebih cepat. Dengan adanya aplikasi kriptografi dengan menerapkan algoritma elgamal pada PT. Pixelindo dapat menghindari kehilangan data penjualan dan tidak dapat dicuri oleh pihak lain yang tidak bertanggung jawab.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama, dosen pembimbing yaitu bapak Wirhan Fahrozi, M.Kom, kepada orang tua, kepada sahabat dari penulis dan kepada kelas IF stambuk 2020 yang telah banyak memberikan masukan dan saran dalam penyelesaian penelitian ini.

REFERENSI

- [1] Alfiah, Fifit, Rio Sudarji, and Dzakwan Taqiyyuddin Al Fatah. 2020. "Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nis san Jatake." *ADI Bisnis Digital Interdisiplin Jurnal* 1(1):22–34.
- [2] Anjani, Urai Icha, Cucu Suhery, and Uray Ristian. 2020. "Prediksi Permintaan Produk Kopi Bubuk Menggunakan Metode Double Exponential Smoothing Berbasis Website (Studi Kasus: PT. Fastrata Buana)." *Coding Jurnal Komputer Dan Aplikasi* 8(1).
- [3] Arthalia, Ika. 2021. "Penggunaan Website Sebagai Sarana Evaluasi Kegiatan Akademik Siswa Di SMA Negeri 1 Punggur Lampung Tengah." *JIKI (Jurnal Ilmu Komputer & Informatika)* 1(2).
- [4] Azis, Nur, Gali Pribadi, and Manda Savitrie Nurcahya. 2020. "Analisa Dan Perancangan Aplikasi Pembelajaran Bahasa Inggris Dasar Berbasis Android." *Ikraith-Informatika* 4(3):1–5.
- [5] Hasugian, Abdul Halim, Raissa Amanda Putri, and Annisa Shafira Zuhri. 2023. "Penerapan Metode Elgamal Untuk Mengamankan Teks Pada File Dokumen Word." *KLIK: Kajian Ilmiah Informatika Dan Komputer* 4(2):1143–53.
- [6] Husaini, Fahri, Akim M. H. Pardede, and Imeldawaty Gultom. 2022. "Penerapan Enkripsi Menggunakan Metode Elgamal Guna Meningkatkan Keamanan Data." *JUKI: Jurnal Komputer Dan Informatika* 4(1):67–73.
- [7] Rahman, Adithya. 2022. "Sistem Informasi Penjualan Dan Pembelian Alat Pemadam Api Ringan Berbasis Web Pada Koperasi Di Dinas Kebakaran Dan Penanggulangan Bencana Kota Bandung."
- [8] Rahmasari, Tiara. 2019. "Perancangan Sistem Informasi Akuntansi Persediaan Barang Dagang Pada Toserba Selamat Menggunakan Php Dan Mysql." *@ Is The Best: Accounting Information Systems and Information Technology Business Enterprise* 4(1):411–25.
- [9] Siambaton, Mhd Zulfansyuri. 2023. "Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal Dan XOR Dari Serangan Hacker." *Sudo Jurnal Teknik Informatika* 2(4):176–87.
- [10] Sumartini, Lilis Cucu, and Dini Fajriany Ardining Tias. 2019. "Analisis Kepuasan Konsumen Untuk Meningkatkan Volume Penjualan Kedai Kopi Kala Senja." *Jurnal E-Bis (Ekonomi-Bisnis)* 3(2):111–18.
- [11] Yani, Ahmad, Beni Saputra, and Redaksi Tim Jurnal. 2018. "RANCANG BANGUN SISTEM INFORMASI EVALUASI SISWA DAN KEHADIRAN GURU BERBASIS WEB: Studi Kasus Di SMK Nusa Putra Kota Tangerang."

-
- [12] Yudistira, Dharma. 2022. “Perancangan Aplikasi Penyandian Agenda Pribadi Menggunakan Algoritma Kunci Public Elgamal.” *Journal of Computing and Informatics Research* 2(1):17–21.
 - [13] Darmawan, R. (2023). Perancangan Aplikasi Kriptografi Menggunakan Algoritma RC4 (Rivest Code 4) Untuk Mengamankan Pesan Email di PT CREATIFACTORY. *OKTAL: Jurnal Ilmu Komputer dan Sains*, 2(03), 740-753.
 - [14] Oktawijaya, S., Zufria, I., & Hasugian, A. H. (2023). Sistem keamanan folder dengan menggunakan algoritma rivest code 4. *Jurnal Multimedia dan Teknologi Informasi (Jatilima)*, 5(02), 45-52.
 - [15] Oktasari, L. (2021). Perbandingan Algoritma RC4+ dan RC4a dalam Pengamanan File Teks. *Bulletin of Computer Science Research*, 1(3), 83-92.