Implementasi Algoritma *Blowfish* Untuk Pengamanan Data Transaksi Dalam Aplikasi Berbasis *Website E-commerce*

Implementation of the Blowfish Algorithm to Secure Transaction Data in an E-Commerce Website-based Application

Renki Gunawan[1], Elvi Rahmi[2]
[1,2]Jurusan Teknik Informatika, Politeknik Negeri Bengkalis
E-mail: [1]renki543@gmail.com, [2]elvirahmi@polbeng.ac.id
Received 5 March 2025; Revised 7 May 2025; Accepted 8 May 2025

Abstrak - Keamanan data transaksi merupakan aspek krusial dalam sistem *e-commerce*, khususnya bagi pelaku usaha kecil menengah (UMKM). Penelitian ini bertujuan untuk mengimplementasikan algoritma *Blowfish* dengan mode *Cipher Block Chaining (CBC)* dan panjang kunci *160-bit* guna meningkatkan keamanan data transaksi penjualan. Algoritma Blowfish dipilih karena efisien dan mendukung penggunaan *Initialization Vector (IV)* acak yang memperkuat proteksi terhadap serangan pattern dan dictionary. Data transaksi pelanggan dan pembayaran disimpan dalam bentuk *ciphertext* menggunakan *OpenSSL*. Pengujian dilakukan terhadap 20 data transaksi menggunakan serangan *dictionary* berbasis *OpenSSL*, dan hasil menunjukkan bahwa data tidak dapat didekripsi, membuktikan efektivitas pendekatan ini. Hasil penelitian ini menunjukkan bahwa penggunaan *Blowfish CBC 160-bit* dengan *IV* acak mampu memberikan perlindungan kuat dan efisien dalam konteks aplikasi *e-commerce* untuk UMKM.

Kata kunci: Keamanan Data Transaksi, *Blowfish CBC, Initialization Vector, E-Commerce, Dictionary Attack*

Abstract - *Transaction data security is a crucial aspect in e-commerce systems, especially for small and medium enterprises (UMKM). This study aims to implement the Blowfish algorithm with Cipher Block Chaining (CBC) mode and a 160-bit key length to improve the security of sales transaction data. The Blowfish algorithm was chosen because it is efficient and supports the use of random Initialization Vector (IV) which strengthens protection against pattern and dictionary attacks. Customer transaction and payment data are stored in ciphertext using OpenSSL. Testing was carried out on 20 transaction data using OpenSSL-based dictionary attacks, and the results showed that the data could not be decrypted, proving the effectiveness of this approach. The results of this study indicate that the use of 160-bit Blowfish CBC with random IV can provide strong and efficient protection in the context of e-commerce applications for UMKM.*

Keywords: *Transaction Data Security, Blowfish CBC, Initialization Vector, E-Commerce, Dictionary Attack*

1. PENDAHULUAN

Keamanan data transaksi merupakan aspek penting dalam operasional bisnis, terutama untuk melindungi informasi sensitif seperti data pembeli, metode pembayaran, dan rincian produk yang dibeli. Perlindungan ketat diperlukan agar data tidak disalahgunakan yang berpotensi merugikan bisnis maupun pelanggan[1].Kriptografi menjadi solusi efektif dalam menjaga kerahasiaan, integritas, serta mencegah akses tidak sah terhadap data. Kriptografi bekerja dengan mengubah data asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) yang sulit dipecahkan tanpa kunci yang sesuai[2].Salah satu algoritma kriptografi yang digunakan adalah

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

Blowfish, sebuah algoritma block cipher simetris yang membagi data menjadi *blok 64-bit*, dengan panjang kunci bervariasi antara *32-bit* hingga *448 bit*. *Blowfish* menggunakan struktur Feistel dan *Sbox* dinamis yang bergantung pada kunci enkripsi, menjadikannya fleksibel serta memiliki tingkat keamanan yang tinggi[1].

UMKM yang bergerak di bidang penjualan berbagai kebutuhan rumah tangga menghadapi sejumlah tantangan dalam mengelola transaksi penjualan secara aman dan efisien. Saat ini pencatatan data transaksi dan proses pembayaran masih dilakukan secara manual dan konvensional tanpa sistem keamanan yang memadai sehingga berpotensi memunculkan berbagai risiko seperti kebocoran data transaksi penjualan, manipulasi data keuangan, hingga hilangnya kepercayaan pelanggan terhadap sistem penjualan yang diterapkan. Keamanan data transaksi penjualan sangat penting terutama dalam transaksi online untuk memastikan bahwa data penting seperti nomor rekening pelanggan dan pemilik UMKM Bengkalis tidak bocor atau disalahgunakan oleh pihak yang tidak bertanggung jawab karena kebocoran data tersebut berisiko dimanfaatkan untuk tindakan kejahatan seperti penipuan atau transaksi ilegal yang dapat merugikan pelanggan maupun pihak UMKM sendiri. Selain itu, seiring berkembangnya kebutuhan akan sistem transaksi online yang cepat dan praktis, UMKM juga memerlukan metode atau teknik yang dapat mendukung proses transaksi agar lebih efisien tanpa mengabaikan faktor keamanan sehingga penerapan metode pengamanan data transaksi yang sesuai dengan karakteristik dan kebutuhan UMKM diperlukan agar keamanan data dapat terjamin sekaligus meningkatkan efisiensi dan kenyamanan pelanggan saat melakukan transaksi secara online maupun offline.

Berbagai penelitian sebelumnya telah membuktikan bahwa teknik kriptografi dapat digunakan secara efektif untuk meningkatkan keamanan data transaksi. menerapkan algoritma *AES* untuk mengamankan sistem e-marketplace. Hasilnya menunjukkan bahwa *AES* mampu menjaga kerahasiaan data transaksi, namun algoritma ini membutuhkan sumber daya komputasi yang relatif tinggi, sehingga kurang ideal untuk lingkungan UMKM[3]. menerapkan algoritma simetris *RC5* pada sistem web untuk mengenkripsi data transaksi. *RC5* memang tergolong ringan, namun penelitian tersebut tidak memanfaatkan mode operasi enkripsi seperti *CBC*, yang dapat meningkatkan keamanan dengan mencegah pola ciphertext yang berulang[4]. menggunakan metode *Base64* dalam sistem pencatat barang. Namun, Base64 bukanlah algoritma enkripsi yang sebenarnya, melainkan metode encoding, sehingga tingkat keamanannya sangat terbatas dan tidak cocok digunakan untuk melindungi data transaksi sensitif[5]. Keberhasilan penelitian ini yaitu terciptanya aplikasi pengamanan data transaksi menggunakan algoritma AES 128-bit untuk melindungi data transaksi di PT. Mitsubishi Electric Indonesia[6].

Berdasarkan latar belakang dan beberapa penelitian terkait sebelumnya sebagai acuan, penelitian ini mengembangkan aplikasi penjualan barang dengan mengimplementasikan algoritma kriptografi *Blowfish CBC 160-bit* untuk meningkatkan keamanan data transaksi penjualan barang di UMKM. Perbedaan utama dalam penelitian ini terletak pada penerapan *Blowfish CBC 160-bit* pada backend aplikasi dengan *IV* (*Initialization Vector*) yang dihasilkan secara acak di setiap proses enkripsi, sehingga setiap hasil enkripsi bersifat unik dan sulit diprediksi oleh pihak yang tidak berkepentingan. Selain itu, sistem transaksi juga didesain agar mendukung metode pembayaran transfer langsung melalui virtual account, di mana pengguna akan mendapatkan nomor virtual account yang unik untuk setiap transaksi yang dilakukan. Penerapan algoritma *Blowfish CBC 160-bit* dipilih karena algoritma ini dikenal memiliki tingkat keamanan yang tinggi dengan proses enkripsi yang efisien meskipun menggunakan kunci sepanjang *160-bit*, menjadikannya lebih aman terhadap upaya pencurian data maupun manipulasi oleh pihak yang tidak bertanggung jawab. Kombinasi antara keamanan data menggunakan *Blowfish CBC 160-bit* dan kemudahan pembayaran melalui virtual account diharapkan mampu menciptakan sistem penjualan barang yang aman, efisien, serta mempermudah pelanggan dalam melakukan transaksi. Selain itu, penerapan metode *IV* yang berubah-ubah di setiap proses enkripsi semakin meningkatkan keamanan, karena pola enkripsi tidak mudah ditebak sehingga melindungi data transaksi selama proses pengelolaan data

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

berlangsung.

2. METODE PENELITIAN

Penelitian ini berfokus pada penerapan algoritma kriptografi Blowfish untuk pengamanan data transaksi pada aplikasi e-commerce. Untuk mencapai tujuan tersebut, metode pengembangan sistem dijelaskan secara singkat tanpa membahas detail pendekatan seperti Waterfall, website, dan *e-commerce* yang tidak secara langsung berkaitan dengan inti kriptografi.

2.1 Implementasi Algoritma *Blowfish CBC 160-bit*

Blowfish merupakan algoritma enkripsi blok simetris yang mengolah data dalam blok *64-bit* dan mendukung panjang kunci variatif dari *32-bit* hingga *448-bit*. Dalam penelitian ini, digunakan panjang kunci sebesar *160-bit* dan mode operasi *Chiper Blocck Chaining (CBC)* yang mengharuskan adanya *Initialization Vector (IV)* sebagai input awal. Mode *CBC* dipilih karena mampu menyamarkan pola-pola dalam *plaintext* dengan menjadikan hasil enkripsi satu blok sebagai masukan untuk blok berikutnya. *IV* dihasilkan secara acak setiap kali proses enkripsi dilakukan, sehingga untuk data *plaintext* yang sama, hasil *ciphertext* akan selalu berbeda. Hal ini memberikan perlindungan lebih terhadap serangan *pattern analysis* dan *dictionary attack*.

Proses Enkripsi *Blowfish CBC 160-bit* dalam Penelitian Ini:

1. *Key Expansion*: Kunci *160-bit* digunakan untuk menghasilkan subkey melalui proses ekspansi.
2. Insialisasi *IV*: *IV* acak dibangkitkan untuk setiap sesi enkripsi dan disimpan bersamaan dengan *chipertext*.
3. Pembagian blok: *Plaintext* dibagi ke dalam blok *64-bit*.
4. Operasi *CBC*:
   Blok pertama dienkripsi setelah di-*XOR* dengan *IV*.
   Blok berikutnya di-*XOR* dengan hasil *chipertext* sebelumnya, lalu di enkripsi.
5. Hasil Akhir: *Chipertext* disimpan di dalam basis data pada kolom *payment_va_name* dan *paymen_va_number*.

Tabel 1 Hasil Pengujian Keamanan *Blowfish CBC 160-bit* terhadap Serangan *Dictionary*

No	Kolom yang diuji	Hasil *Descrypt* dengan *Dictionary*	Status
1	*paymen_va_name*	Gagal	Aman
2	*paymen_va_number*	Gagal	Aman

Dengan penggabungan antara *IV* acak, mode *CBC*, dan panjang kunci *160-bit*, algoritma *Blowfish* dalam penelitian ini mampu memberikan keamanan tinggi tanpa beban komputasi besar. Proses ini sangat cocok diterapkan pada UMKM yang memerlukan efisiensi dan kecepatan dalam pemrosesan data.

2.2 *Blowfish*

Blowfish merupakan algoritma kriptografi yang termasuk dalam cipher blok, yaitu metode enkripsi yang bekerja dengan membagi pesan menjadi beberapa blok data berukuran tetap, yaitu *64-bit* per blok. *Blowfish* mampu mengenkripsi data dalam unit *8 byte* per blok. Jika panjang pesan bukan kelipatan *8 byte*, maka sistem akan menambahkan padding agar panjangnya sesuai standar blok 64-bit.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

Keunggulan *Blowfish* terletak pada fleksibilitas panjang kunci, yang dapat dipilih mulai dari *32-bit* hingga *448-bit*. Secara umum, algoritma *Blowfish* terdiri dari dua tahap utama, yaitu:

1. *Key Expansion* berfungsi untuk mengubah kunci (minimal *32-bit* dan maksimal *448-bit*) menjadi rangkaian subkey yang di perlukan untuk enkripsi dan dekripsi. Total, dihasilkan 4168byt subkey melalui proses ini.
2. Data adalah proses enkripsi data menggunakan struktur *Feistel Network* yang terdiri dari 16 putaran. Setiap putaran melibatkan permutasi yang bergantung pada kunci dan subtitusi yang bergantung pada kombinasi kunci dan data. Operasi yang digunakan meliputi sejumlah, *XOR*, dan pencarian nilai dalam table menggunakan *S-box* yang telah diinisialisasi.

Tahapan Detail Proses *Blowfish*

1. Inisialisasi *P-array* dan *S-boxes* menggunakan konstanta yang diambil dari representasi nilai Pi dalam bentuk hexadecimal.
2. Setiap elemen *P-array* akan di-*XOR* dengan potongan kunci sepanjang *32-bit* yang diambil secara berurutan dari kunci utama pengguna. Proses ini diulang sampai seluruh *P-array* selesai di-*XOR*.
3. Setelahnya, dilakukan proses enkripsi terhadap string kosong (semua bit bernilai nol) menggunakan *P-array* dan *S-boxes* yang telah dimodifikasi.
4. Hasil enkripsi string kosong tersebut digunakan untuk memperbarui nilai P1 dan P2.
5. Proses enkripsi dilanjutkan menggunakan hasil baru ini sebagai input untuk memperbarui P3 dan P4, dan seterusnya.
6. Tahapan ini terus diulang sampai seluruh *P-array* dan *S-boxes* telah diperbarui sepenuhnya.
7. Setelah proses inisialiasasi selesai, barulah *plaintext* asli yang ingin dienkripsi diproses menggunakan algoritma *blowfish* melalui 16 putaran *Feistel Network*, hingga menghasilkan *chipertext*[1].

2.3 *E-Commerce*

Penjualan dalam platform *E-Commerce* adalah proses transaksi jual beli yang dilakukan secara online melalui platform digital seperti situs web atau aplikasi. Pelanggan dapat mencari, memilih, dan membeli produk atau layanan tanpa harus mengunjungi toko fisik. Proses ini mencakup pencarian produk, pemilihan item, pembayaran, dan konfirmasi transaksi, yang semuanya dirancang untuk memberikan pengalaman yang efisien dan nyaman bagi pengguna[7].

2.4 *Website*

Website adalah sekumpulan halaman web yang saling terhubung dan menyajikan informasi dalam berbagai format, termasuk teks, gambar, dan animsi. Website dapat diakses melalui koneksi internet dan dirancang untuk digunakan oleh individu, organisasi, atau perusahaan[8].

2.5 Kriptografi

Kriptografi merupakan cabang ilmu yang berfokus pada pengembangan serta penerapan metode-metode matematis yang bertujuan untuk melindungi informasi dari akses yang tidak sah. Dalam kriptografi, terdapat dua konsep utama yang sangat penting, yaitu proses enkripsi dan dekripsi[9]. Kriptografi berperan penting dalam keamanan informasi dengan memastikan kerahasiaan, integritas, dan keaslian data. Melalui enkripsi, data hanya dapat diakses oleh pihak yang berwenang, menjaga privasi dan mencegah akses tidak sah. Selain itu, kriptografi memastikan bahwa data tidak diubah selama transmisi, menjaga integritas informasi. Teknik ini juga digunakan untuk otentikasi, memastikan bahwa entitas yang mengakses data benar-benar siapa yang mereka klaim[10].

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

3. HASIL DAN PEMBAHASAN

3.1 Hasil Penerapan *Blowfish*

Pada proses ini, data transaksi penjualan dienkripsi menggunakan algoritma *Blowfish CBC 160-bit*, di mana metode *Cipher Block Chaining* mengandalkan *IV (Initialization Vector)* yang bersifat acak. Setiap data transaksi yang dienkripsi akan mendapatkan *IV* yang berbeda, sehingga meskipun transaksi yang sama dienkripsi ulang, hasil *ciphertext* yang dihasilkan akan selalu berubah. Teknik ini memastikan keamanan tambahan dengan mencegah pola-pola data yang berulang yang bisa dieksploitasi oleh pihak luar. Berikut ini adalah langkah-langkah untuk melakukan enkripsi *Blowfish 160-bit*:

1. Inisialisasi *P-Array*

Tabel 2 Inisialisasi *P-Array*

P-array	***Hexadecimal***	***Biner (32-bit)***
P0	243F6A88	00100100 00111111 01101010 10001000
P1	85A308D3	10000101 10100011 00001000 11010011
P2	13198A2E	00010011 00011001 10001010 00101110
P3	03707344	00000011 01110000 01110011 01000100
P4	A4093822	10100100 00001001 00111000 00100010
P5	299F31D0	00101001 10011111 00110001 11010000
P6	082EFA98	00001000 00101110 11111010 10011000
P7	EC4E6C89	11101100 01001110 01101100 10001001
P8	452821E6	01000101 00101000 00100001 11100110
P9	38D01377	00111000 11010000 00010011 01110111
P10	BE5466CF	10111110 01010100 01100110 11001111
P11	34E90C6C	00110100 11101001 00001100 01101100
P12	C0AC29B7	11000000 10101100 00101001 10110111

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

P-array	*Hexadecimal*	*Biner (32-bit)*
P13	C97C50DD	11001001 01111100 01010000 11011101
P14	3F84D5B5	00111111 10000100 11010101 10110101
P15	B5470917	10110101 01000111 00001001 00010111
P16	9216D5D9	10010010 00010110 11010101 11011001
P17	8979FB1B	10001001 01111001 11111011 00011011

2. Inisialisasi *S-Array*

Tabel 3 Inisialisasi *S-Array*

S-Array	*Hexadecimal*	*Biner (32-bit)*
S1,0	D1310BA6	11010001 00110001 00001011 10100110
S2,0	4B7A70E9	01001011 01111010 01110000 11101001
S3,0	E93D5A68	11101001 00111101 01011010 01101000
S4,0	3A39CE37	00111010 11000011 01110010 11100110

3. *Plaintext* = 50819194

Tabel 4 Mengubah *Plaintext* menjadi Biner

Karakter	***ASCII***	***Biner (8-bit)***
5	53	00110101
0	48	00110000
8	56	00111000
1	49	00110001
9	57	00111001
1	49	00110001
9	57	00111001
4	52	00110100

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

4. Pembagian *Plaintext* menjadi 2 bagian *XL* dan *XR* menjadi:
   XL: 00110101 00110000 00111000 00110001
   XR: 00111001 00110001 00111001 00110100

5. Pembangkitan Sub Kunci: Kunci “krip”

Tabel 5 Pembangkitan Sub Kunci

Karakter	***ASCII***	***Biner (8-bit)***
k	107	01101011
r	114	01110010
i	105	01101001
p	112	01110000

Biner Kunci:
01101011 01110010 01101001 01110000

6. Proses Iterasi dan Penerapan Sub-Kunci

Untuk iterasi pertama, P0 diubah dengan melakukan *XOR* antara P0 dan kunci. Proses ini diulang untuk setiap nilai P-array dan hasilnya digunakan dalam iterasi *Blowfish*.

Contoh untuk iterasi pertama:

P0 XOR Key (4-byte pertama dari kunci)

P0: 00100100 00111111 01101010 10001000

Key: 01101011 01110010 01101001 01110000

Hasil *XOR*:

01001111 01001101 00000011 11111000

XL XOR P0

XL: 00110101 00110000 00111000 00110001

P0: 01001111 01001101 00000011 11111000

Hasil:

01111010 01111101 00111011 11001001

Proses dilanjutkan dengan fungsi F dan penggantian *XL* ↔ *XR* hingga 16 iterasi.

7. Iterasi Proses Enkripsi

XL XOR P0 dilakukan, hasilnya akan diproses lebih lanjut dengan fungsi F.

Fungsi *F*(*XL*): Fungsi ini memecah *XL* menjadi empat bagian (a, b, c, d) dan memanipulasi bagian tersebut dengan menggunakan nilai dari *S-Array*.

Fungsi *F*(*XL*):

F(XL) = (((S0.a + S1.b mod 2^32) XOR S2.c) + S3.d mod 2^32)

Hasil fungsi F kemudian di-*XOR*-kan dengan *XR*, dan nilai *XL* dan *XR* ditukar untuk iterasi berikutnya.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

8. Setelah 16 Iterasi

Setelah dilakukan 16 iterasi, nilai *XL* dan *XR* yang baru akan di-*XOR*-kan dengan P16 dan P17, dan kedua nilai tersebut digabungkan untuk menghasilkan *ciphertext 64-bit*.

9. Hasil *chipertext*

Nilai biner yang dihasilkan setelah 16 iterasi digabungkan menjadi ciphertext dan dikonversi kembali ke dalam bentuk *ASCII* untuk menghasilkan hasil akhir.

Ciphertext akhir:

Ñ‚@¿-\xad^ (dalam bentuk *ASCII -compatible*)

Berikut ini adalah hasil penerapan *Blowfish CBC 160-bit* pada *database* sistem penjualan barang, khususnya dibagian tabel *Order* kolom *payment_va_name* dan *payment_va_number*.

payment_va_name	payment_va_number
DHH3QMjQtEw2jk3LhkVgPA==	I8ELoR+BddYmYFMRv61rYq1IktnXjZLy316krjWXT4I=
PVZ9gwlh8qM3qjimpaq0ow==	D8/NJGLhRKzH+v+ykPstNNQiMYoopnm5sUcihdTtkbs=
wtW5W6ctI1YfgtMlbY1rQQ==	EhBwgKDTGOpOA+BnZJoZdckxKrOYdNX211QpWVVph90=
Af5dxApccIiE9folhXXLmg==	L6w0Jz8+zFDzlk0rTWyvac7mSQJPkYn/6dndFiN8lK0=
66wKpyJdXIJcIQAkPlnVmA==	jPacilqRy0etwguu94uGztvWrI6hLnlgc+8NMNzZv/g=
hpOEBsd/zZofEdW448rIBA==	udY8a9IG09YyXPqYnLnNHarLv99diDB4AieS/Mkgy18=
XQ1KcspzkVvLebP0AY4cqg==	fwlWEDesnFbXm0M/JEhBXTVeWT+EbNQhx+NllcO31Bc=
Y3wU8zup34no5M1AhLse+w==	TwQ/ZhrLtNA+OIYE7jBOzwmHgQ0abyr+aOPKWbKK4z0=
DLArrL5dUFgJ5PEO8HmWxw==	qoVdBLX/7/cBVWBrdnq0vRmBUeBZXPPVH9MtF8W86Yg=
hRa1uohX5vyTYM4ktFnT4g==	urMLiMa8+2MYWu48eAFnMdsMX+MtbJDHjmJqUz4I6so=
+MxTUYDKG6iiJy3hKs6Lvw==	+Xt58fVKJTzY3sQeO5Rn7THzWxGY+z5vVXUVMnn3ypM=
qFU6y286E27a28pCuhqung==	715ahu14xRO43207Joo0MWDG7Y1G3tiQ4spJon9/D6s=
kHxT4eQeuXhPBMkw/oneNw==	3KHZ56R6axnNi4MLu2PYZCNRRGQMEGXmaqPO1YdfNLo=
otYz1Y8yULUGlhG16v4eUw==	rIxVEtht+z5GyRV8C0HCZv/n44qoTAX8iTbk4FjxM08=
+U8Yeaf34ArKQtNKWs+Oow==	4CMqQiEFKWQkjjsL2cZFqncmL437F87MDcnEEaUnuMQ=
1e0ginmo40/Oi4NUtillsQ==	5bYYnOWJ3ZpgdRuxDeoxFXYS1btPHV7W5OYuDZSKnEo=
O4aloMxvAj6VKAop/bjrBg==	2CNOngG8yrau80linLXKwUCOnBKJy18pW3qEzY2OxYw=
Ndw0jHHud3bRxqi6wVXqAA==	nbzBiHLUj89+8o9UfjJAj16qIjGcwpMHO3iabhbfvn0=
AAMI27vXTD9VKS2V4P3upw==	d9+gg57sLGwKcAQhAmRKoo21KkgO0t/F9SK9LqOUEwo=
Mkrzf68/ejZPt7XqlAYIng==	zq63keDAJ72Ch6M8xyhvS8FTT1CEUPB7a7RakrqAkIo=

Gambar 1 Hasil Enkripsi *Blowfish CBC 160-bit*

3.2 Hasil Pengujian Keamanan *Blowfish CBC 160-bit*

Pengujian dilakukan dengan menggunakan 20 data transaksi penjualan barang yang diambil dari kolom *payment_va_name* dan *payment_va_number* untuk menguji seberapa kuat enkripsi *Blowfish CBC 160-bit* saat menghadapi serangan *Dictionary* menggunakan *tool OpenSSL*. Berdasarkan hasil uji coba, tidak ada satu pun data transaksi penjualan barang yang berhasil dibuka kembali atau didekripsi.

Table 6 Hasil Pengujian Keamanan *Blowfish CBC 160-bit*

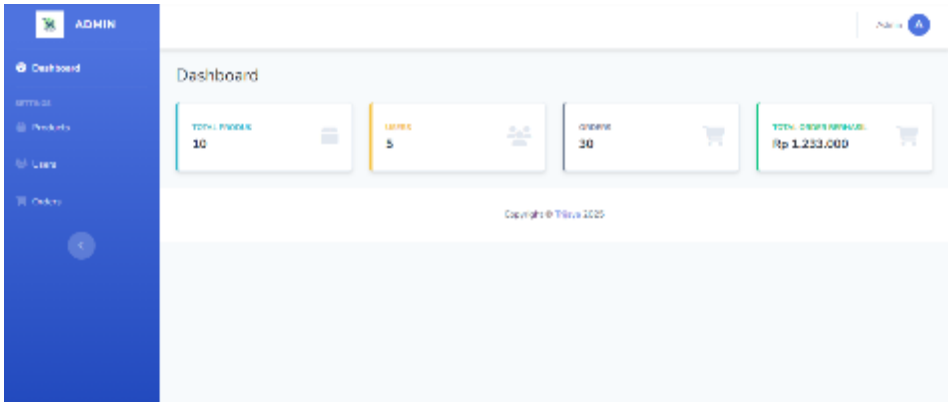
e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

No	Payment_va_name	Payment_va_number	Hasil Pengujian
1	DHH3QMjQtEw2jk3LhkVgPA==	I8ELoR+BddYmYFMRv61rYq1IktnXjZLy316krjWXT4l=	Tidak Berhasil
2	PVZ9gw1h8qM3qjimpaq0ow==	D8/NJGLhRKzH+v+ykPstNNQiMYoopnmSsUcihdTtkbs=	Tidak Berhasil
3	wtW5W6ctI1YfgtMlbY1rQQ==	EhBwgKDTGOpOA+BnZJoZdckxKrOYdNX2l1QpWVVph90=	Tidak Berhasil
4	Af5dxApccIiE9foIhXXLmg==	L6w0Jz8+zFDzIk0rTWyvac7mSQJPkYn/6dndFiN8lK0=	Tidak Berhasil
5	66wKpyJdXIJclQAkP1nVmA==	jPaci1qRy0etwguu94uGztvWrI6hLn1gc+BNMNzZv/g=	Tidak Berhasil
6	hpOEBsd/zZofEdW448rIBA==	udY8a9IG09YyXPqYnLnNHarLv99diDB4AieS/Mkgy18=	Tidak Berhasil
7	XQ1KcspzkVvLebP0AY4cqg==	fwlWEDesnFbXm0M/JEhBXTVeWT+EbNQhx+NIlcO31Bc=	Tidak Berhasil
8	Y3wU8zup34no5M1AhLse+w==	TwQ/ZhrLtNA+OIYE7jBOzwmHgQ0abyr+aOPKWbKK4z0=	Tidak Berhasil
9	DLArrL5dUFgJ5PEO8HmWxw==	qoVdBLX/7/cBVWBrdnq0vRmBUeBZXPPVH9MtF8W86Yg=	Tidak Berhasil
10	hRa1uohX5vyTYM4ktFmT4g==	urMLiMa8+2MYWu48eAFnMdsMX+MtbJDHjmJqUz4l6so=	Tidak Berhasil
11	+MxTUYDKGGiiJy3hKs6Lvw==	+Xt58fVKJTzY3sQeO5Rn7THzWxGY+z5vVXUVMnn3ypM=	Tidak Berhasil
12	qFUGy286E27a2BpCuhqung==	7l5ahu14xRO43207Joo0MWDG7Y1G3tiQ4spJon9/D6s=	Tidak Berhasil
13	kHxT4eQeuXhPBMkw/omeNw==	3KHZ56R6axnNi4MLu2PYZCNRRGQMEGXmaqPO1YdfNLo=	Tidak Berhasil
14	otYz1Y8yULUGlhG1Gv4eUw==	rlxVEtht+zSGyRV8C0HCZv/n44qoTAX8iTbk4FjxM08=	Tidak Berhasil
15	+U8Yeaf34ArKQtNKWs+Oow==	4CMqQiEFKWQkjjsL2cZFqncmL437F87MDcnEEaUnuMQ=	Tidak Berhasil
16	le0ginmo40/Oi4NUtillsQ==	5bYYnOWJ3ZpgdRuxDeoxFXYSlbtPHV7W5OYuDZSKnEo=	Tidak Berhasil
17	O4aloMxvAj6VKAop/bjrBg==	2CNOngG8yrau80linLXKwUCOnBKJy18pW3qEzY2OxYw=	Tidak Berhasil
18	Ndm0jHHud3bRxqi6wVXqAA==	nbzBiHLUj89+Bo9UfjJAj16qIjGcwpMHO3iabhbfvn0=	Tidak Berhasil
19	AAMI27vXTD9VKS2V4P3upw==	d9+gg57sLGwKcAQhAmRKoo21KkgO0t/F9SK9LqOUEwo=	Tidak Berhasil
20	Mkrzf68/ejZPt7XqlAYIng==	d9+gg57sLGwKcAQhAmRKoo21KkgO0t/F9SK9LqOUEwo=	Tidak Berhasil

3.3 Hasil Perancangan

1. Hasil Perancangan *Admin.*

Perancangan sistem *admin* ini bertujuan untuk mempermudah admin dalam menghitung jumlah pesanan. Berikut adalah hasil rancangan yang telah dibuat.



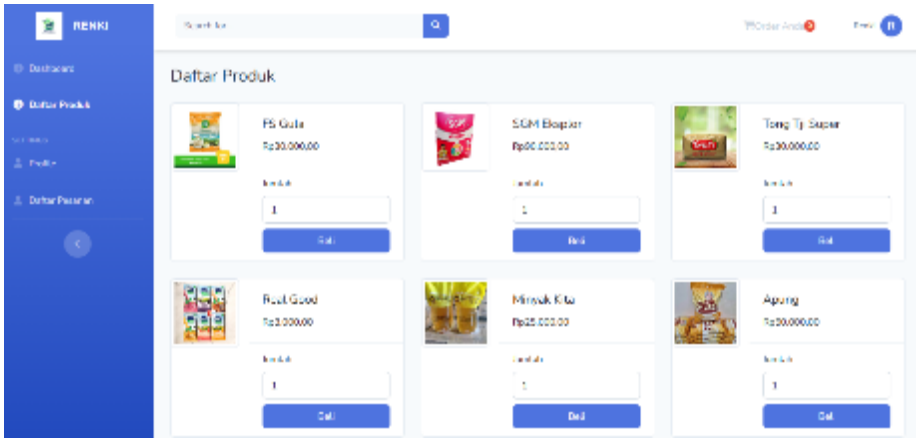
Gambar 2 Tampilan *Admin*

Gambar 4 Ini adalah hasil rancangan fitur yang ada, di mana admin dapat melihat pesanan yang masuk beserta jumlahnya.

2. Hasil Perancangan *User.*

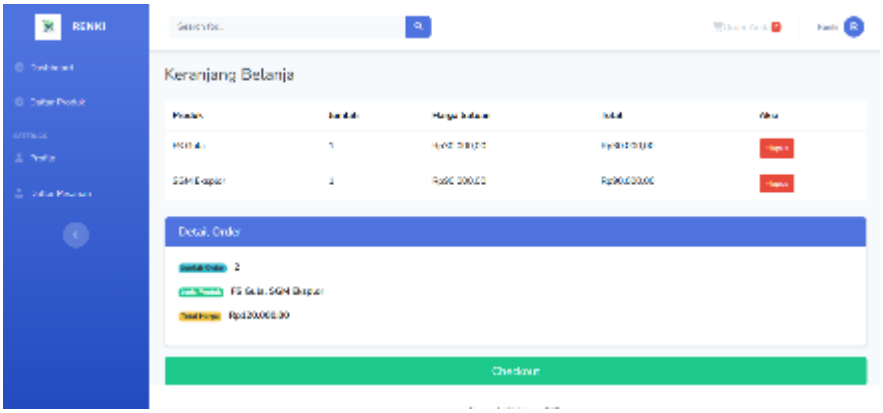
Pada aplikasi penjualan barang, *user* dapat melakukan pembelian produk, memilih metode pembayaran, melakukan pembayaran dan mendapatkan kuitansi. Berikut ini adalah hasil perancangan *User.*

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472



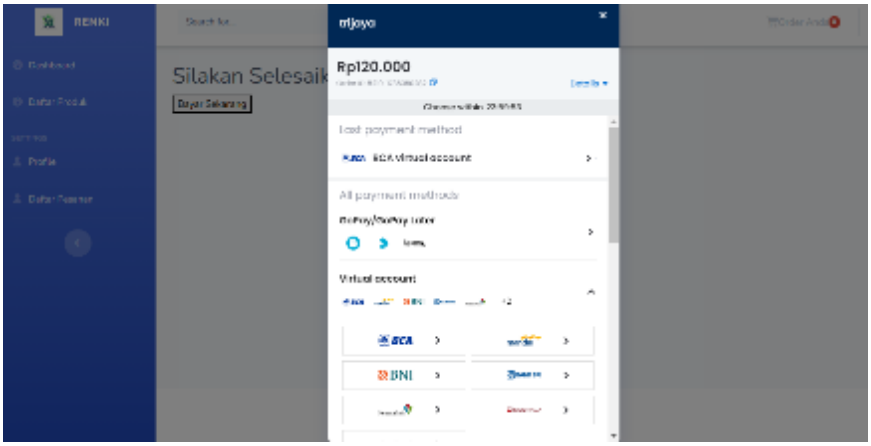
Gambar 3 Tampilan Menu Produk

Gambar 5 menunjukkan bahwa tampilan menu produk dan menu pembayaran, sehingga *user* bisa melakukan pemilihan produk dan melihat total harga dari produk yang dibeli serta melakukan pembayaran.



Gambar 4 Tampilan Menu Pembayaran

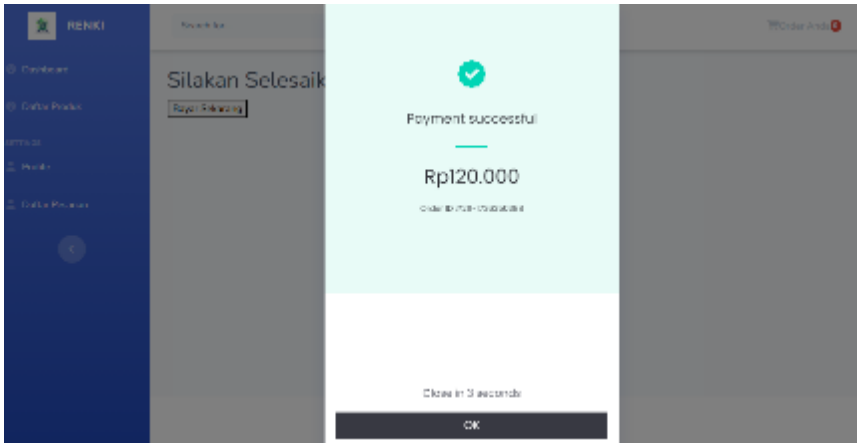
Gambar 6 menunjukkan bahwa tampilan menu pembayaran, sehingga *user* bisa melihat total harga dari produk yang dibeli serta melakukan pembayaran.



Gambar 5 Tampilan Menu Metode Pembayaran

Gambar 7 menunjukkan bahwa tampilan menu metode pembayaran dan kuitnsi, sehingga *user* bisa melakukan pemilihan metode pembayaran.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472



Gambar 6 Tampilan Bukti Pembayaran

Gambar 8 menunjukkan bahwa tampilan bukti pembayaran, sehingga *user* bisa mendapatkan bukti pembayaran setelah selesai melakukan pembayaran.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian, algoritma *Blowfish CBC 160-bit* berhasil diterapkan pada *Order.php* untuk mengenkripsi data transaksi, sehingga meningkatkan keamanan data pelanggan dan metode pembayaran. Data tersimpan dalam bentuk *ciphertext* yang sulit diakses pihak tidak berwenang. Pengujian serangan dictionary dengan *OpenSSL* menunjukkan algoritma ini memiliki keamanan tinggi. Untuk pengembangan ke depan, enkripsi disarankan diterapkan pada tabel lain, pengujian keamanan diperluas, serta dukungan panjang kunci lebih besar atau kombinasi algoritma tambahan dapat diterapkan untuk perlindungan optimal.

DAFTAR PUSTAKA

[1] M. Penyejuknate, S. Waluyo, I. Susanti, and D. Anggoro, "Implementasi Sistem Kriptografi Dengan Algoritma Blowfish Untuk Mengamanakan Database Pada Minimarket Happymart," pp. 1–8, 2021, [Online]. Available: https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/8632/3399

[2] S. Vivi Wahdini, D. Hartama, I. Okta Kirana, Poningsih, and Sumarno, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 3, pp. 101–107, 2021.

[3] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *J. Comput. Syst. Informatics*, vol. 4, no. 1, pp. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.

[4] C. Akhiar and Subandi, "Penerapan Algoritma Simetri Rc 5 Untukmengenkripsifile Transaksi Penjualan Berbasis Web," *Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 2, no. 2, pp. 158–166, 2023.

[5] T. Lovian and I. Fitri, "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang," *J. Media Inform. Budidarma*, vol. 6, no. 1, p. 692, 2022, doi: 10.30865/mib.v6i1.3513.

[6] F. A. Sitorus, N. B. Nugroho, and U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," *J. CyberTech*, no. x, pp. 1–15, 2020.

[7] Hairullah, C. R. A. Pramartha, and I. A. G. S. Putra, "Aplikasi Keamanan E-Commerce Berbasis Web Menggunakan Metode Algoritma Blowfish," *JNATIA J. Nas. Teknol. Inf.*

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472

dan Apl., vol. 1, no. 1, pp. 79–88, 2022.

[8] Rina Noviana, "Pembuatan Aplikasi Penjualan Berbasis Web Monja Store Menggunakan Php Dan Mysql," *J. Tek. dan Sci.*, vol. 1, no. 2, pp. 112–124, 2022, doi: 10.56127/jts.v1i2.128.

[9] K. Andriani and B. H. Hayadi, "Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (Rsa) Pad a Toko Baju Family," *J. Sci. Soc. Res.*, vol. 5, no. 3, p. 664, 2022, doi: 10.54314/jssr.v5i3.1018.

[10] A. Utama and R. F. Siahaan, "Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada Easy Tronik dengan Metode RC-5," *J. Ilmu Komput. dan Sist. Inf.*, vol. 3, no. 3, pp. 29–39, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/86

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i2.12472