Jurnal CyberTech
Vol. . No. , April 2020, pp.
E-ISSN: 30-08-2020

PENERAPAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDART* 128 BIT UNTUK PENGAMANAN DATA PINJAMAN NASABAH PADA KOPERASI WALET

Efrat Simbolon [*], Kamil Ermansyah, S.Kom., M.Kom [**], Ita Mariami, S.Kom., M.Kom[*]
[#1]Program Studi Sistem Informasi, STMIK Triguna Dharma
[#2,3]Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:

Keyword:
Data Pinjaman Nasabah, Kriptografi, AES 128

ABSTRACT

Data Pinjaman Nasabah merupakan sebuah data penting yang dimana data tersebut tidak boleh diketahui oleh anggota ataupun nasabah yang tidak berkepentingan. Alasan kenapa data tersebut dikatakan rahasia adalah untuk menghindari tindakan manipulasi data yang akan mengacaukan dan merusak manajemen koperasi.

Dengan membangun sistem pengamanan data Advanced Encryption Standart 128 bit Untuk Pengamanan Data Pinjaman Nasabah Pada Koperasi Walet, diharapkan dapat membantu mengamankan Data Pinjaman Nasabah secara baik, aman dan cepat, sehingga informasi yang ada pada berkas perusahaan tersebut tidak dapat diketahui oleh pihak lain yang tidak berkepentingan.

Output yang dihasilkan dari pengmanan data menggunakan metode AES 128 bit adalah teks berbentuk acak yang tidak akan dapat dipahami oleh orang yang idak berkepentingan maupun orang yang ingin merusak data manajemen koperasi walet terkecuali pihak koperasi walet yang mengetahui sandi untuk mendekripsikan teks acak yang telah di enkripsikan.

***Kata Kunci** : Data Pinjaman Nasabah, Kriptografi, AES 128*

Corresponding Author :
Nama : Efrat Simbolon
Kantor : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : efratleoo@gmail.com

1. PENDAHULUAN

Kegiatan pinjam-meminjam uang adalah salah satu kebutuhan manusia dimana kegiatan ini telah dilakukan masyarakat sejak masyarakat mengenal uang sebagai alat pembayaran. Hampir semua masyarakat telah menjadikan kegiatan pinjam-meminjam uang sebagai sesuatu yang sangat diperlukan untuk mendukung perkembangan kegiatan perekonomiannya dan meningkatkan taraf kehidupannya Bagi perkembangan ekonomi suatu negara, uang merupakan suatu kebutuhan. Bahkan bagi negara maju sekalipun, uang sangat berperan dalam perkembangan ekonomi negaranya. Hal ini disebabkan karena untuk menjalankan pembangunan, uang masih dianggap sektor yang paling vital menurut tinjauan ekonomi. Uang tersebut dapat digunakan untuk mendirikan usaha-usaha kecil dan digunakan untuk keperluan lainnya. Adapun salah satu cara untuk mendapatkan uang adalah melalui kredit [1].

Koperasi walet adalah sebuah organisasi ekonomi yang dimiliki dan dioperasikan oleh orang-orang demi kepentingan bersama. Koperasi ini melandaskan kegiatan berdasarkan prinsip gerakan ekonomi rakyat yang berdasarkan asas kekeluargaan. Data Pinjaman Nasabah adalah sebuah data yang dimana di dalamnya tertulis dengan jelas nama dan keterangan lengkap nasabah yang melakukan peminjaman beserta informasi lainnya. Data Pinjaman Nasabah merupakan sebuah data penting yang dimana data tersebut tidak boleh diketahui oleh anggota ataupun nasabah yang tidak berkepentingan. Alasan kenapa data tersebut dikatakan rahasia adalah untuk menghindari tindakan manipulasi data yang akan mengacaukan dan merusak manajemen koperasi.

Untuk itu ada sebuah cara dalam ilmu komputer yang mampu menangani pengamanan Data Pinjaman Nasabah tersebut, hal ini mungkin dapat membantu Koperasi Walet dalam mengamankan Data Pinjaman Nasabah sehingga tidak merugikan koperasi. Ilmu tersebut merupakan ilmu Kriptografi, dimana Kriptografi merupakan teknik dalam merubah atau mengacak teks asli dengan sebuah kunci dan membentuk hasil enkripsi agar tidak terbaca oleh orang atau user yang tidak memiliki kunci atau pun hak akses [2].

Dari permasalahan yang telah dijelaskan diatas, diharapkan dapat dibangun sistem yang membantu Koperasi Walet dalam mengamankan Data Pinjaman Nasabah. Berdasarkan permasalahan tersebut, maka diangkatlah judul karya ilmiah yaitu **"Penerapan Kriptografi *Advanced Encryption Standart* 128 bit Untuk Pengamanan Data Pinjaman Nasabah Pada Koperasi Walet".**

2. KAJIAN PUSTAKA

2.1 Koperasi

Secara umum, koperasi dapat diartikan sebagai badan usaha yang dimiliki serta dikelola para anggotanya. Namun, ada pengertian lain dari koperasi menurut beberapa ahli. Salah satunya dari Bapak Koperasi, Mohammad Hatta. Menurutnya, koperasi adalah usaha bersama guna memperbaiki atau meningkatkan kehidupan atau taraf ekonomi berlandaskan asas tolong menolong.

Sementara itu, Arifinal Chaniago mengartikan koperasi sebagai suatu perkumpulan yang bekerja sama dalam menjalankan sebuah usaha secara kekeluargaan guna meningkatkan kesejahteraan anggotanya. Pengelolaan sebuah koperasi, para anggotanya dapat dengan bebas untuk keluar dan masuk dari badan usaha tersebut.

2.2 Nasabah

Nasabah adalah orang atau badan hukum yang mempunyai rekening baik rekening simpanan atau pinjaman pada pihak bank. Sehingga nasabah merupakan orang yang biasa berhubungan dengan atau menjadi pelanggan bank. Dengan kata lain nasabah adalah pihak atau orang yang menggunakan dan secara sengaja menjadi langganan bank yang di percayai nya.

2.3 Kriptografi

Kriptografi adalah ilmu teknik enkripsi dimana "naskah asli" (*plaintext*) diacak dengan menggunakan suatu kunci enkripsi menjadi "naskah acak yang akan susah dibaca" (*ciphertext*). Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata "kriptografi" di bagi menjadi dua, yaitu *kripto* dan *graphia*. Dimana *kripto* yang memiliki arti *secret* (rahasia) dan *Graphia* berarti *writing* (tulisan) [5] .

2.4 Metode AES 128

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde. Proses di dalam AES merupakan transformasi terhadap *state* [9]. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai *state*. Enkripsi AES adalah transformasi terhadap *state* secara berulang dalam beberapa ronde. *State* yang menjadi keluara ronde k menjadi masukan untuk ronde ke-k +1.

Pada Proses enkripsi awalnya teks asli dibentuk sebagai sebuah *state*. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut *AddRoundKey*). Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde. AES menggunakan 4 jenis transformasi yaitu:

a. *SubBytes*, sebagai transformasi subtutusi.
b. *ShiftRows*, sebagai transformasi permutasi.

c. *MixColumns*, sebagai transformasi pengacakan.
d. *AddRoundKey*, sebagai transformasi penambahan kunci.

2.4 UML (Unified Modeling Language)

Pada perkembangan teknologi perangkat lunak, diperlukan adanya bahasa yang digunakan untuk memodelkan perangkat lunak yang akan dibuat dan perlu adanya standarisasi agar orang di berbagai negara dapat mengerti pemodelan perangkat lunak [11]. Seperti yang kita ketahui bahwa menyatukan banyak kepala untuk menceritakan sebuah ide dengan tujuan untuk memahami hal yang sama tidaklah mudah. Oleh karena itu, diperlukan sebuah bahasa pemodelan perangkat lunak yang dapat dimengerti oleh banyak orang [12].

Unified Modelling Language (UML) adalah bahasa pemodelan untuk sistem atau perangkat lunak yang berparadigma berorientasi objek. Abstraksi konsep dasar UML terdiri dari structural classification, dynamic behavior, dan model management dapat kita pahami main concepts sebagai term yang akan muncul pada saat membuat diagram dan view adalah kategori dari diagram tersebut. [13].

2.5 Flowchart

Flowchart (Bagan Alir) adalah bagan(*chart*) atau diagram yang digunakan untuk menunjukkan alir suatu proses (*flow*) di program atau prosedur sistem secara logika. *Flowchart* merupakan sebuah gambaran secara simbolik dari suatu algoritma atau prosedur dalam penyelesaikan suatu masalah, *Flowchart* difungsikan untuk memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan pada analisis permasalahan, disamping itu *Flowchart* juga berguna sebagai sarana dalam melakukan komunikasi antar pemrogram yang bekerja dalam tim suatu proyek. *Flowchart* membantu memahami urutan-urutan logika yang rumit dan panjang [15].

Flowchart membantu mengkomunikasikan jalannya program ke orang lain (bukan pemrogram) akan lebih mudah [15]. *Flowchart* atau bagan alir merupakan suatu bagan difungsikan untuk menunjukkan arah aliran kegiatan dan data-data yang dimiliki program sebagai suatu proses eksekusi, dan *Flowchart* biasanya berisi simbol-simbol grafis yang mudah dibaca. [16]

3. METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode Penelitian yang dilakukan pada tahap ini adalah mendapatkan data yang akan digunakan untuk menyelesaikan masalah dengan dengan mengadakan studi langsung kelapangan untuk mengumpulkan data.

Adapun metode dalam penelitian ini mencakup :

1. Teknik Pengumpulan Data

   Teknik pengumpulan data berupa suatu pernyataan tentang sifat, keadaan, kegiatan tertentu dan sejenisnya. Pengumpulan data dalam penelitian di Koperasi Walet tentang pengamanan data pinjaman nasabah menggunakan 2 cara berikut merupakan uraian yang digunakan :

   a. Wawancara

      Pengumpulan data dengan melakukan tanya jawab langsung dengan narasumber dari objek yang diteliti untuk memperoleh yang diinginkan. Wawancara dilakukan guna mendapatkan alur kerja pada objek yang diteliti yang akan digunakan dalam menentukan fitur-fitur yang akan dibangun. Pada tahapan wawancara dilakukan dengan cara mewawancarai staff pada Koperasi Walet tentang data pinjaman nasabah yang ingin diamankan. Berikut ini adalah data yang diperoleh dari Koperasi Walet

Tabel 3.1. Form Data Cicilan Pinjaman Nasabah.

Nama Nasabah	Usaha	Pinjaman	Cicilan yang sudah terbayar	Jumlah Cicilan yang berjalan	Jumlah Cicilan	Keterangan
Yatini	Warkop	1,500,000	600,000	Cicilan ke-6	15	-
Hary Pratama	Rujak	500,000	200,000	Cicilan ke-2	5	-
Bayu Akbar	Telur Gulung	750,000	750,000	Cicilan ke-7	7	Lunas
Nita Handayani	Salad Buah	300,000	100,000	Cicilan ke-2	3	-
Nursiah	Ayam Penyet	400,000	100,000	Cicilan ke-1	4	-
IIS Pitriani	Kue Keliling	750,000	150,000	Cicilan ke-1	5	-
Sumarni	DG	500,000	100,000	Cicilan ke-1	5	-
Firmanto	Telur Gulung	500,000	200,000	Cicilan ke-1	5	-
Firton Gurning	Jamur Goreng	500,000	300,000	Cicilan ke-6	10	-

3.2 Metodologi Perancangan Sistem

Metodologi Perancangan Sistem adalah suatu tahapan yang harus dilakukan setelah menganalisis sebuah masalah, pada tahapan inilah perancangan sebuah sistem direncanakan. Salah satu cara dalam merancang atau membangun sebuah sistem adalah dengan menggunakan Metode *Waterfall*.

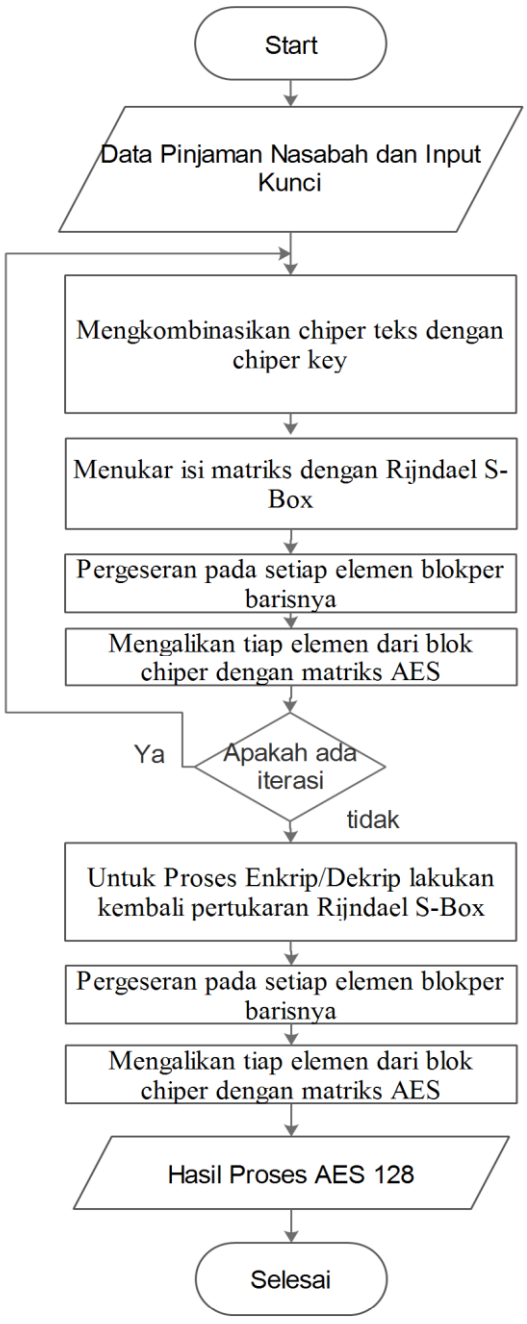
Metode *Waterfall* digunakan untuk menyediakan pendekatan alur hidup perangkat lunak secara sekuensial terurut dimulai dari analisis, desain, pengkodean, pengujian dan tahap pendukung (*support*). Sesuai dengan rumusan masalah yang menggunakan pendekatan *Classic or Waterfall Algorithm* maka berikut ini adalah teknik perancangan sistem yang digunakan:

a. Analisis Masalah dan Kebutuhan
   Pada tahapan Analisis Masalah dan Kebutuhan, dilakukan dengan penelitian, wawancara ke Koperasi Walet . Dimana penelitian pada tahap ini dilakukan dengan cara mencari permasalahan dan persoalan persoalan tentang pinjaman nasabah yang ingin diamankan.
b. Perancangan Sistem dan Pemodelan
   Tahap Perancangan dan Pemodelan berfokus pada struktur data, arsitektur perangkat lunak, *representasi interface*, dan *detail* (algoritma) prosedural. Pada tahapan ini dirancanglah tampilan program dan *database* yang akan digunakan pada sistem. Yang sebelumnya telah dimodelkan dengan menggunakan *Unified Modelling Language* (UML).
c. Pengkodean
   Pengkodean dilakukan dengan menterjemahkan hasil dari Perancangan dan Pemodelan ke dalam bahasa pemrograman berbasis *Desktop Programing* agar dikenali oleh komputer agar menjadi suatu sistem yang menjadi solusi dari permasalahan untuk mengamankan data pinjaman nasabah dengan menggunakan model AES 128 Bit.
d. Percobaan Awal
   Melakukan pengujian program atau sistem yang telah dikodekan agar mengetahui *bug-bug* yang ada pada program atau sistem yang telah dirancang agar diperoleh sistem yang berjalan sesuai dengan yang telah dirancang sebelumnya. Pada tahapan ini, program atau sistem yang telah dibangun akan di ujicoba sendiri, dan melihat setiap detil program apakah berjalan sesuai dengan yang telah dirancang ataukah masih ada kesalahan.
e. Percobaan Akhir
   Pada tahapan percobaan akhir, sistem yang telah melalui tahapan Percobaan Awal akan diterapkan pada *user*, dan dilakukan pengujian oleh *user*. Dalam tahap ini ditinjau pula apakah program sudah layak untuk digunakan pada Koperasi Walet .
f. Implementasi Sistem

Implementasi merupakan tahapan akhir setelah sistem melalui 5 tahapan sebelumnya dan layak untuk digunakan. Pada tahapan ini dilihat pula perkembangan aplikasi, dan melihat sejauhmana aplikasi atau sistem dapat bekerja melakukan mengamankan data pinjaman nasabah dengan akurat.

3.3 Algoritma Sistem

Algoritma sistem merupakan langkah-langkah yang dilakukan sebuah sistem dalam memproses dan menyelesaikan suatu permasalahan. Berikut ini adalah *flowchart* atau alur dari pemecahan permasalahan dengan menggunakan metode AES 128 Bit.



Gambar 3.1 *Flowchart* AES 128 Bit

Tabel 3.2 *Form* Data Cicilan Pinjaman Nasabah

Nama Nasabah	Usaha	Pinjaman	Cicilan yang sudah terbayar	Jumlah Cicilan yang berjalan	Jumlah Cicilan	Keterangan
Yatini	Warkop	1,500,000	600,000	Cicilan ke-6	15	-

Dikarenakan pemrosesan untuk algoritma AES 128 menggunakan konsep *Block Chipper* maka untuk tahap awal (sampel) dalam kasus ini akan diambil blok text "600.000 cicilan ke 6" dengan *ChiperKey* : 1234123412341234

Tabel 3.3 Konversi Ascii

Text	Kode ASCII
6	54
0	48
0	48
0	48
0	48
0	48
C	99
I	105
C	99
I	105
L	108
A	97
N	110
K	107
E	101
6	54

Membentuk Plaintext dan Chipperkey menjadi blok16 Byte
Plaintext =

54	48	48	48
48	48	99	105
99	105	108	97
110	107	101	54

Dalam Hexadesimal =

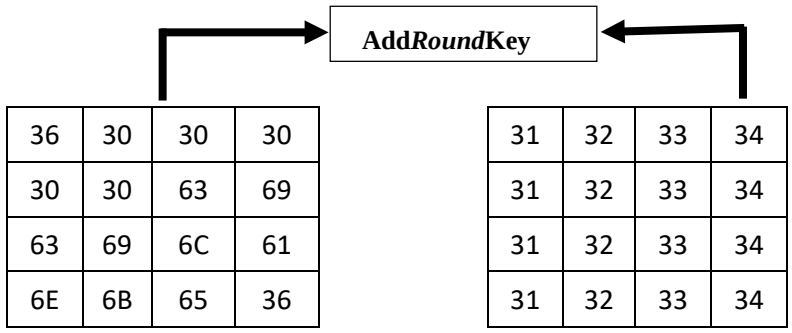
36	30	30	30
30	30	63	69
63	69	6C	61
6E	6B	65	36

Chipper Key =

49	50	51	52
49	50	51	52
49	50	51	52
49	50	51	52

Dalam Hexadesimal =

31	32	33	34
31	32	33	34
31	32	33	34
31	32	33	34



Hasil XOR

68	53	47	5D
5F	5B	13	43
50	40	58	5B
41	12	13	14

Langkah selanjutnya Sub*Bytes()* yaitu mensubtitusikan St_3 dalam bentuk heksadesimal kedalam tabel **S-Box** sehingga menghasilkan St_4. Dimana diketahui $S_{r,c}$ sebagai *state* 3 serta *r* (*row*) merupakan baris dan *c* (*coloum*) merupakan kolom. Digambarkan **'68'** menjadi **'45'** sebagai berikut :

Tabel 3.4 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	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	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	6	5	A0	52	3B	D6	B3	29	E3	2F	84

						E	A									
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	**45**	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	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	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

Berikut ini adalah hasil dari proses penggunaan S-Box

45	ED	A0	4C
CF	39	7D	1A
53	09	6A	39
83	C9	7D	FA

Kemudian dilanjutkan dengan proses *ShiftRows()* dengan menggeser secara *cyclic* sebagai berikut :

45	ED	A0	4C
CF	39	7D	1A
~~53~~	~~09~~	~~6A~~	~~39~~
~~45~~	~~ED~~	~~A0~~	~~4C~~
~~83~~	~~C9~~	~~7D~~	~~FA~~
~~39~~	~~7D~~	~~1A~~	~~CF~~
6A	39	53	09
FA	83	C9	7D

		45	ED	A0	4C
	CF	39	7D	1A	
53	09	6A	39		
83	C9	7D	FA		

3.3.2 Proses Enkripsi

Langkah selanjutnya yaitu MixColoums() dihasilkan dari perkalian antara koefisien { ‘02’ ; ‘03’ ; ‘01’ ; ‘01’ } yang ditetatapkan Rijndael dengan (per-word). Operasi yang dilakukan sebagai perkalian matriks dengan merepresentasikan ke dalam bentuk polinomial sehingga mendapatkan Persamaan, dijelaskan sebagai berikut :

w0 = 45 39 6A FA
w1 = ED 7D 39 83
w2 = A0 1A 53 C9
w3 = 4C CF 9 7D

Sebagai contoh w0 = 45396AFA dibawah ini

s0,c = ([02] • 45) xor ([03] • 39) xor ([01] • 6A) xor ([01] • FA)
s1,c = ([01] • 45) xor ([02] • 39) xor ([03] • 6A) xor ([01] • FA)
s2,c = ([01] • 45) xor ([01] • 39) xor ([02] • 6A) xor ([03] • FA)
s3,c = ([03] • 45) xor ([01] • 39) xor ([01] • 6A) xor ([02] • FA)

Representasi polinomial :

‘01’ = 00000001 = 1 ; elemen identitas (•)
’02’ = 00000010 = x
‘03’ = 00000011 = $x + 1$
‘45’ = 01000101 = $x^6 \square x^2 \square 1$
‘39’ = 00111001 = $x^5 \square x^4 \square x^3 \square 1$
‘6A’ = 01101010 = $x^6 \square x^5 \square x^3 \square x$
‘FA’ = 11111010 = $x^7 \square x^6 \square x^5 \square x^4 \square x^3 \square x$

1. s0,c = ([02] • 45) xor ([03] • 39) xor ([01] • 6A) xor ([01] • FA)

   ([02] • 45) = (x) • ($x^6 \square x^2 \square 1$) = $x^7 \square x^3 \square x$ = 10001010

   ([03] • 39) = $(x + 1)$ • ($x^5 \square x^4 \square x^3 \square 1$)
   = ($x^6 \square x^5 \square x^4 \square x$)+ ($x^5 \square x^4 \square x^3 \square 1$)
   = $x^6 \square x^3 \square x$+1 = 01001011

   ([01] • 6A) = (1) • ($x^6 \square x^5 \square x^3 \square x$) = 01101010

   ([01] • FA) = (1) • ($x^7 \square x^6 \square x^5 \square x^4 \square x^3 \square x$) = 11111010

2. s1,c = ([01] • 45) xor ([02] • 39) xor ([03] • 6A) xor ([01] • FA)

   ([01] • 45) = (1) • ($x^6 \square x^2 \square 1$) = 01000101

   ([02] • 39) = (x) • ($x^5 \square x^4 \square x^3 \square 1$)= $x^6 \square x^5 \square x^4 \square$ x = 01110010

   ([03] • 6A) = $(x + 1)$ • ($x^6 \square x^5 \square x^3 \square x$)
   = ($x^7 \square x^6 \square x^4 \square x^2$) + ($x^6 \square x^5 \square x^3 \square x$) = $x^7 \square x^5 \square x^4 \square x^3 \square x^2 \square x$
   = 10111110

   ([01] • FA) = (1) • ($x^7 \square x^6 \square x^5 \square x^4 \square x^3 \square x$) = 11111010

3. s2,c = ([01] • 45) xor ([01] • 39) xor ([02] • 6A) xor ([03] • FA)

   ([01] • 45) = (1) • ($x^6 \square x^2 \square 1$) = 01000101

   ([01] • 39) = (1) • ($x^5 \square x^4 \square x^3 \square 1$) = 00111001

   ([02] • 6A) = (x) • ($x^6 \square x^5 \square x^3 \square x$) = ($x^7 \square x^6 \square x^4 \square x^2$) = 11010100

   ([03] • FA) = $(x + 1)$ • ($x^7 \square x^6 \square x^5 \square x^4 \square x^3 \square x$)
   = ($x^8 \square x^7 \square x^6 \square x^5 \square x^4 \square x^2$) + ($x^7 \square x^6 \square x^5 \square x^4 \square x^3 \square x$)

$= (x^8 \square x^3 \square x^2 \square x) = 100001110$

$= 100001110$ xor $100011011 = 00010101$

4. s3,c = ([03] • 45) xor ([01] • 39) xor ([01] • 6A) xor ([02] • FA)

([03] • 45) = $(x + 1) \bullet (x^6 \square x^2 \square 1)$

$= (x^7 \square x^3 \square x) + (x^6 \square x^2 \square 1)$

$= (x^7 \square x^6 \square x^3 \square x^2 \square x + 1) = 11001111$

([01] • 39) = $(1) \bullet (x^5 \square x^4 \square x^3 \square 1) = 00111001$

([01] • 6A) = $(1) \bullet (x^6 \square x^5 \square x^3 \square x) = 01101010$

([02] • FA) = $(x) \bullet (x^7 \square x^6 \square x^5 \square x^4 \square x^3 \square x)$

$= (x^8 \square x^7 \square x^6 \square x^5 \square x^3 \square x^2) = 111101100$

$= 111101100$ xor $100011011 = 011110111$

Penjumlahan (□)

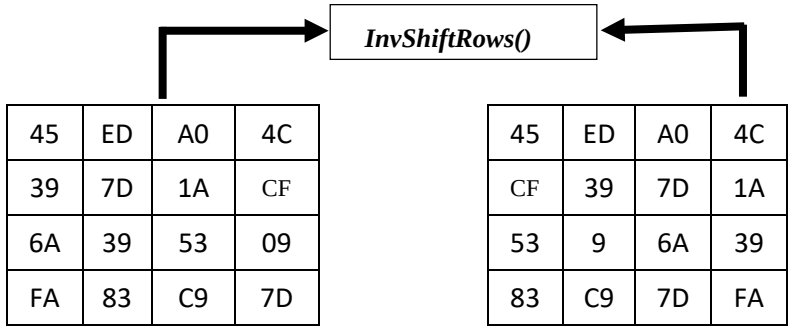
10001010	01000101	01000101	11001111
01001011	01110010	00111001	00111001
01101010	10111110	11010100	01101010
11111010	11111010	00010101	11110111
01010001	00110011	10111101	01101011
51	**33**	**BD**	**6B**

Chipertext yang terbentuk =

tHvinIoeVkOrMX+o3xWm0lgpsrFBeaZ8WXENSaCtBcULTdVJCK+qYyXC+dgxmuZR

3.3.3 Proses Dekripsi

Diasumsikan untuk round selanjutnya sama dengan simulasi di atas, hanya saja kunci yang digunakan pada *AddRounKey* menggunakan *key schedule.* Dekripsi merupakan penterjemahan *ciphertext* menjadi ke bentuk semula atau plaintext. Berikut ini akan disimulasikan pada Round ke-10 (Final Round) yang merupakan invers dari Cipher yang mana proses MixColoums() tidak diikut sertakan pada round ini. Dijelaskan dibawah ini



Tabel 3.5 S-Box Invers

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB

1	7C	E 3	39	82	9 B	2 F	F F	8 7	34	8E	43	44	C4	DE	E9	CB
2	54	7 B	94	32	A 6	C 2	2 3	3 D	E E	4C	95	0B	42	FA	C3	4E
3	08	2 E	A 1	66	2 8	D 9	2 4	B 2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	8 6	**6 8**	9 8	1 6	D 4	A4	5C	C C	5D	65	B6	92
5	6C	70	48	50	F D	E D	B 9	D A	5E	15	46	57	A7	8D	9D	84
6	90	D 8	A B		8 C	B C	D 3	0 A	F7	E4	58	05	B8	B3	45	06
7	D 0	2 C	1E	8F	C A	3 F	0 F	0 2	C1	AF	BD	03	01	13	8A	6B
8	3 A	91	11	41	4 F	6 7	D C	E A	97	F2	CF	C E	F0	B4	E6	73
9	96	A C	74	22	E 7	A D	3 5	8 5	E 2	F9	37	E8	1C	75	DF	6E
A	47	F1	1 A	71	1 D	2 9	C 5	8 9	6F	B7	62	0E	AA	18	BE	1B
B	F C	56	3E	4 B	C 6	D 2	7 9	2 0	9 A	DB	C0	FE	78	CD	5A	F4
C	1F	D D	A 8	33	8 8	0 7	C 7	3 1	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A 9	1 9	B 5	4 A	0 D	2 D	E5	7A	9F	93	C9	9C	EF
E	A 0	E 0	3 B	4 D	A E	2 A	F 5	B 0	C8	EB	BB	3C	83	53	99	61
F	17	2 B	04	7E	B A	7 7	D 6	2 6	E 1	69	14	63	55	21	0C	7D

Berikut adalah hasil S-box Invers

68	53	47	5D
5F	5B	13	43
50	40	58	5B
41	12	13	14

Langkah terakhir yaitu *AddRounKey()* dengan mengoprasikan XOR (lihat Tabel 2.3) antara St3 dan St4 . Sehingga menghasilkan St5 sebagai plaintext, dijelaskan sebagai berikut :

68	53	47	5D	
5F	5B	13	43	XOR
50	40	58	5B	

41	12	13	14

31	32	33	34
31	32	33	34
31	32	33	34
31	32	33	34

Hasil XOR

36	30	30	30
30	30	63	69
63	69	6C	61
6E	6B	65	36

Plaintext dalam bentuk *decimal* =

54	48	48	48
48	48	99	105
99	105	108	97
110	107	101	54

=>

6	0	0	0
0	0	C	I
C	I	L	A
N	K	E	6

Dari hasil dekripsi diatas maka terbentuk kembali plaintext dengan kalimat “ 600000 cicilanke6 ”

REFERENSI

[1] O. Dra Sri Purwantini, D. Rusdianti and M. dan Paulus Wardoyo, "KAJIAN PENGELOLAAN DANA KOPERASI SIMPAN PINJAM KONVENSIONAL DI KOTA SEMARANG," *Jurnal Dinamika Sosial Budaya*, vol. 18, no. 1, 2016.

[2] A. R. Tulloh, Y. Permanasari and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, 2016.

[3] D. Nurnaningsih and A. A. Permana, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," *JURNAL TEKNIK INFORMATIKA*, vol. 11, no. 2, pp. 177-186, 28 11 2018.

[4] F. Nandar Pabokory, I. Fitri Astuti and A. Harsa Kridalaksana, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD," 2015.

[5] M. E. A. Ely Setyo Astuti,Binar Prihadmantyo, "IMPLEMENTASI_ALGORITMA_KRIPTOGRAFI_RC4_DAN_METODE_," *Jurnal Teknologi Informatika dan Terapan* , vol. 4, no. 2, pp. 81-87, 2017.

[6] M. M. Amin, J. T. Komputer, P. Negeri and S. Palembang, "IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS," *Jurnal Pseudocode*, vol. 2, 2016.

[7] Arif Prayitno Nurdin, "ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHA SIA MENGGUNAKAN ALGORITMA CIPHER TRANSPOSITION," *JESIK*, vol. 3, no. 1, pp. 1-3, 2017.

[8] R. Sulaiman, D. Stmik and A. Luhur, "Konferensi Nasional Sistem Informasi 2018 STMIK Atma Luhur Pangkalpinang," 2018.

[9] A. Prameshwari, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *EKSPLORA INFORMATIKA*, vol. 8, no. 1, 2018.

[10] A. R. Tulloh, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, 2016.

[11] Suendri, "Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan)," *ALGORITMA: Jurnal Ilmu Komputer dan Informatika*, p. 1, 2018.

[12] W. Aprianti, U. Maliha, J. Teknik Informatika, P. Negeri, T. Laut, J. A. Y. Km, P. T. Laut and K. Selatan, "SISTEM INFORMASI KEPADATAN PENDUDUK KELURAHAN ATAU DESA STUDI KASUS PADA KECAMATAN BATI-BATI KABUPATEN TANAH LAUT," 2016.

[13] Sutejo, "Pemodelan UML Sistem Informasi Geografis Pasar Tradisional Kota Pekanbaru," *Jurnal Teknologi Informasi & Komunikasi Digital Zone, `Universitas Lancang Kuning* , vol. 7, 2016.

[14] S. Rosa, "Rekayasa perangkat lunak," Bandung, Informatika, 2017.

[15] R. Nurmalina, J. A. Yani Km, T. Laut and K. Selatan, "Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut)," *Jurnal Integrasi*, vol. 9, no. 1, pp. 84-91, 2017.

[16] d. E. F. R. Rasim1), Wawan Setiawan2), "Metodologi Pembelajaran Berbasis Komputer Dalam Upaya Menciptakan Kultur Pembelajaran Berbasis Teknologi Informasi dan Komunikasi," *2*, vol. 1, no. SSN:1979-9264 , 2008.

[17] P. Dwiyana Liksha, "APLIKASI AKUNTANSI PENGOLAHAN DATA JASA SERVICE PADA PT. BUDI BERLIAN MOTOR LAMPUNG," *Pefi Dwiyana Liksha JUSINTA*, vol. 1, no. 1, p. 1, 2018.

[18] N. David, M. Veronika and Y. Darnita, "RANCANG BANGUN APLIKASI TES TOEFL MENGGUNAKAN ALGORITMA QUICK SORT BERBASIS KOMPUTER," *Jurnal Pseudocode*, vol. 2, 2015.

[19] N. E. Putri and S. Azpar, "Sistem Informasi Pengolahan Data Pendidikan Anak Usia Dini (PAUD) Terpadu Amalia Syukra Padang," *Jurnal Edik Informatika* , vol. 2, 2019.

[20] T. Nata Lega and B. Eka Purnama, "PEMBANGUNAN SISTEM INFORMASI PERPUSTAKAAN PADA SEKOLAH MENENGAH ATAS NEGERI PUNUNG," *IJCSS - Indonesian Jurnal on Computer Science*, p. 1, 2019.

BIBLIOGRAFI PENULIS

Data Diri

Nama	: Efrat Simbolon
Tempat/Tanggal Lahir	: Maransar, 16 Desember 1996
Jenis Kelamin	: Laki-Laki
Agama	: Kristen
Status	: Belum Menikah
Pendidikan Terakhir	: Sekolah Menengah Atas
Kewarganegaraan	: Indonesia
E-mail	: efratleoo@gmail.com

	Kamil Ermansyah, S.Kom., M.Kom
	Ita Mariami, S.Kom., M.Kom