PERTEMUAN 13
PENERAPAN ALJABAR LINIER DI DALAM ILMU KOMPUTER

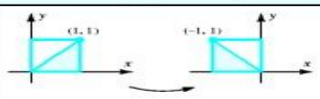
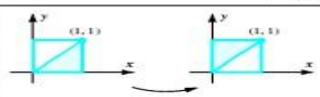
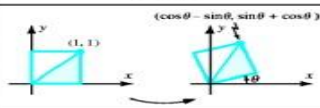
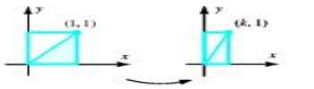
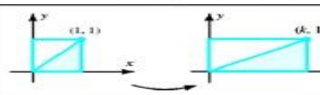
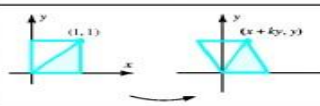
A. Tujuan Pembelajaran

Pada akhir pertemuan Mahasiswa mampu membuat kriptografi dan steganografi lalu menerapkannya untuk transformasi geometri, membuat game dan mengolah citra digital.

B. Uraian Materi

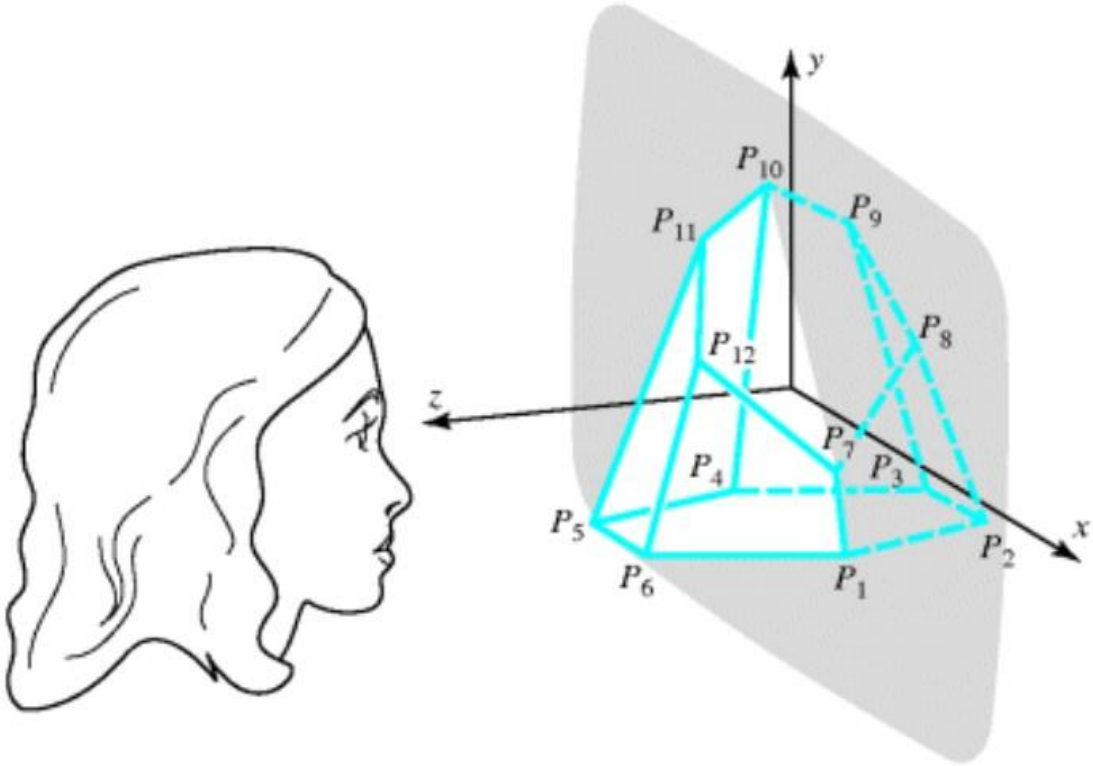
1. Penerapan Aljabar Linier di dalam Komputer Grafis

Didalam (Atmadja, Bandung, & Bandung, 2016) unsur komponen penunjang computer adalah grafis computer. Grafis computer berhubungan dengan image, warna, bentuk dan grafik. Baik dalam bentuk 2 dimensi maupun 3 dmensi. Pemprosesan grafis computer tidak lepas dari pembelajaran aljabar linear karena matrik dan operasinya sangat mempengaruhi.

Operator	Standard Matrix	Effect on the Unit Square
Reflection about the y-axis	$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$	
Reflection about the x-axis	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	
Reflection about the line $y = x$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	
Counterclockwise rotation through an angle θ	$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$	
Compression in the x-direction by a factor of k $(0 < k < 1)$	$\begin{bmatrix} k & 0 \\ 0 & 1 \end{bmatrix}$	
Expansion in the x-direction by a factor of k $(k > 1)$	$\begin{bmatrix} k & 0 \\ 0 & 1 \end{bmatrix}$	
Shear in the x-direction with factor $k > 0$	$\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$	
Shear in the x-direction with factor $k < 0$	$\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$	

Gambar 1. Operator utuk pembuatan grafis

Contoh jika kita ingin memvisualisasikan objek 3 dimensi dengan menampilkan berbagai padangan pada layer video. Objek yang kita ingin tampilkan merupakan tampilan dari sejumlah segmen garis lurus. Contoh berdasarkan ilustrasi gambar dibawah ini.

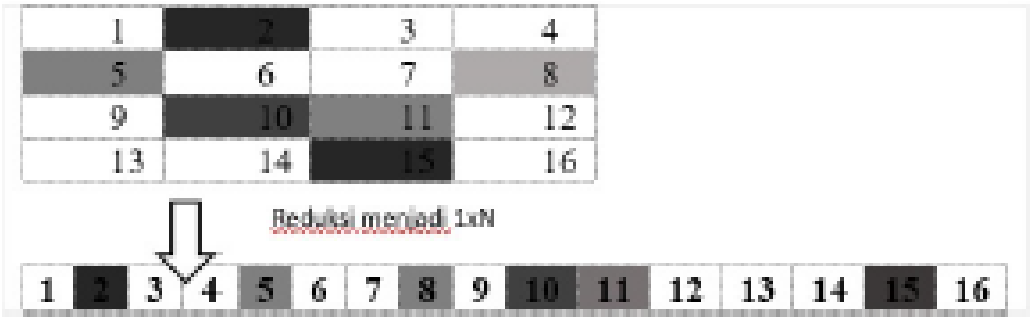


Gambar 2. Visualisasi gambar 3 dimensi

Gambar diatas memperkenalkan sistem kordinat XYZ untuk menanamkan objek. Kami mengarahkan kordinat sistem sehingga asal-usulnya berada ditengah layer video dan XY-pbjek bertepatan dengan bidang datar layar. Ini mengakibatkan seorang pengamat hanya akan melihat proyeksi pandangan objek 3 dimensi ke 2 dimensi.

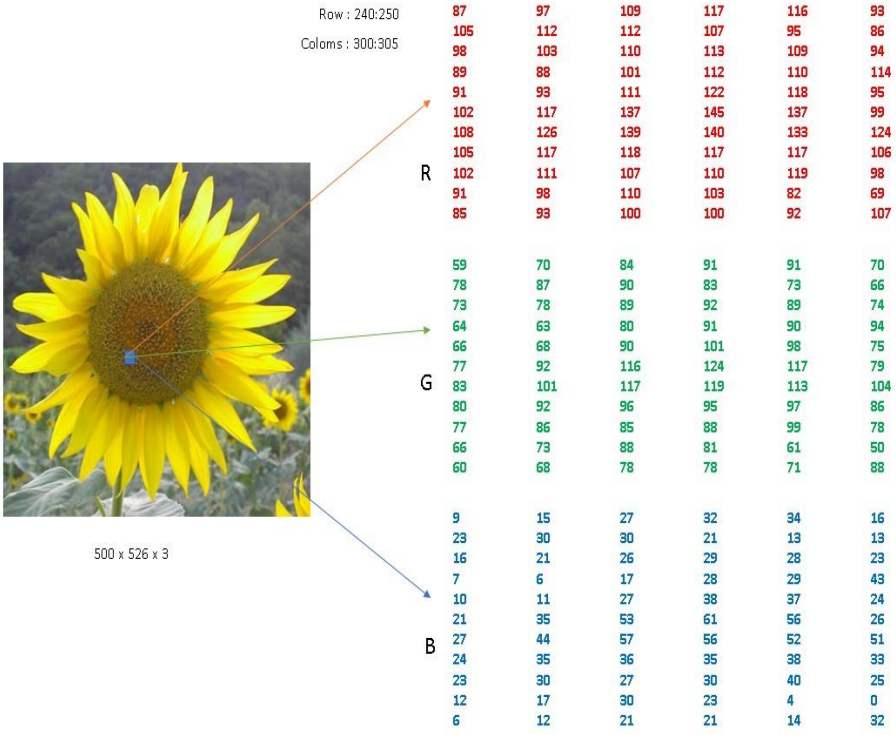
2. Penerapan Aljabar Linier dalam Image Processing

Didalam penelitian (Perani Rosyani, 2017) menjelaskan tentang penerapan aljabar linear didalam bidang image processing dalam proses pengenalan wajah. Didalam penerapannya matriks mxn di ubah menjadi matrik 1xn.



Gambar 1. Perubahan matriks MxN menjadi 1xcN

Penggunaan matrik ini untuk meningkatkan akurat didalam sebuah pecbngenalan gambar untuk pengenalan wajah dengan metode Principal ComponentAnalisys (PCA). Selain penggunaan matriks di atas aljabar linear dapat digunakan untuk mengekstrahsb, k warna didalam gambar. Karna gambar mempunya banyak jenis komponen warna seperti RGB, HSV, YCbCr, LAB, Dll. Contoh yang di terapkan adalah penggunaan warna RGB didalam gambar bunga matahari. Penelitian terkait mengenai ekstraksi warna terdapat didalam penelitian (P. Rosyani, Taufik, Waskita, & Apriyanti, 2019) yang mengekstrak setiap komponen warna untuk mendapatkan nilai akurasi terbaik.

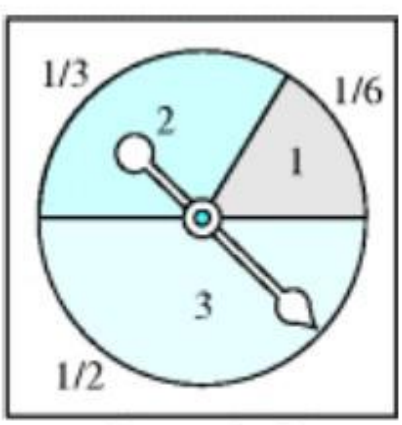


Gambar 2 Bedah Image

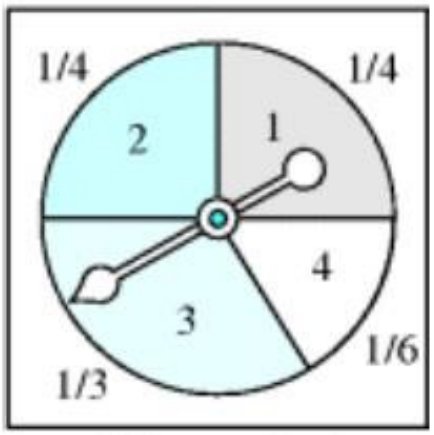
Didalam gambar 2 menjelaskan tentang implementasi matriks warna didalam sebuah gambar dengan ukuran 500 x 526 x 3, angka 3 menunjukan warna yang didalam memiliki 3 komponen warna yaitu R,G dan B didalam 1 titik akan memiliki nilai yang berbeda-beda dengan rentang ukuran warna 0 – 255. Gambar di atas di ambil dengan titik row : 240:250, dan colom : 300:305.

3. Penerapan Aljabar Linier di dalam Strategi Game

Untuk memperkenalkan konsep dasar dari teori game, kami akan mem[ertimbangkan jenis permainan karbaval berikut yang kedua pemainnya setuju untuk bermain bersama. Kami memanggil peserta dalam permainan dengan nama pemain R dan pemain C. setiap pemain memiliki roda stasioner dan pointer bergerak diatasnya. Seperti gambar di bawah ini. Dengan alas an kami akan memanggil roda dari pemain R didalam baris sedangkan roda pemain C didalam kolom.



Row-wheel of player *R*



Column-wheel of player *C*

Untuk pemain R di letakan didalam baris dengan nomor 1, 2 Dan 3 sedangkan untuk kolom ditempatkan nomor 1,2,3, dan 4. Untuk memainkan game ini pemain R mempunyai 3 peluang untuk bergerak sedangkan pemain C mempunyai 4 peluang utnuk bergerak. Setiap Gerakan berdasarkan gerakan masing-masing, pemain C kemudian melakukan pembayaran uang ke pemain R sesuai dengan tabel dibawah ini.

		Player *C*'s Move			
		1	**2**	**3**	**4**
Player *R*'s Move	**1**	\$3	\$5	–\$2	–\$1
	2	–\$2	\$4	–\$3	–\$4
	3	\$6	–\$5	\$0	\$3

Misalnya, jika roda pemain R berhenti diangka 1 dan rodan pemain C berhenti di angka 2, maka pemain C harus membayar $5 kepada pemain R. beberapa entri didalam tabel tersebut ada yang benilai positif dan negative. Ini di maksudkan bahwa pemain R melakukan pembayaran positif kepada pemain C. karena berhenti pada bari 1 dan kolom 2. Misalnya lagi jika roda pemain R menunjukan angka 2 dan roda pemain C menunjukan angka 4, maka pemain R membayar pemain C dengan jumlah $ 4, karena nilai didalam entri adalah -$ 4. Jadi dengan cara ini nilai positif memberikan keuntungan bagi pemain R sedangkan nilai negative memberikan keuntungan bagi pemain C. Didalam game ini pemain tidak memiliki kendali atas gerakan yang ditentukan. Karena gerakan berdasarkan putaran yang disengaja.

4. Penerapan Aljabar Linier dalam Kriptografi

Kriptografi banyak digunakan untuk menjaga aspek keamanan informasi. Kemanan dalam bentuk kode rahasia ini bertujuan untuk mempertahankan privasi informasi yang ditransmisikan melalui jalur komunikasi public. Dalam Bahasa kriptografi, kode disebut ***cipher***, pesan yang tidak dikodekan disebut ***plaintext***, dan pesan yang diberi kode disebut ***chiphertext***. Proses konversi dari plaintext ke chiphertext disebut ***enchiphering***, dan proses proses kebalikannya dari konversi chiphertext ke plaintext disebut ***dechiperring***.(Corporation, 2008) Didalam penelitian (Amalia & Rosyani, 2018) menjelaskan tentang penggunaan kriptografi.

Dijelaskan adanya proses enkripsi XOR.

Diketahui *Plainteks* = “qspwqtttrvpA000.”. Dengan kunci = ‘ABCDE’.Panjang kunci XOR akan melakukan padding untuk mengenkripsi plain teks.

a. *Plainteks* = qspwqtttrvpA000.
b. Kunci *padding* = ABCDEABCDEABCDEA

Nilai karakter-karakter tersebut akan dikonversi kedalam kode biner kemudian dilakukan oprasi XOR pada tiap-tiap karakter antara plaintek terhadap kuncinya, sehingga didapat hasil sebagai berikut:

q	s	p	w	q	
0111 0001	0111 0011	0111 0000	0111 0111	0111 0001	
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	
0011 0000	0011 0001	0011 0011	0011 0011	0011 0100	
0	1	2	3	4	
t	t	t	r	v	
0111 0100	0111 0100	0111 0100	0111 1100	0111 1100	
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	
0011 0101	0011 0110	0011 0111	0011 1000	0011 1001	
5	6	7	8	9	
p	A	0	0	0	.
0000 0000	0000 0000	0000 0000	0000 0000	0000 0000	0000 0111
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	0100 0001
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	0100 0110
A	B	C	D	E	F

Dari hasil operas diatas didapat plainteks baru dari cipherteks yang dihasilkan dari operasi XOR yaitu: ‘0123456789ABCDEF’

Dalam scenario Enkripsi AES

Misalkan sebuah plainteks memiliki kunci seperti berikut:

Plaiteks : 0 1 2 3 4 5 6 7 8 9 A B C D E F

Dalam HEX : 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46

Kunci : A B C D E F G H I J K L M N O P

Dalam HEX : 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50

a. *AddRoundKey*

30	34	38	43	XOR	41	45	49	4D	=	71	71	71	0E
31	35	39	44		42	46	4A	4E		73	73	73	0A
32	36	41	45		43	47	4B	4F		71	71	0A	0A
33	37	42	46		44	48	4C	50		77	1F	0E	16

b. *SubBytes*

71	71	71	0E	=	A3	A3	A3	AB
73	73	73	0A	*SubByte*	8F	8F	8F	67
71	71	0A	0A		A3	A3	67	67
77	1F	0E	16		F5	C0	AB	47

c. *SiftRow*

A3	A3	A3	AB
8F	8F	8F	67
A3	A3	67	67
F5	C0	AB	47

A3	A3	A3	AB	
	8F	8F	8F	67
		A3	A3	67	67
F5	C0	AB	47	

A3	A3	A3	AB
8F	8F	67	8F
67	67	A3	A3
47	F5	C0	AB

d. *MixColoms*

A3	A3	A3	AB
8F	8F	67	8F
67	67	A3	A3
47	F5	C0	AB

02	03	01	01	X	A3	=	07	07	B5	67	96
01	02	03	01		8F		06	06	41	CC	2A
01	01	02	03		67		2B	2B	B1	91	69
03	01	01	02		47		FB	FB	E3	9A	A8

Ambil 4 *byte* terakhir , yaitu 4D 4E 4F 50 , lalu geser *byte* pertama menjadi *byte* terakhir. Hasilnya 4E 4F 50 5D. substitusikan dengan s-box, hasilnya adalah 2F 84 53 E3.

Selanjutnya XOR kan dengan konstatnta nilai tertentu dari pengguna.

2F XOR 01=0010 1111 XOR 0000 0001 = 0010 1110 = 2E

84 XOR 00=1000 0100 XOR 0000 0000 = 1000 0100 = 84

53 XOR 00= 0101 0011 XOR 0000 0000 = 0101 0011 = 53

E5 XOR 00=1110 0011 XOR 0000 0000 = 1110 0011 = E5

Langkah terakhir XOR-kan 2E 84 53 E5 dengan 4 *byte* pertama kunci awal yaitu 41 42 43 44.

2E XOR 41= 0010 1110 XOR 0100 0001 = 0110 1111 = 6F

84 XOR 2 = 1000 0100 XOR 0100 0010 = 1100 0110 = C6

53 XOR 43= 0101 0011 XOR 0100 0011 = 0001 0000 = 10

E5 XOR 44= 1110 0011 XOR 0100 0100 = 1010 0111 = A7

Hasil proses XOR diatas adalah 6F C6 10 A7 yang merupakan 4 *byte* pertama dari kunci yang baru untuk *byte*. Untuk 4 *byte* ke 2, kita tinggal melakukan operasi xor antara 4 *byte* operasi XOR antara 4 *byte* kunci selanjutnya dengan 6F C6 10 A7.

Demikian seterusnya hingga didapatkan 16 *byte* set kunci yang baru. Ekspansi keseluruhan dapat dilihat padac tabel-tabel dibawah ini

Round 1

6F	2A	63	2E
C6	80	CA	8B
10	57	1C	53
A7	EF	A3	F3

Round 2

50	7A	19	37
2B	AB	61	EA
1D	4A	56	5
96	79	DA	29

Round3

D3	49	80	87
40	EB	8A	60
B8	F2	A4	A1
0C	75	AF	86

Round 4

0B	A2	12	95
72	99	13	73
FC	0E	AA	0B
1B	6E	C1	47

Round 5

94	36	24	b1
59	C0	D3	F3
5C	52	F8	F3
31	5F	9E	D9

Round 6

54	62	46	F7
44	84	57	F7
69	3B	C3	30
F9	A6	38	E1

Round 7

7C	1E	58	AF
40	C4	93	64
91	AA	69	59
91	32	0F	EE

Round 8

BF	A1	F9	56
8B	4F	DC	B8
B9	13	7A	23
E8	DF	D0	3E

Round 9

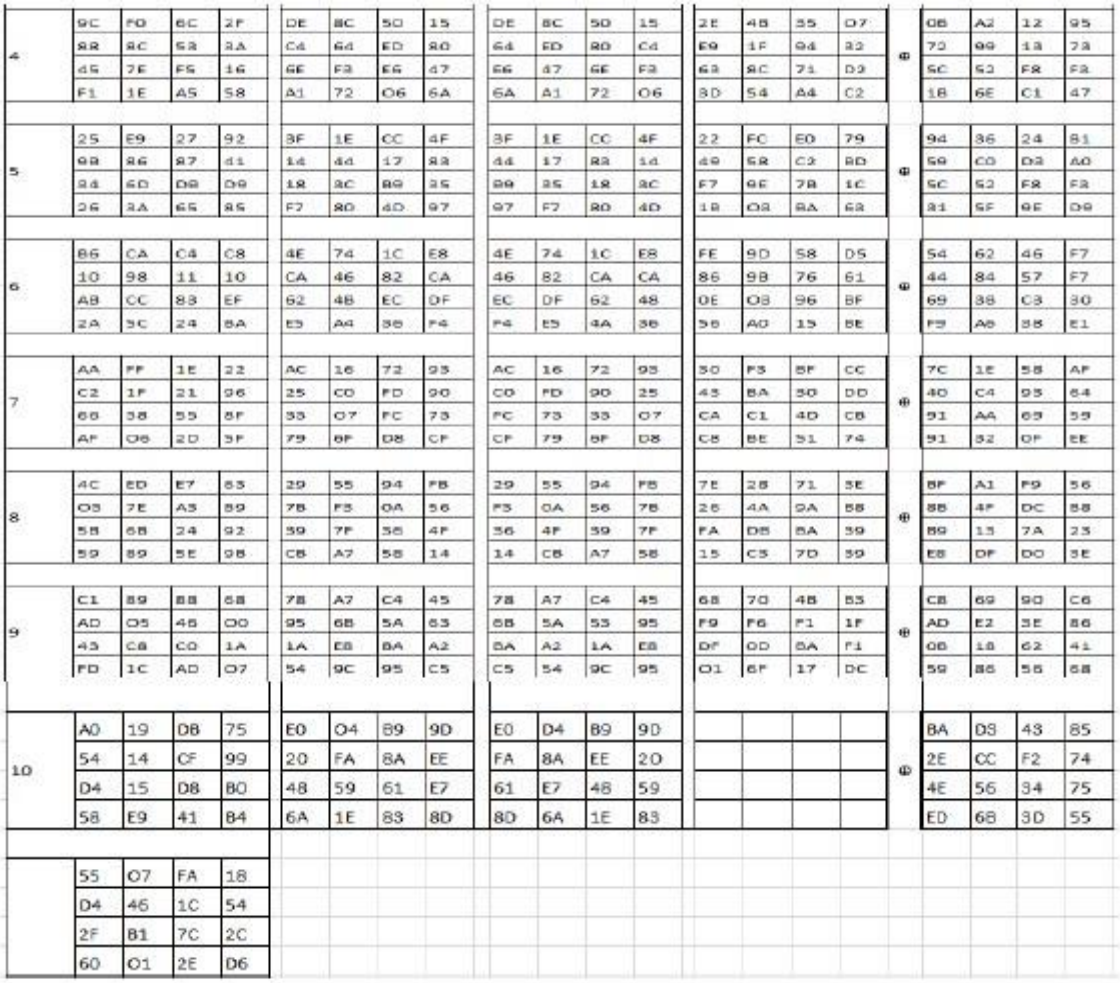
C8	69	90	C6
AD	E2	3E	86
0B	18	62	41
59	86	56	68

Round 10

BA	D3	43	85
2E	CC	F2	74
4E	56	34	75
ED	6B	3D	55

Tabel 1. Tabel ekspand Chipstext

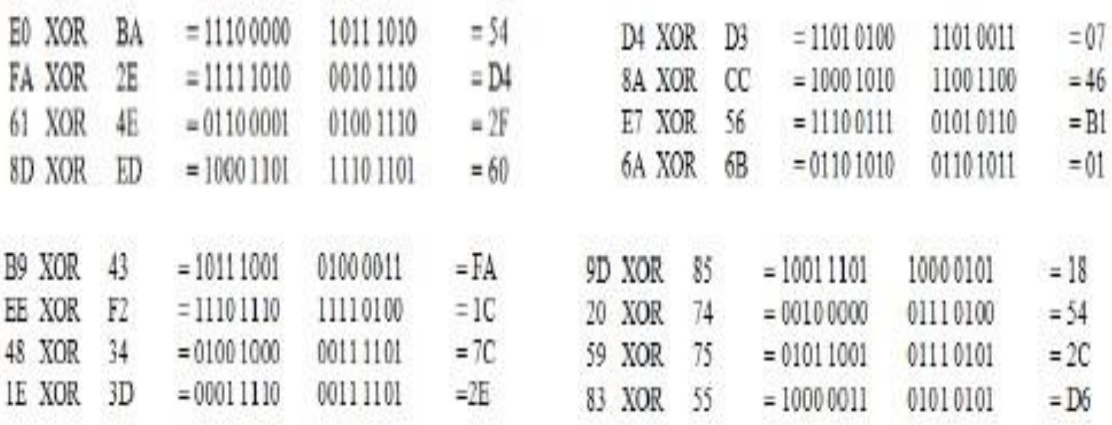
Round	Mulai				Setelah SubByte				Setelah Shift Row				Setelah MixColomns					Nilai Roundkey			
0	30	34	38	43													⊕	41	45	49	4D
	31	03	39	44														42	46	4A	4E
	32	36	41	45														43	47	4B	4F
	33	37	42	46														44	48	4C	50
1	71	71	71	0E	A3	A3	A3	A8	A3	A3	A3	A8	07	85	67	96	⊕	6F	2A	63	2E
	73	73	73	0A	8F	8F	8F	67	8F	8F	67	8F	06	41	CC	2A		C6	80	CA	8B
	71	71	0A	0A	A3	A3	67	67	67	67	A3	A3	28	81	91	69		10	57	1C	53
	77	1F	0E	16	F5	C0	AB	47	47	F5	C0	AB	FB	E5	9A	AB		A7	EF	A3	F3
2	68	9F	04	B8	45	DB	F2	6C	45	DB	F2	6C	C1	98	26	ED		50	7A	19	37
	C0	C1	06	A1	BA	78	6F	32	78	6F	32	BA	E4	7C	0C	EE		2B	AB	61	EA
	3B	E6	8D	3A	E2	8E	5D	80	5D	80	E2	8E	28	0F	8F	08		1D	4A	56	05
	5C	0C	39	58	4A	FE	12	39	39	4A	FE	12	60	3F	6A	A4		96	79	DA	29
3	91	E1	3F	DA	81	F8	75	57	81	F8	75	57	4F	59	DC	A8	⊕	D3	49	80	87
	CF	D7	6D	04	8A	0E	3C	F2	0E	3C	F2	8A	C8	67	D9	5A		E8	EB	8A	60
	35	45	09	0D	96	6E	35	D7	35	D7	96	6E	FD	8C	51	87		B8	F2	A4	A1
	F6	46	80	8D	42	5A	E7	5D	5D	42	5A	E7	FD	6B	0A	DE		0C	75	AF	86



Output ari keseluruhan *Round* adalah:

54 D4 2F 60 07 46 B1 01 FA 1C 7C 2E 18 54 2C D6

Dari proses:



C. Contoh Soal/Tugas

1. Menurut anda adakah implementasi aljabar linear didalam kehidupan sehari-hari!? Jelaskan dan sebutkan!

2. Buatlah contoh implementasi aljabar dalam kehidupan sehari – hari menggunakan matlab?

3. Buatlah laha satu contoh kasus dalam konversi warna RGB ke matriks?

4. Bisa anda jelaskan cara mengkonversi matriks warna RGB ke matrik warna HSV?

5. Silakan konversi plaintext dibawah ini menjadi chippertext
   Plain A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   Cipher D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
   Dari kata UNIVERSITAS PAMULANG?

D. Daftar Pustaka

Amalia, R., & Rosyani, P. (2018). "Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android". *Faktor Exacta*, *11*(4), 370. https://doi.org/10.30998/faktorexacta.v11i4.2878

Atmadja, J., Bandung, I. T., & Bandung, J. G. (2016). Penerapan Aljabar Lanjar pada Grafis Komputer, 1–9.

Corporation, B. (2008). *Additional applications*. *International Series in Operations Research and Management Science* (Vol. 123). https://doi.org/10.1007/978-0-387-09421-2_10

Rosyani, P., Taufik, M., Waskita, A. A., & Apriyanti, D. H. (2019). "Comparison of color model for flower recognition". *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, 10–14. https://doi.org/10.1109/icitisee.2018.8721026

Rosyani, Perani. (2017). "Pengenalan Wajah Menggunakan Metode Principal Component Analysis (PCA) dan Canberra Distance". *Jurnal Informatika Universitas Pamulang*, *2*(2), 118. https://doi.org/10.32493/informatika.v2i2.1515