JURNAL CYBER TECH STMIK TRIGUNA DHARMA
P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard)

Ariansyah Putra Ramadani Tarigan[1], Puji Sari Ramadhan[2], Kahiri Ibnutama[3]

[1]Program Studi Sistem Informasi, STMIK Triguna Dharma

Email: [1]ariantarigan7@gmail.com,[2]pujisariramadhan@gmail.com,[3]mr.ibnutama@gmail.com
Email Penulis Korespondensi: ariantarigan7@gmail.com

Abstrak− Perusahaan dagang adalah perusahaan yang membeli barang untuk dijual kembali tanpa harus mengubah bentuk fisik barang tersebut. Perusahaan dagang adalah suatu mata rantai dari sebuah saluran distribusi yang menghubungkan antara produsen dan konsumen, baik itu konsumen industri maupun konsumen akhir. UD. Enos Ginting adalah salah satu usaha dagang di kota medan yang menjual sepatu. Di dalam UD Enos Ginting kumpulan data dan informasi transaksi yang terjadi adalah suatu tanggung jawab bagi beberapa pihak yang bersangkutan. Karna itu, setiap laporan harus disusun dengan akurat. Dalam komunikasi data terdapat suatu teknik untuk merahasiakan data yang dikenal dengan kriptografi. Kriptografi adalah suatu teknik pengamanan data yang berguna untuk menjaga kerahasiaan dan keaslian data. Kriptografi bertujuan agar data dan informasi yang bersifat rahasia tidak bisa diketahui ataupun dimanfaatkan oleh pihak yang tidak berhak menerimanya. Data dan informasi penting seringkali dijadikan target oleh para penyerang.Advanced Encryption Standard (AES) adalah salah satu algoritma kriptografi yang bisa digunakan untuk mengamankan data. AES bekerja pada blok 128-bit atau 16 karakter, artinya AES bisa digunakan untuk enkripsi teks sepanjang 16 karakter Tidak hanya teks AES juga bisa digunakan untuk ekkripsi file dokumen yang panjangnya lebih dari 16 karakter dengan cara melakukan enkripsi perblok secara pararel untuk membuat proses enkripsi dan dekripsi menjadi lebih mudah. Hasil penelitian merupakan terciptanya sebuah aplikasi yang dapat mengenkripsi dan dekripsi file Excel yang nantinya diharapkan dapat membantu UD.Enos Ginting dalam meningkatkan keamanan data penjualan.

Kata Kunci : Kriptografi, Algoritma AES 128, Data Penjualan, Enkripsi, Dekripsi.

Abstract− A trading company is a company that buys goods for resale without having to change the physical form of the goods. A trading company is a link in a distribution channel that connects producers and consumers, both industrial consumers and final consumers. UD. Enos Ginting is a trading business in the city of Medan that sells shoes. Within UD Enos Ginting, the collection of data and transaction information that occurs is the responsibility of several parties concerned. Therefore, each report must be prepared accurately. In data communication, there is a technique for keeping data confidential, known as cryptography. Cryptography is a data security technique that is useful for maintaining the confidentiality and authenticity of data. Cryptography aims so that confidential data and information cannot be known or used by parties who are not entitled to receive it. Important data and information are often targeted by attackers. Advanced Encryption Standard (AES) is one of the cryptographic algorithms that can be used to secure data. AES works on blocks of 128-bits or 16 characters, meaning that AES can be used to encrypt text as long as 16 characters. description becomes easier. The result of this research is the creation of an application that can encrypt and decrypt Excel files which is expected to help UD.Enos Ginting in improving the security of sales data.

Keywords: Cryptography, AES 128 Algorithm, Sales Data, Encryption, Decryption.

1. PENDAHULUAN

Perusahaan dagang adalah perusahaan yang membeli barang untuk kemudian dijual kembali tanpa harus mengubah bentuk fisik barang tersebut. Perusahaan dagang adalah suatu mata rantai dari sebuah saluran distribusi yang menghubungkan antara pihak produsen dan pihak konsumen, baik itu konsumen industri maupun konsumen akhir.

Memperhatikan perusahaan dagang baik secara *online* ataupun *offline* dengan jumlah transaksi yang tinggi setiap hari, bulan, bahkan setiap tahunnya, maka seorang pengusaha wajib untuk mempelajari data transaksi secara berkala. Data atau laporan penjualan merupakan sekumpulan informasi transaksi yang disusun sebagai bahan analisa penjualan, dan data-data tersebut memiliki Banyak kegunaan bagi seorang pengusaha. Data dan Informasi penjualan akan sangat membantu para pengusaha dalam menyusun strategi untuk mengembangkan usahanya, seperti mengevaluasi bagaimana tren pasar dan kebiasaan pelanggan yang kerap kali berubah.

UD. Enos Ginting adalah salah satu usaha dagang di kota medan yang menjual sandal dan sepatu. Di dalam UD Enos Ginting kumpulan data dan informasi transaksi yang terjadi adalah suatu tanggung jawab bagi beberapa pihak yang bersangkutan. Karna itu, setiap laporan harus disusun dengan akurat. Dalam suatu bisnis,

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

kumpulan data dan informasi penjualan jelas tidak boleh diremehkan. Mengingat kumpulan data dan informasi tersebut memiliki pengaruh yang besar terhadap banyak aspek dalam perusahaan dagang.

Dalam komunikasi data terdapat suatu teknik untuk merahasiakan data yang dikenal juga dengan kriptografi. Kriptografi adalah suatu teknik pengamanan data yang berguna untuk menjaga kerahasiaan data (*secresy*) dan keaslian data (*authenticity*)[1]. Kriptografi bertujuan agar data dan informasi yang bersifat rahasia tidak bisa diketahui ataupun dimanfaatkan oleh pihak yang tidak berhak menerimanya. Data dan informasi penting seringkali dijadikan target oleh para penyerang. Dan biasanya serangan tersebut dilakukan oleh *hacker* ataupun dari orang dalam seperti pegawai yang tidak merasa puas[2]

Kata kriptografi (*Cryptography*) berasal dari dua suku kata dalam bahasa Yunani yaitu *cryptos* dan *graphein*. Kata *cryptos* mempunyai arti menyembunyikan, sedangkan *graphein* mempunyai arti tulisan, maka arti dari Kriptografi adalah ilmu untuk menjaga keamanan pesan (Schneier, 1996)[5]. Ketika suatu pesan (*message*) dikirim maka isi pesan tersebut kemungkinan dapat disadap oleh pihak yang tidak berhak untuk tahu isi dari pesan tersebut. Maka untuk menjaga keamanan pesan tersebut dapat mengubah isi pesan menjadi suatu kode yang tidak dapat dibaca maupun dimengerti pihak lain. Kriptografi sudah sangat lama sekali digunakan oleh para tentara Sparta yang ada di Yunani sekitar awal tahun 400 SM, dan alat yang digunakan pada saat itu adalah scytale yaitu pita panjang dari kertas papirus dan juga sebatang silinder. Kemudian pesan ditulis baris perbaris, jika pita dilepas maka huruf-huruf yang ada didalamnya telah berbaris dan membentuk pesan rahasia. Pesan hanya bisa dibaca jika penerima melilitkan pesan ke silider yang memiliki diameter yang sama dengan diameter silinder yang digunakan oleh pengirim.

Dalam kriptografi ada dua konsep utama yaitu enkripsi dan dekripsi. Proses enkripsi merupakan proses ketika informasi diubah sehingga tidak dapat dikenali lagi sebagai informasi awalnya dengan menggunakan metode dan algoritma tertentu sedangkan proses dekripsi merupakan kebalikan dari proses enkripsi yaitu mengembalikan bentuk informsi yang sudah disamarkan tersebut kembali ke bentuk informasi awal[3].

Advanced Encryption Standard (AES) adalah salah satu algoritma kriptografi yang bisa digunakan untuk mengamankan data. AES bekerja pada blok 128-*bit* atau 16 karakter, artinya AES bisa digunakan untuk enkripsi teks sepanjang 16 karakter[4]. Tidak hanya teks AES juga bisa digunakan untuk ekkripsi *file* dokumen yang panjangnya lebih dari 16 karakter dengan cara melakukan enkripsi perblok secara pararel untuk membuat proses enkripsi dan dekripsi menjadi lebih mudah.

Latar belakang kelahiran AES adalah karena *standard* enkripsi yang lama yaitu DES dianggap sudah tidak aman lagi digunakan karena kunci DES dapat ditemukan secara *Brute-force*. Oleh karena itu perlu diusulkan algoritma standard enkripsi yang baru sebagai pengganti DES[8][9].

Lembaga nasional dan teknologi Amerika yaitu *National Institute of Standards and Technology* (NIST) mengusulkan kepada pemerintah federal AS untuk membuat sebuah standar kriptografi baru, maka pada bulan november tahun 2001 diputuskan algoritma *Rijndael* yang dibuat oleh Vincent Rijmen dan Joan Daemen dari Belgia sebagai algoritma yang baru untuk menggantikan DES dan diberi nama AES[10].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian dilakukan untuk mendapatkan informasi dan data yang *valid* yang akan di enkripsi sesuai dengan judul Penerapan Kriptografi Untuk pengaman Data Sepatu Dengan Metode AES

Adapun teknik-teknik dalam mengambil pengumpulan data adalah sebagai berikut:

1. Observasi
   Observasi dilakukan dengan cara mengikuti kegiatan secara langsung pada UD. Enos Ginting mengamati, mempelajari data penjualan, serta mencari masalah yang dihadapi pihak UD. Enos Ginting. Dari masalah-masalah yang didapat akan dibuat rumusan masalah serta cara penyelesaiannya
2. Wawancara
   Untuk mendapatkan informasi yang mendalam dan data sesuai dengan yang dibutuhkan dalam penelitian, kegiatan wawancara dilakukan secara langsung dengan pihak UD. Enos Ginting.
3. Studi Literatur
   Studi Literatur merupakan sumber yang mendukung sebagai landasan teoritis untuk mengkaji masalah yang dibahas. Sumber yang digunakan dalam penelitian ini diantaranya Jurnal Nasional, buku dan Sumber-sumber lainnya. Diharapkan dengan literatur tersebut dapat mempermudah menyelesaikan masalah pada proses pengenkripsian .

2.2 Studi kasus dan penyelesaian

Dalam metode penelitian pada penerapan Kriptografi untuk keamanan data UD. Enos Ginting dengan menggunakan metode Advanched Encryption Standard terdapat dua bagian yang harus dilakukan, yaitu studi pustaka dan pengumpulan data. Pengumpulan data dalam penelitian ini menggunakan teknik wawancara.

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

Kegiatan tersebut dilakukan dengan mewawancarai narasumber pemilik UD. Enos Ginting yaitu: Bapak Enos Ginting. Dari pengumpulan data yang dilakukan diperoleh data yang akan dilakukan penelitian sebagai berikut:

Tabel 1. Data Penjualan Sepatu

NO	Kode Barang	Nama Sepatu	Tanggal	Jumlah penjualan	Harga	Pendapatan	Nama kostumer	User	Kode user
1	40015	Adidas neos city	16 -12 - 2021	3	Rp.150.000	Rp.450.000	Siti susanti	Enos	101
2	60020	Kodachi hitam	16 -12 - 2021	2	Rp.95.000	Rp.190.000	Siti susanti	Enos	101
3	20032	Boots yumeida	18 -12 - 2021	5	Rp.95.000	Rp.475.000	Supriadi sembiring	Ari	102
4	12021	Sandal swallow original	18 -12 - 2021	7	Rp.15.000	Rp.105.000	Jhony Marpaung	Enos	101
5	20033	Sepatu sekolah PROATT	19 -12 - 2021	2	Rp.100.000	Rp.200.000	Ayu Agustina	Enos	101
6	12021	Sandal swallow original	19 -12 - 2021	10	Rp.15.000	Rp.150.000	Ebenezer Keliat	Ari	102
7	12021	Sandal swallow original	20 -12 - 2021	12	Rp.15.000	Rp.180.000	Kerno Siregar	Ari	102
8	12032	Sendal slide casual pria	20 -12 - 2021	3	Rp. 100.000	Rp.300.000	Kerno Siregar	Ari	102
9	40016	Adidas Gazelle	20 -12 - 2021	1	Rp.300.000	Rp.300.000	Aldi Tumanggor	Enos	101

Kriptografi yang digunakan untuk mengamankan data dan dokumen adalah dengan menggunakan metode AES-128. Perhitungan metode AES yang digunakan untuk enkripsi dan dekripsi *file* dan dokumen untuk pengamanan data UD. Enos GInting. Berikut merupakan proses perhitungan dengan metode AES.

1. Menentukan *Plaintext* Dan *Chiper key*

   Adapun penyelesaian metode AES dalam peneitian ini adalah dengan melakukan enkripsi dan dekripsi Data Penjualan di UD. Enos Ginting. adapun contoh yang akan dienkripsi yaitu dengan *plaintext* : "Adidas neos city" *key* : "KriptografiAES01".

   Plaintext dalam bilangan *hexadecimal :*

A	d	i	d	A	S		n	E	o	S		c	i	t	y
41	64	69	64	61	73	20	6E	65	6F	73	20	63	69	74	79

   Setelah menentukan *plaintext* dan *chiperkey*, maka langkah selanjutnya akan dilakukan xor antara *plaintext* dan *chiperkey* untuk menghasilkan blok baru.

2. Ekspansi kunci

   Pembangkitan kunci untuk AES-128 *bit* menggunakan 4 *words* (16 *byte*) sebagai masukan dan kemudian menghasilkan perluasan kunci (*key*) menjadi 44 *words* (176 *bytes*). *Round key* dibutuhkan dalam proses enkripsi dan juga dekripsi pada metode AES[4]. Pada kasus ini *key* yang akan digunakan yaitu: "KriptografiAES01".

   a. Urutkan kunci kedalam blok yang berukuran 128 *bit*. Kemudian konversi kunci kedalam bentuk *hexadecimal*.

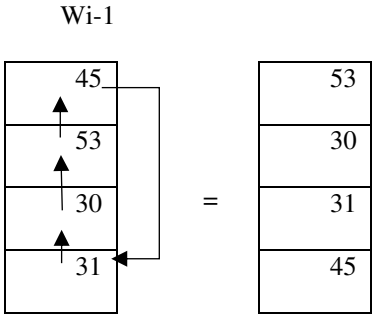
K	r	i	p	t	o	g	r	a	f	i	A	E	S	0	1
4B	72	69	70	74	6F	67	72	61	66	69	41	45	53	30	31

   b. Langkah selanjutnya adalah menyusun kunci yang sudah diubah menjadi bentuk *hexadecimal* kedalam *state* yang berukuran 4 x 4.

4B	74	61	45
72	6F	66	53
69	67	69	30
70	72	41	31

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

c. Kemudian untuk mendapatkan kolom pertama pada *subkey*, langkah pertama adalah melakukan *RotWord*, yaitu dengan cara menggeser tiap *bit* pada kolom yang ke-4 keatas satu kali dari kunci ronde yang ke-0.



d. Setelah itu hasil dari *RotWord* tersebut ditukar dengan nilai yang ada pada tabel S-Box (*SubBytes*)[14].

Tabel 1 S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	**63**	**7C**	**77**	**7B**	**F2**	**6B**	**6F**	**C5**	**30**	**01**	**67**	**2B**	**FE**	**D7**	**AB**	**76**
1	**CA**	**82**	**C9**	**7D**	**FA**	**69**	**47**	**F0**	**AD**	**D4**	**A2**	**AF**	**9C**	**A4**	**72**	**C0**
2	**B7**	**FD**	**93**	**26**	**35**	**3F**	**F7**	**CC**	**34**	**A5**	**E5**	**F1**	**71**	**D8**	**31**	**15**
3	**04**	**C7**	**23**	**C3**	**18**	**96**	**05**	**9A**	**07**	**12**	**80**	**E2**	**EB**	**27**	**B2**	**75**
4	**09**	**83**	**2C**	**1A**	**1B**	**6E**	**5A**	**A0**	**52**	**3B**	**D6**	**B3**	**29**	**E3**	**2F**	**84**
5	**53**	**D1**	**00**	**ED**	**20**	**FC**	**B1**	**5B**	**6A**	**CB**	**BE**	**39**	**4A**	**4C**	**58**	**CF**
6	**D0**	**EF**	**AA**	**FB**	**43**	**AD**	**33**	**85**	**46**	**F9**	**02**	**7F**	**50**	**3C**	**9F**	**A8**
7	**51**	**A3**	**40**	**8F**	**92**	**9D**	**38**	**F5**	**BC**	**B6**	**DA**	**21**	**10**	**FF**	**F3**	**D2**
8	**CD**	**0C**	**13**	**EC**	**5F**	**97**	**44**	**17**	**C4**	**A7**	**7E**	**3D**	**64**	**5D**	**19**	**73**
9	**60**	**81**	**4F**	**DC**	**22**	**2A**	**90**	**88**	**46**	**EE**	**B8**	**14**	**DE**	**5E**	**0B**	**DB**
A	**E0**	**32**	**3A**	**0A**	**49**	**06**	**24**	**5C**	**C2**	**D3**	**AC**	**62**	**91**	**95**	**E4**	**79**
B	**E7**	**C8**	**37**	**6D**	**8D**	**D5**	**4E**	**A9**	**6C**	**56**	**F4**	**EA**	**66**	**7A**	**AE**	**08**
C	**BA**	**78**	**25**	**2E**	**1C**	**A6**	**B4**	**C6**	**EB**	**DD**	**74**	**1F**	**4B**	**BD**	**8B**	**8A**
D	**70**	**3E**	**B5**	**66**	**48**	**03**	**F6**	**0E**	**61**	**35**	**57**	**B9**	**86**	**C1**	**1D**	**9E**
E	**E1**	**F8**	**98**	**11**	**69**	**D9**	**8E**	**94**	**9B**	**1E**	**87**	**E9**	**CE**	**55**	**28**	**DF**
F	**8C**	**A1**	**89**	**0D**	**BF**	**E6**	**42**	**68**	**41**	**99**	**2D**	**0F**	**B0**	**54**	**BB**	**16**

53		ED
30		04
31	=	C7
45		6E

e. Tahap yang terakhir adalah melakukan *xor* antara hasil *SubBytes* dengan kolom pertama (wi -4) dari *RoundKey* ke-0 dan kolom ke-1 dari tabel Rcon.

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

Tabel 2 Rcon

Rcon	1	2	3	4	5	6	7	8	9	10
	01	02	04	08	10	20	40	80	1B	36
	00	00	00	00	00	00	00	00	0	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00

		Wi -4		Rcon		
ED	⊕	4B	⊕	01	=	A7
04		72		00		76
C7		69		00		AE
6E		70		00		1E

f. Selanjutnya Untuk mendapatkan kolom yang ke-2, ke-3 dan ke-4 untuk *RoundKey* ke-1 lakukan *xor* antara wi dengan kolom ke-2 dari *RoundKey* ke-0 (wi -4). Ulangi langkah c sampai f hingga mendapat *RoundKey* ke-10.

Wi -1		Wi -4		
A7	⊕	74	=	D3
76		6F		19
AE		67		C9
1E		72		6C

Berikut ini merupakan hasil dari proses ekspansi kunci dari ronde ke-0 sampai ronde ke-10 yang telah diperoleh.

Tabel 3. Hasil Proses Ekspansi Kunci

Round Key 0				*Round Key 1*				*Round Key 2*				*Round Key 3*			
4B	74	61	45	A7	D3	B2	F7	D4	07	B5	42	9A	9D	28	6A
72	6F	66	53	76	19	7F	2C	16	0F	70	5C	09	06	76	2A
69	67	69	30	AE	C9	A0	90	32	FB	5B	CB	C3	38	63	A8
70	72	41	31	1E	6C	2D	1C	76	1A	37	2B	5A	40	77	5C
Round Key 4				*Round Key 5*				*Round Key 6*				*Round Key 7*			
77	EA	C2	A8	E6	0C	CE	66	84	88	46	20	0C	84	C2	E2
CB	CD	BB	91	11	DC	67	F6	FC	20	47	B1	0A	2A	6D	DC
89	B1	D2	7A	4A	FB	29	53	57	AC	85	D6	FA	56	D3	05
58	18	6F	33	9A	82	ED	DE	A9	2B	C6	18	1E	35	F3	EB
Round Key 8				*Round Key 9*				*Round Key 10*							
0A	8E	4C	AE	3C	B2	FE	50	EF	5D	A3	F3				
61	4B	26	FA	BD	F6	D0	2A	7A	8C	5C	76				
13	45	96	93	71	34	A2	31	F1	C5	67	56				
86	B3	40	AB	62	D1	91	3A	31	E0	71	4B				

2.3 Enkripsi

1. *Plaintext* yang akan digunakan dalam proses enkripsi adalah “Adidas neos city”.

A	d	i	d	a	s		n	e	o	s		c	i	t	y
41	64	69	64	61	73	20	6E	65	6F	73	20	63	69	74	79

2. Untuk melakukan proses enkripsi yang harus dilakukan adalah menyusun 16 byte pertama dari *plaintext* kedalam *state* 4 x 4

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

41	61	65	63
64	73	6F	69
69	20	73	74
64	6E	20	79

3. Kemudian lakukan proses *AddRoundKey*, yaitu dengan melakukan *xor* antara *plaintext* dengan *Roundkey* ke-0[6].

41	61	65	63	⊕	4B	74	61	45	=	0A	15	04	26
64	73	6F	69		72	6F	66	53		16	1C	09	3A
69	20	73	74		69	67	69	30		00	47	1A	44
64	6E	20	79		70	72	41	31		14	1C	61	48

4. Proses di atas akan menjadi masukan (pra-ronde) untuk *round* ke-1 dan akan diproses dengan empat transformasi yaitu: transformasi *SubBytes*, transformasi *ShiftRow*, transformasi *MixColumns* dan transformasi *AddRoundKey*[7].
   a. SubBytes
   Hasil dari pra-ronde kemudian diubah dengan nilai yang ada pada table S-Box.

0A	15	04	26
16	1C	09	3A
00	47	1A	44
14	1C	61	48

→

67	59	F2	F7
47	9C	01	80
63	A0	A2	1B
FA	9C	EF	52

   b. *ShiftRows*
   Untuk proses *ShiftRows*, geser tiga baris terakhir dari *array state* secara siklik. Jumlah pergeseran ditentukan dengan nilai baris (r). Baris r = 0 tidak digeser, Baris r = 1 digeser 1 *byte* ke kiri, baris r = 2 digeser 2 *byte* ke kiri, dan baris r = 3 digeser 3 *byte* ke kiri[11].

r = 0 →
r – 1 →
r = 2 →
r = 3 →

67	59	F2	F7
47	9C	01	80
63	A0	A2	1B
FA	9C	EF	52

–

67	59	F2	F7
9C	01	80	47
A2	1B	63	A0
52	FA	9C	EF

   c. *MixColumns*
   Pada transformasi *MixColumn* akan dilakukan perkalian antara *state* hasil *ShiftRows* dengan *matriks MixColumns* dengan mengkonversikan setiap kolom dengan *polynomial*[12].

02	*03*	*01*	*01*
01	*02*	*03*	*01*
01	*01*	*02*	*03*
03	*01*	*01*	*02*

.

67	59	F2	F7
9C	01	80	47
A2	1B	63	A0
52	FA	9C	EF

=

[02 03 01 01] → 67, 9C, A2, 52

({02 . 67} ⊕ {03 . 9C} ⊕ {01. A2} ⊕ {01 . 52})
(02 . 67) = (0010) . (0110 0111)

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

$= (X) . (X^6 + X^5 + X^2 + X + 1)$
$= X^7 + X^6 + X^3 + X^2 + X$
= 1100 1110 = "CE"

Lakukan xor untuk setiap hasil yang didapat dari proses perkalian di atas.
= 1100 1110 ⊕ 1011 1111 ⊕ 1010 0010 ⊕ 0101 0010
= 1000 0001 = "81"

Berikut ini adalah hasil dari perhitungan *mixcolumns*:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

.

67	59	F2	F7
9C	01	80	47
A2	1B	63	A0
52	FA	9C	EF

=

81	50	9B	73
EB	8C	D0	6D
52	7B	0B	C1
33	1E	CD	20

d. *AddRoundKey*
Langkah terakhir pada enkripsi untuk putaran pertama adalah proses *AddRoundKey* yaitu dengan melakukan *xor* antara hasil *MixColumn* dengan *RoundKey* ke-1[13].

81	50	9B	73
EB	8C	D0	6D
52	7B	0B	C1
33	1E	CD	20

⊕

RoundKey 1

A7	D3	B2	F7
76	19	7F	2C
AE	C9	A0	90
1E	6C	2D	1C

=

26	83	29	84
9D	95	AF	41
FC	B2	AB	51
2D	72	E0	3C

Ulangi proses *SubBytes*, *ShiftRows*, *MixColumn* dan *AddRoundKey* hingga sembilan kali putaran, dan pada putaran yang ke-10 (*final round*) hanya akan dilakukan proses *SubBytes*, *Shiftrows* dan *AddRoundkey* untuk mendapatkan *chipertext*.
Berikut adalah hasil dari *round* ke-1 sampai *round* ke-10 pada proses enkripsi.

Tabel 4 Hasil Proses Enkripsi

Round 1				*Round 2*				*Round Key 3*			
26	83	29	84	D6	46	8A	C8	55	78	52	7A
9D	95	AF	41	F8	A1	43	07	86	B0	FE	CA
FC	B2	AB	51	0D	A4	C6	9C	01	27	62	60
2D	72	E0	3C	F1	36	70	7A	72	33	ED	D5
Round 4				*Round 5*				*Round 6*			
0F	CF	E1	52	9F	AE	6A	FB	04	6F	CD	29
04	37	14	D9	AE	8D	27	F8	E6	75	87	A9
D8	CD	00	98	A5	1E	B5	B7	41	A0	14	2F
0C	2C	FA	64	7F	5C	48	CB	69	C6	13	3B
Round 7				*Round 8*				*Round 9*			
57	1A	FA	A7	02	08	98	DD	98	EC	4C	B8
2E	6A	47	38	97	10	D9	90	78	34	EB	D7
47	D3	67	72	1C	61	8E	2B	C4	63	A1	9A
AB	3D	0C	8B	96	6A	DE	FF	04	7E	A3	3F
Round 10											
A9	93	8A	9F								
62	65	52	CA								

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

C3	7D	7B	AD
44	12	82	41

Dan hasil enkripsi dengan metode AES 128 *bit* menghasilkan *Chipertext* sebagai berikut "A9, 62, C3, 44, 93, 65, 7D, 12, 8A, 52, 7B, 82, 9F, CA, AD, 41 ".

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan ditunjukkan hasil dari perancangan sistem yang telah dibangun yaitu aplikasi pengamanan data penjualan UD. Enos Ginting dengan metode AES. Hasil yang akan ditampilkan adalah hasil tampilan antarmuka dari sistem yang telah dibangun serta hasil pengujian sistem yang telah dilakukan.

a. *Form Login*

Pada bagian sistem ini dilengkapi dengan Halaman *login*. Halaman *Login* digunakan untuk melakukan verifikasi *username* dan *password*.

Gambar 1. Tampilan Halaman *Form Login*

b. *Form* Menu Utama

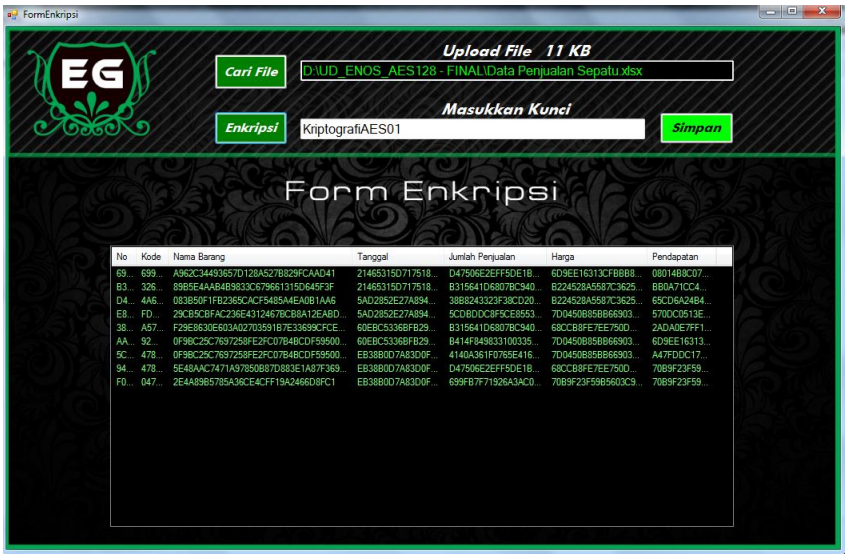
Menu utama adalah tampilan awal ketika user memasuki sistem. Halaman ini berisi tampilan luar tentang sistem kriptografi untuk pengamanan data penjualan pada UD. Enos Ginting.

Gambar 2. Tampilan Halaman *Form* Menu Utama

c. *Form* Enkripsi

Ketika *user* menekan tombol enkripsi maka sistem akan menampilkan halaman *form* enkripsi. *Form* Enkripsi adalah *Form* yang digunakan untuk melakukan enkripsi terhadap data penjualan.

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index



Gambar 3. Tampilan Halaman Setelah Data di Enkripsi

d. *Form* Dekripsi

Dalam *form* menu utama, ketika *user* menekan tombol dekripsi maka sistem akan menampilkan halaman *form* dekripsi. *Form* dekripsi adalah *Form* yang digunakan untuk melakukan dekripsi terhadap data *chipertext*.

Gambar 4. Tampilan Halaman Form Setelah Data di Dekripsi

4. KESIMPULAN

Berdasarkan hasil pembahasan tentang aplikasi kriptografi unruk pengamanan data penjualan sepatu yang telah dikemukakan, maka dapat diperoleh beberapa kesimpulan, adapun kesimpulan tersebut adalah sebagai berikut:

Dalam menganalisa data penjualan sepatu, langkah pertama yang dilakukan adalah memperoleh data penjualan dari UD. Enos Ginting melalui observasi dan wawancara. Kemudian data dianalisa sesuai dengan perhitungan algoritma AES (*Advanced Encrytion Standard*). Dan menerapkan perhitungan ke dalam pemograman *dekstop* dengan aplikasi VB 2010.

UCAPAN TERIMAKASIH

Terima Kasih diucapkan kepada kedua orang tua serta keluarga yang selalu memberi motivasi, doa dan dukungan moral maupun materi, serta pihak-pihak yang telah mendukung dalam proses pembuatan jurnal ini yang tidak dapat disebutkan satu persatu. Kiranya jurnal ini bisa memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

P-ISSN : 1978-6603 ; E-ISSN : 2615-3475
Volume 5. Nomor 1, Edisi April 2023
https://ojs.trigunadharma.ac.id/index.php/jct/index

REFERENCES

[1] L. Sodikin, T. Hidayat, and U. Wiralora, "ANALISA KEAMANAN E - COMMERCE MENGGUNAKAN METODE," vol. 3, no. 2, pp. 8–13, 2020.

[2] E. K. Gost et al., "Jurnal Teknologi Informasi dan Komunikasi STMIK Subang, April 2018 ISSN: 2252-4517," no. April, pp. 49–66, 2018.

[3] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Jurnal Pendidikan Sains dan Komputer," vol. 2, no. 1, pp. 163–171, 2022.

[4] V. No, D. Balai, P. Sungei, M. F. Fachrozi, and H. Fahmi, "Penerapan Metode AES-128 Untuk Pengamanan Data Absensi FingerPrint," vol. 3, no. 3, pp. 1–8, 2021.

[5] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," vol. 4, pp. 78–86, 2020, doi: 10.30865/komik.v4i1.2590.

[6] A. Pariddudin and F. Syauqi, "Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket," vol. 10, no. 2, pp. 43–52, 2020.

[7] P. Studi, T. Informatika, and U. M. Sukabumi, "STUDI TERHADAP ADVANCED ENCRYPTION STANDARD (AES) DAN," vol. 7, no. 1, 2017.

[8] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," vol. 4, no. 1, pp. 49–57, 2020, doi: 10.29099/ijair.v4i1.154.

[9] A. Susilo et al., "Pengamanan File Video dengan algoritma Advanced Encryption Standard (AES)," vol. 2, no. 1, pp. 28–32, 2020.

[10] A. K. Aes, "IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DI BALAI DESA TANDING MARGA DENGAN METODE STEGANOGRAFI LSB DAN ALGORITMA KRIPTOGRAFI AES," vol. 7, no. 1, pp. 63–71, 2021.

[11] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web," vol. 7, no. 1, pp. 148–155, 2020, doi: 10.30865/jurikom.v7i1.1943.

[12] A. Kak, "Lecture 8 : AES : The Advanced Encryption Standard Lecture Notes on ' Computer and Network Security ' Goals :," no. 3, 2021.

[13] B. Force, "PENINGKATAN PENGAMANAN DATA FILE MENGGUNAKAN ALGORITMA KRIPTOGRAFI," pp. 14–25.

[14] L. H. Sijabat, N. I. Syahputri, and M. Khairani, "Kriptografi dan Steganografi Penyembunyian Pesan Pada Media Audio Menggunakan Algoritma AES," vol. 6341, no. April, pp. 1–7, 2021.