BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Terkait

2.1.1. Implementasi Algoritma ROT 13 Dalam Pengaman Data Kelahiran Pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Kabanjahe

Penelitian oleh Mikael Marpaung pada tahun 2020 bertujuan untuk menerapkan algoritma kriptografi ROT 13 dalam mengamankan data kelahiran pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Kabanjahe. Hasil yang diperoleh menunjukan bahwa algoritma ROT 13 dapat diimplementasikan dan diuji untuk mengamankan akta kelahiran. Dari penelitian yang dilakukan, peneliti menyarankan untuk penelitian selanjtnya melakukan kombinasi dari dua atau lebih algoritma kriptografi agar keamanan data lebih tinggi [6].

2.1.2. AES Encryption: Study and Evaluation

Penelitian yang dilakukan oleh Ahmad Loay Sousi, Dalia Yehya, dan Mohamad Joudi pada tahun 2020 dan diterbitkan oleh Rafik Hariri University. Peneliti mengimplementasikan algoritma kriptografi AES dan menganalisa algoritma tersebut. Hasil yang diperoleh oleh peneliti menunjukkan bahwa algoritma AES merupakan algoritma dengan keamanan tertinggi dibandingkan dengan algoritma lainnya seperti DES, 3DES, dll. Peneliti menyarankan menggunakan algoritma AES untuk mengamankan data dibandingkan menggunakan algoritma lainnya [7].

2.1.3. Aplikasi Pengaman Dokumen Simpan Pinjam Uang Di Pusat Koperasi Kartika "A" Bukit Barisan Menggunakan Metode *Advanced Encryption Standard* (AES)

Jurnal Cybertech oleh Rosodana Ito Hasibuan, Azannudin, S.Kom., M.Kom, dan Muhammad Syaifuddin, S.Kom., M.Kom yang dipublikasikan tahun 2020. Peneliti membuat suatu aplikasi berbasis *visual basic* sebagai penyimpanan dokumen pada Koperasi Kartika yang sebelumnya masih menggunakan cara manual dalam penyimpanan dokumen-dokumen penting.

Dalam membuat aplikasi, peneliti menerapkan algoritma kriptografi AES 128 untuk mengenkripsi data sehingga terjamin keamanannya. Hasil yang diperoleh dari penelitiannya yaitu aplikasi yang dibuat oleh peneliti dapat mempermudah koperasi dalam menyimpan dokumen simpan pinjam uang di *database*, mengamankan dokumen simpan pinjam uang, serta kemudahan dalam penggunaan aplikasi karena tampilan aplikasi dokumen yang dibuat sederhana. Pada penelitian selanjutnya, peneliti menyarankan untuk menggunakan algoritma kriptografi AES dengan jumlah bit yang lebih banyak sehingga lebih sulit dipecahkan dan menjaga keamanan dokumen-dokumen penting dengan lebih baik [8].

2.1.4. **Implementasi Super Enkripsi Menggunakan Metode *Rail Fance Cipher dan Metode Caesar Chiper Pada Data Pasien Klinik Eka Karigas***

Jurnal Sains Komputer dan Informatika yang ditulis oleh Fery Fernando dan Magdalena A. Ineke Pakereng pada tahun 2022 membahas mengenai penerapan algoritma kriptografi super enkripsi pada data pasien. Algoritma yang dipakai oleh peneliti yaitu algoritma *rail fance cipher* dan *caesar cipher.* Tujuan dilakukannya penelitian tersebut adalah untuk mengamankan data pasien di Klinik Eka Karigas agar terhindar dari pencurian data. Hasil yang diperoleh yaitu data-data penting dapat diamankan menggunakan super enkripsi namun penggunaan algoritma klasik dirasa kurang aman karena hanya melakukan pertukaran pada huruf-hurufnya. Sehingga, peneliti menyarankan untuk menambahkan algoritma kriptografi *modern* pada salah satu algoritma dimetode super enkripsi [9].

2.1.5. **Implementasi Algoritma *Vigenere Cipher* dan ROT 13 Untuk Keamanan Pesan Pada Aplikasi *Chatting***

Jurnal *of Informatics and Computer* yang ditulis oleh Desi Puspita Sari dan Nidia Enjelita Saragih dan dipublikasikan pada tahun 2023 membahas mengenai penerapan algoritma super enkripsi menggunakan *vigenere cipher* dan ROT13 pada aplikasi *chatting.* Tujuan dilakukannya penelitian tersebut yaitu untuk menyandikan suatu pesan menjadi kode-kode abstrak sehingga pesan dalam

aplikasi terjamin keamanannya. Hasil yang diperoleh dari penelitian yang dilakukan yaitu super enkripsi dapat mengamankan pesan pada aplikasi *chatting.* Namun, masih ada keterbatasan karakter pada penyandian, sehingga diharapkan pada penelitian selanjutnya dilakukan kombinasi algoritma dengan karakter yang lebih banyak [10].

2.1.6.**Implementasi *Caesar Chiper* dan *Advanced Encryption Standard* (AES) Pada Pengaman Data Pajak Bumi**

Jurnal Ilmiah Matrik yang dibuat oleh Fitri Nuraeni, Yoga Handoko Agustin, dan Angga Eka Purnama dan dipublikasikan tahun 2020, membahas mengenai penerapan dua algoritma kriptografi yaitu algoritma *Caesar Chiper* dan AES 128 untuk menjaga keamanan sistem informasi data pajak bumi dan bangunan tingkat desa. Hasil yang diperoleh dari penelitian yang dilakukan yaitu dibuatnya sistem informasi mempermudah pengelolaan data pajak bumi dan bangunan dan dengan diterapkannya super enkripsi maka data meminimalisir terjadinya kebocoran data. Namun, peneliti berharap pada penelitian selanjutnya tidak hanya data login saja yang diubah, namun beberapa data penting lainnya [11].

2.1.7.**Rancang Bangun Website Kriptografi Untuk Pengaman *File* Gambar Digital**

Jurnal yang ditulis oleh Ferdy Febrianto pada tahun 2022 yang diterbitkan di Jurnal Khatulistiwa Informatika, membahas mengenai perancangan sistem untuk membantu mengamankan data gambar digital dengan mengenkripsi menggunakan BASE 64. Hasil dari penelitian tersebut membuktikan bahwa *file* berbentuk gambar dapat terenkripsi walaupun ukuran *file* menjadi lebih besar. Tetapi ketika dilakukan dekripsi untuk mengembalikan gambar seperti semula, ukuran *file* menjadi sama seperti awal serta tidak penurunana kualitas pada gambar. BASE 64 dapat menjadi alternatif untuk pengenkripsian data sehingga membantu pengguna dalam mengamkan *file*. Namun, peneliti juga menyarankan untuk mengkombinasi BASE 64 dengan algoritma lainnya, karena BASE 64 tidak menggunakan kunci pada proses enkripsi maupun dekripsinya [12].

Tabel 2.1 Persamaan dan Perbedaan Dengan Penelitian Sebelumnya

No	Penulis	Tahun	Judul	Perbedaan	Persamaan
1	Mikael Marpaung	2020	Implementasi Algoritma ROT 13 Dalam Pengaman Data Kelahiran Pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Kabanjahe	Objek penelitian yang berbeda yaitu data kelahiran dan tempat penelitian yang berbeda, serta belum menerapkan super enkripsi.	Algoritma kriptografi yang digunakan sama yaitu algoritma ROT 13.
2	Ahmad Loay Sousi, Dalia Yehya, dan Mohamad Joudi	2020	AES Encryption: Study & Evaluation	Pada penelitian yang dilakukan fokus utamanya untuk menganalisa AES dengan algoritma lainnya.	Algoritma yang digunakan sama yaitu AES.
3	Rosodana Ito Hasibuan, Azannudin, S.Kom., M.Kom, dan Muhammad Syaifuddin, S.Kom., M.Kom	2020	Aplikasi Pengaman Dokumen Simpan Pinjam Uang Di Pusat Koperasi Kartika "A" Bukit Barisan Menggunakan Metode *Advanced Encryption Standard* (AES)	Tempat penelitian berbeda yaitu di Koperasi Kartika A, jumlah byte pada AES yang berbeda yaitu 128-bit, dan belum menerapkan super enkripsi	Tujuan penelitian yang sama yaitu mengimplementasikan algoritma kriptografi AES untuk keamanan *database* di lingkungan koperasi.
4	Fery Fernando dan Magdalena A. Ineke Pakereng	2022	Implementasi Super Enkripsi Menggunakan Metode Rail Fance Cipher dan Metode Caesar Chiper Pada Data Pasien Klinik Eka Karigas	Perbedaan penerapan algoritma yang kedua menggunakan algoritma klasik *rail fance chipper*. Objek penelitian yang berbeda yaitu data pasien di Klinik Eka Karigas, dan belum menerapkan super enkripsi.	Penerapan super enkripsi sama-sama menggunakan caesar chipper di salah satu algoritmanya.

No	Penulis	Tahun	Judul	Perbedaan	Persamaan
5	Desi Puspita Sari dan Nidia Enjelita Saragih	2023	Implementasi Algoritma *Vigenere Cipher* dan ROT 13 Untuk Keamanan Pesan Pada Aplikasi *Chatting*	Perbedaan objek penelitian yaitu pesan pada aplikasi *chatting* serta salah satu algortima yang digunakan yaitu *vigenere cipher*.	Menggunakan kriptografi super enkripsi dengan salah satu algoritmanya yaitu ROT 13.
6	Fitri Nuraeni, Yoga Handoko Agustin, dan Angga Eka Purnama	2020	Implementasi *Caesar Chiper* dan *Advanced Encryption Standard* (AES) Pada Pengaman Data Pajak Bumi	Objek penelitian yang berbeda yaitu data pajak bumi, Algoritma kriptografi yang digunakan berbeda yaitu *Caesar Chiper*, serta jumlah byte pada AES yang berbeda yaitu 128-bit.	Peneliti sama-sama menggunakan super enkripsi dengan salah satu algoritma yang diterapkan sama yaitu AES.
7	Ferdy Febrianto	2022	Rancang Bangun Website Kriptografi Untuk Pengaman *File* Gambar Digital	Pada penelitian yang dilakukan tidak mengkombinasikan algoritma BASE 64 dengan algoritma kriptografi lainnya.	Algoritma yang digunakan sama yaitu BASE 64 serta objek penelitian sama yaitu *file* gambar.

2.2. Dasar Teori

2.2.1. Koperasi

Koperasi merupakan organisasi berbadan hukum yang menjadi bagian dari usaha pembangunan nasional berdasarkan asas kekeluargaan. Keberhasilan suatu koperasi ditentukan oleh jalannya pengelolaan keuangan berdasarkan laporan keuangan yang diterbitkan oleh koperasi berisikan data simpan pinjam anggota koperasi. Simpan pinjam pada koperasi telah membantu banyak sekali masyarakat menengah kebawah untuk mendapatkan pinjaman dengan mudah sebagai modal usaha, kesehatan, pendidikan, dan lain-lain [13].

Koperasi Ngudi Rahayu merupakan bentuk usaha yang menyediakan jasa simpan pinjam. Beralamatkan di Jl. Suparto No.13 Kecamatan Baturaden Kabupaten Banyumas. Koperasi Ngudi Rahayu memiliki anggota sebanyak 49 orang. Anggota Koperasi Ngudi Rahayu merupakan warga Desa Purwosari. Di Koperasi Ngudi Rahayu sistem simpan pinjam hanya dapat dilakukan oleh anggota koperasi. Ketika seseorang hendak menjadi anggota koperasi, ia harus menyertakan informasi data diri diantaranya nama, nomor KTP, tempat tinggal, nomor telepon.

2.2.2. *Website*

Website merupakan layanan yang dapat berjalan diatas teknologi internet. *Website* berisikan halaman informasi yang dapat diakses dimanapun selama terkoneksi menggunakan jaringan internet. Berisikan beberapa komponen yang terdiri dari teks, gambar, suara, serta animasi yang membentuk suatu rangka bangunan yang berkaitan. Halaman pada *website* dapat diakses karena adanya teknologi *web server* sebagai penyedia halaman, HTML sebagai bahasa baku, serta HTTP sebagai jalur dokumen *web* dikirimkan [14].

2.2.3. *Personal Home Page* (PHP)

PHP merupakan software *open source* sebagai bahasa pelengkap HTML yang berfungsi untuk membuat sebuah aplikasi dinamis dan memungkinkan terjadinya pengolahan serta pemrosesan data. Semua *syntax* yang diberikan pada server akan dijalankan sepenuhnya namun yang dikirimkan ke *browser* hanyalah hasil saja.

PHP berfungsi untuk membangun sebuah aplikasi berbentuk *website.* Dari *web browser* program yang ditulis menggunakan bahasa PHP akan di*parsing* oleh *interprenter* PHP didalam *web server,* lalu diterjemahkan dalan dokumen HTML yang selanjutnya ditampilkan Kembali oleh *web server* [15].

2.2.4.MySQL

MySQL yang disebut juga SQL atau *Structured Query Language* berfungsi untuk mengolah *database* dari berbagai ukuran mulai dari kecil sampai yang sangat besar. MySQL bersifat relasional yang artinya data didalam *database* akan dikelola dan dikelompokkan pada beberapa tabel terpisah sehingga akan mempercepat manipulasi data. SQL memungkinkan pengguna untuk mengetahui lokasi atau proses informasi sebuah data disusun. SQL juga sebuah bahasa pemrogaman yang dirancang khusus untuk mengirim perintah *query* terhadap sebuah *database* [16].

2.2.5. Keamanan *Database*

Database adalah sekumpulan informasi yang tersimpan secara sistematik didalam komputer dan dapat diakses menggunakan suatu program apabila ingin memperoleh informasi yang terdapat dalam *database* tersebut. Pengertian umum dari *database* yaitu suatu sistem penyimpanan berisikan data-data yang diinput didalamnya. Sistem *database* mulai banyak dipergunakan dalam berbagai bidang, tidak hanya pada bidang teknologi, melainkan pada perusahaan besar hingga kecil, perkantoran, universitas, supermarket, hingga rumah-rumah [17].

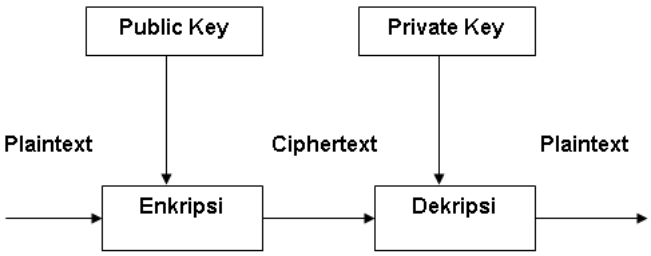
Ada banyak sekali keuntungan dari *database,* salah satunya yaitu kemampuan dalam berbagi data dan informasi serta memungkinkan akses dalam mengontrol data yang bertujuan untuk *data mining.* Namun, dengan kelebihan yang ada, *database* juga memiliki kekurangan. Kekurangan yang menjadi fokus utama yaitu dalam masalah keamanan. Keamanan *database* didefinisikan sebagai perlindungan data-data terhadap berbagai akses yang tidak sah maupun yang memiliki kewenangan untuk mengakses data dengan melakukan kontrol terhadap apa yang dapat diakses serta bagaimana caranya [18]. Menjaga keamanan pada *database*

sangatlah penting untuk mencegah berbagai bentuk ancaman baik ancaman fisik, geografis, maupun digital.

2.2.6. Kriptografi

Kriptografi diangkat dari bahasa Yunani yaitu "*cryptos*" berarti "*secret*" atau tersembunyi dan "*graphein*" berarti "*writing*" atau catatan. Secara umum, kriptografi diartikan sebagai ilmu atau seni dalam pengamanan suatu pesan. Kriptografi memiliki dua proses penting yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah bentuk suatu informasi atau data yang terkirim menjadi sulit diketahui menggunakan algoritma tertentu. Sedangkan proses dekripsi adalah proses mengubah informasi yang telah terenkripsi menjadi informasi awal.

Kriptografi memiliki dua tipe yaitu klasik dan modern. Kriptografi klasik digunakan sebelum adanya komputer dengan menggunakan metode subtitusi dan transposisi. Kriptografi modern merupakan tipe kriptografi yang mengacu pada kriptografi klasik dan dikirim melalui jaringan komputer. Berikut merupakan proses enkripsi dan dekripsi pada kriptografi :



Gambar 2.1. Alur Kriptografi

1. *Plaintext*

   Plaintext merupakan sebuah pesan berisikan informasi yang mudah dibaca serta dimengerti. *Plaintext* yang merupakan pesan bermakna akan diproses langsung menggunakan algoritma kriptografi.

2. *Ciphertex*

   Ciphertext yang bisa disebut juga dengan *cryptosystem* merupakan *plaintext* yang telah berisi sandi. Pesan pada *ciphertext* akan sulit dibaca karena telah melalui proses enkripsi untuk mengubah *plaintext* menjadi karakter-karakter

yang tidak memiliki makna dan bertujuan untuk mengamankan data didalamnya.

3. Kunci (*key*)

   Key merupakan peranan penting dalam kriptografi. Keamanan kriptografi biasanya bergantung pada kerahasiaan dalam memberikan *key*. *Key* berisikan parameter berbentuk string atau deretan bilangan yang digunakan untuk transformasi enkripsi dan dekripsi.

4. Kriptosistem (*cryptosystem*)

   Cryptosystem merupakan implementasi perangkat lunak algoritma kriptografi untuk mentransformasikan pesan asli menjadi *ciphertext* atau sebaliknya [19].

2.2.7.BASE 64

BASE 64 merupakan algoritma enkripsi dan dekripsi suatu data biner ke dalam format ASCII. Karakter yang dihasilkan pada transformasi BASE64 terdiri dari A..Z, a..z dan 0..9, simbol "+" dan "/", serta tambahan simbol "=" pada dua karakter terakhir sebagai pengisi pad atau bisa disebut sebagai penggenap data biner [20]. Tabel indeks BASE 64 dapat dilihat pada gambar 2.10.

Value	*Encoding*	*Value*	*Encoding*	*Value*	*Encoding*	*Value*	*Encoding*
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	-
15	P	31	f	47	v	63	_
						(*pad*)	=

Gambar 2.2. Indeks bilangan BASE 64

Pada format *file* gambar pengenkripsian BASE 64 melalui langkah-langkah berikut :

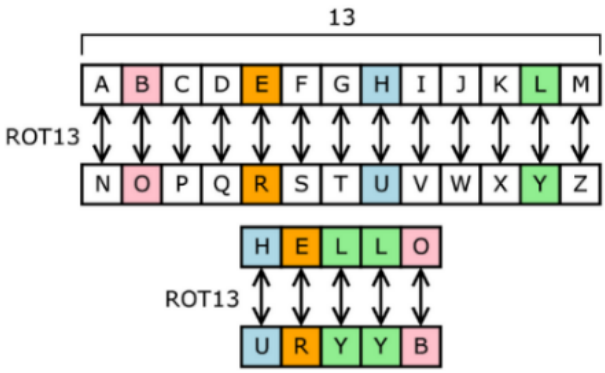
1. Ambil *file* gambar lalu pecah menjadi blok-blok data per-3 *bytes.*

Contoh : 01011011 11100010 10011001

2. Gabungkan 3 *bytes* menjadi 24 bit.
   Contoh : 010110111110001010011001
3. Pecah 24 bit menjadi 6 bit.
   Contoh : 010110 111110 001010 011001
4. Konversi setiap 6 bit ke dalam nilai desimal dengan nilai maksimal yang dapat dihasilkan dari 6 bit adalah 63.
   Contoh : 22 62 10 25
5. Jadikan nilai desimal sebagai *indeks* BASE 64.
   Contoh : W+al.

2.2.8.ROT 13

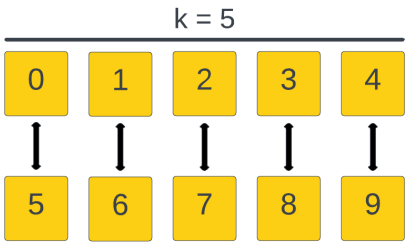
Algoritma ROT 13 (rotate by 13 places) merupakan salah satu algoritma dari perkembangan pergantian *Caesar Cipher* sederhana yang ditemukan pada sistem UNIX. Dalam ROT 13 pergeseran menggunakan *Caesar Chipher* sebesar k = 13. Huruf A pada ROT 13 diganti dengan N, huruf B diganti O, dan seterusnya.



Gambar 2.3. Pemetaan huruf dengan ROT 13

Gambar 2.1 merupakan pemetaan huruf-huruf plainteks dengan huruf-huruf cipherteks menggunakan ROT13. Pesan HELLO apabila disandikan menggunakan ROT13 akan menjadi URRYB [21].

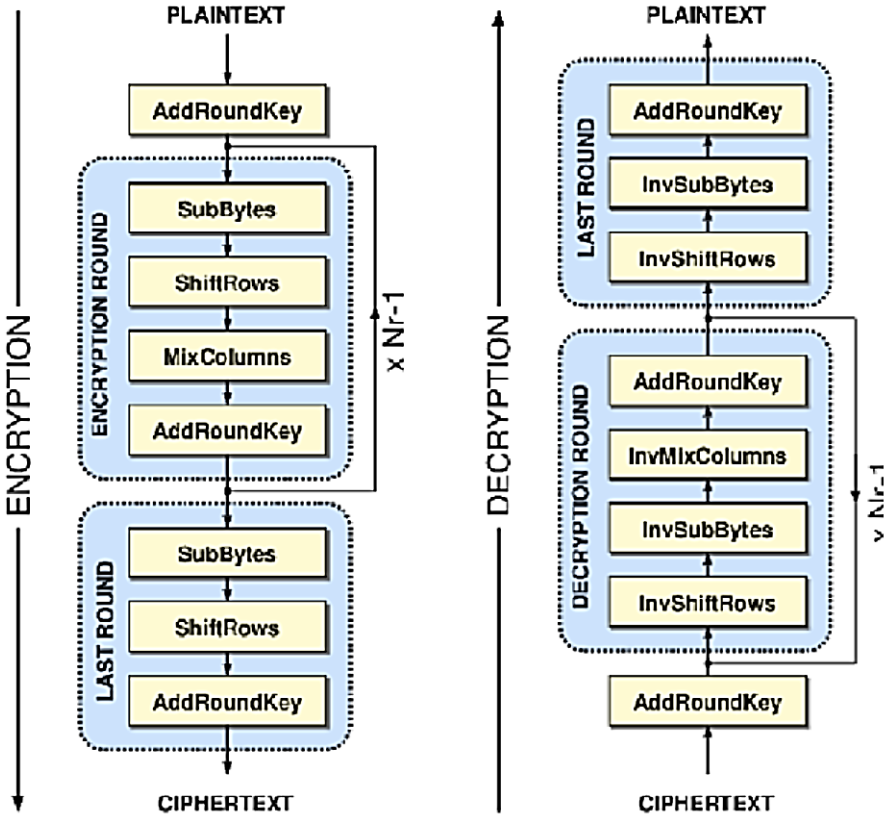
Pada penelitian ini, ROT 13 dikembangkan tidak hanya pergesaran pada huruf namun juga pergeseran pada angka. Pergeseran pada angka sebesar k = 5. Berikut merupakan pemetaannya :



Gambar 2.4. Pergesaran angka

2.2.9. AES 256

Advanced Encryption Standard (AES) dibuat pada tahun 1997. NIST mengumumankan bahwasannya algoritma enkripsi *Data Encryption Standard* (DES) akan digantikan oleh AES karena sudah tertinggal zaman dan dianggap tidak aman lagi. Di dalam kriptografi salah satu faktor penting dalam menjaga keamanan adalah panjang kunci pada ukuran jumlah bit yang digunakan. AES menetapkan tiga jumlah kunci yaitu AES 128, AES 192, dan AES 256. Semakin Panjang jumlah kunci akan semakin aman data yang disandikan [22]. Berikut merupakan proses enkripsi dan dekripsi pada AES 256 :



Gambar 2. 5. Proses enkripsi dan dekripsi AES

1. Proses Enkripsi AES

Proses enkripsi pada AES 256 melalui 4 proses transformasi *bytes* yaitu *SubBytes, ShiftRows, MixColumns, dan AddRoundKey*. *Plaintext* akan melalui proses *AddRoundKey,* kemudian tranformasi *SubBytes, ShiftRows, MixColumns,* dan Kembali ke *AddRoundKey* secara berulang sebanyak Nr pada putaran terakhir.

a. *Generated Key*

Langkah awal adalah menyediakan blok matriks (*array*) 128-bit berfungsi menyimpan kunci *cipher* yang akan dibangkitkan. Pada AES 256 nantinya terbentuk 2 buah blok matriks 128-bit karena panjang kunci AES 256 sejumlah 32 *byte*. Blok matriks tersebut berisikan kunci *cipher* AES 256 yang sekaligus menjadi kunci ronde ke-0 dan ke-1. Selanjutnya, menemukan kunci ronde ke-2 sampai ke-14 dengan menggunakan transformasi, diantaranya *RotWord, SubBytes,* dan XOR (*Exclusive OR)* menggunakan *RoundConstant* (RCon).

Tabel 2.2. Tabel Reon

KR2	KR4	KR6	KR8	KR10	KR12	KR14
01	02	04	08	10	20	40
00	00	00	00	00	00	00
00	00	00	00	00	00	00
00	00	00	00	00	00	00

b. *AddRoundKey*

AddRoundKey pada enkripsi dan dekripsi AES memiliki proses yang sama, sebuah *round key* ditambahkan pada *state* menggunakan operasi XOR. Setiap *round key* terdiri dari Nb *word* dimana setiap *word* akan dijumlahkan berdasarkan *word* yang bersesuaian, sehingga :

$[S'_0, c, S'_1, S'_2, c, S'_3, c] = [S_0, c, S_1, c, S_2, c, S_3, c]$ XOR $[W_{round*Nb+c}]$ untuk $0 \leq c \leq Nb$.

Proses enkripsi Transformasi *AddRoundKey* pertama kali pada *round* = 0, lalu selanjutnya *round* = *round* + 1. Sedangkan pada proses dekripsinya dilakukan pertama kali pada *round* 14 lalu selanjutnya *round* = *round* – 1 [17].

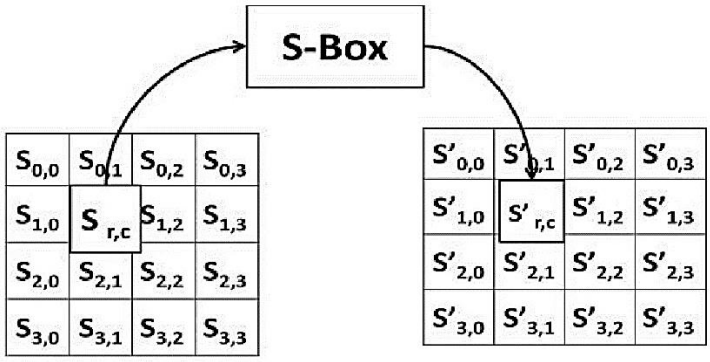
c. *SubBytes*

SubBytes merupakan perpindahan *byte* yang setiap unsur pada *state*nya akan dipetakkan menggunakan sebuah tabel (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	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	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

Gambar 2.6. Tabel *s-box* AES

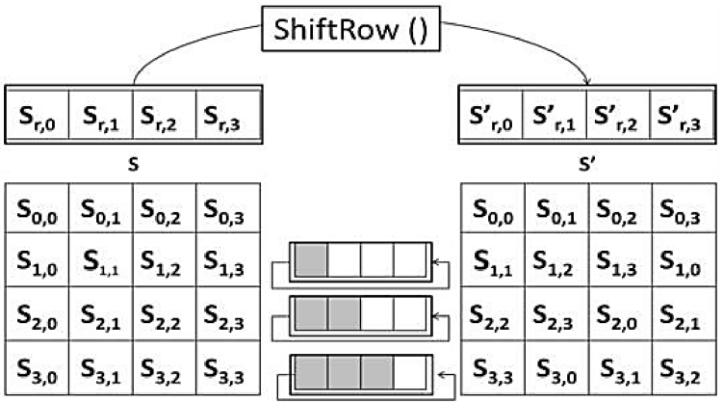
Setiap *byte* di*array state*, dimisalkan S[r,c] = xy, dimana xy merupakan digit *hexadecimal* dari nilai S[r,c]. Maka nilai substitusinya disimbolkan dengan S'[r,c] yang merupakan perpotongan kolom y dengan baris x.



Gambar 2.7. Pemetaan pada *byte* dalam *state*

d. *ShiftRows*

Transformasi *ShoftRows* adalah pertukaran bit dimana bit paling kiri akan ditukar menjadi bit yang paling kanan (rotasi bit).



Gambar 2.8. Tranformasi *shift rows*

e. *MixColumns*

MixColumns menjalankan elemen yang terdapat pada satu kolom di *state* menggunakan perkalian matriks.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Gambar 2.9. Transformasi *mix columns*

Hasil dari perkalian matriks adalah :

$$S'_{0,C} = (\{02\} \cdot S_{0,C}) \oplus (\{03\} \cdot S_{1,C}) \oplus S_{2,C} \oplus S_{3,C}$$

$$S'_{1,C} = S_{0,C} \oplus (\{02\} \cdot S_{1,C}) \oplus (\{03\} \cdot S_{2,C}) \oplus S_{3,C}$$

$$S'_{2,C} = S_{0,C} \oplus S_{1,C} \oplus (\{02\} \cdot S_{2,C}) \oplus (\{03\} \cdot S_{3,C})$$

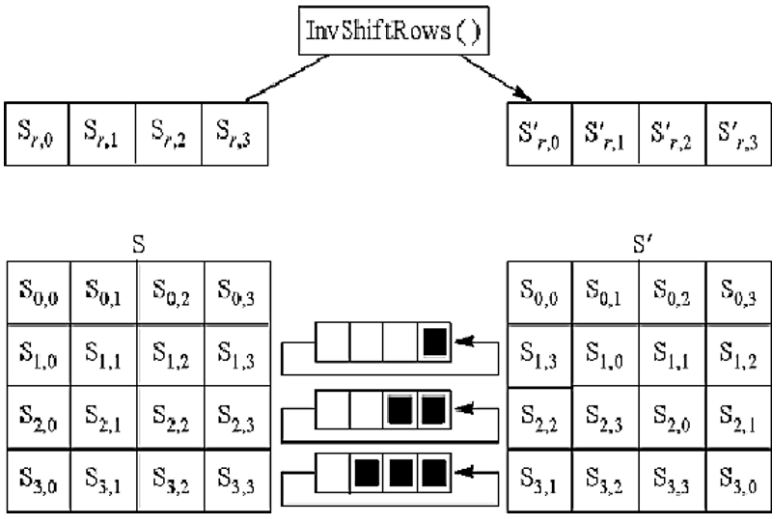
$$S'_{3,C} = (\{03\} \cdot S_{0,C}) \oplus S_{1,C} \oplus S_{2,C} \oplus (\{02\} \cdot S_{3,C})$$

2. Proses Deskripsi AES 256

Transformasi *cipher* diterapkan dalam arah yang berlawanan sehingga menghasilkan *invers cipher* yang mudah dipahami untuk AES 256. Transformasi *byte* yang digunakan dalam *invers chiper* antara lain *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*.

a. *InvShiftRows*

InvShiftRows merupakan lawan dari *ShiftRows*, sehingga dapat digambarkan sebagai berikut :



Gambar 2.10. Transformasi *inv shift rows*

b. *InvSubBytes*

Invers SubBytes merupakan transfer *bytes* yang berkebalikan dari *SubBytes*, pada elemen setiap *state* dipetakan menggunakan tabel S-Box. Berikut merupakan tabel S-Box :

	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	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 2.11. Tabel *inv s-box*

c. *InvMixColumns*

Setiap kolom dalam *state* dikalikan dengan matriks dalam AES [23].

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Gambar 2.12. Matriks perkalian *inv mix columns*