

LAMPIRAN

1. Enkripsi Pesan

String Representations																												
Plaintext:	68616C6F0C0C0C0C0C0C0C0C0C0C0C0C																											
Key:	656C6C797468696E3132333435363738																											
Ciphertext:	D3BE1EB240232DBB49E3D24B20D4FA60																											
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant							
Round 0													0D	78	3D	39	65	74	31	35								
													0D	64	3E	3A	6C	68	32	36								
													00	65	3F	3B	6C	69	33	37								
													16	62	38	34	79	6E	34	38								
Round 1	D7	BC	27	12	D7	BC	27	12	1D	0B	1C	0C	7C	1E	38	1D	61	15	24	11	01							
	D7	43	B2	80	43	B2	80	D7	D6	B9	33	77	20	27	9F	ED	F6	9E	AC	9A								
	63	4D	75	E2	75	E2	63	4D	56	18	84	56	3D	1A	B5	50	6B	02	31	06								
	47	AA	07	18	18	47	AA	07	64	01	C5	A2	8B	80	70	2F	EF	81	B5	8D								
Round 2	10	72	07	A4	10	72	07	A4	AF	FC	1B	62	74	32	F1	99	DB	CE	EA	FB	02							
	B7	CC	DB	55	CC	DB	55	B7	E2	17	09	7D	7B	10	A2	4C	99	07	AB	31								
	27	A2	D5	53	D5	53	27	A2	52	48	50	BF	64	7C	55	BC	36	34	05	03								
	3D	CD	51	15	15	3D	CD	51	03	64	FA	40	6E	88	A3	94	6D	EC	59	D4								
Round 3	92	23	A1	EE	92	23	A1	EE	A4	F2	A5	BE	BC	24	99	79	18	D6	3C	C7	04							
	21	CA	3A	29	CA	3A	29	21	20	67	F2	96	C2	82	BC	E9	E2	E5	4E	7F								
	43	10	FC	65	FC	65	43	10	DD	69	59	F1	A3	23	16	BD	7E	4A	4F	4C								
	9F	C4	0A	22	22	9F	C4	0A	DF	1F	01	0C	BD	91	D6	0F	62	8E	D7	03								
Round 4	65	36	EE	B6	65	36	EE	B6	CE	C3	6E	C8	0C	D7	46	27	C2	14	28	EF	08							
	25	13	65	1E	13	65	1E	25	FC	08	4D	60	37	26	2D	7F	CB	2E	60	1F								
	0A	26	47	7A	47	7A	0A	26	62	29	7C	DE	67	66	7C	92	05	4F	00	4C								
	7A	81	F6	76	76	7A	81	F6	17	B1	24	35	B3	9B	D9	CB	A4	2A	FD	FE								
Round 5	FE	0E	5A	CC	FE	0E	5A	CC	EA	4D	48	30	F8	4B	66	F1	12	06	2E	C1	10							
	9A	F7	D8	D2	F7	D8	D2	9A	24	19	65	83	C6	D5	C9	30	E2	CC	AC	B3								
	85	33	10	4F	10	4F	85	33	08	FF	A5	6F	B6	0E	54	D2	BE	F1	F1	BD								
	6D	14	35	1F	1F	6D	14	35	C0	5F	91	8C	BB	0E	3D	DE	7B	51	AC	52								
Round 6	41	B3	33	A1	41	B3	33	A1	BA	5E	8F	12	E5	07	F8	A4	5F	59	77	B6	20							
	B4	03	DD	04	03	DD	04	B4	3A	3C	42	13	A2	68	BA	58	98	54	F8	4B								
	4E	AB	20	B5	20	B5	4E	AB	25	3A	4D	31	9B	75	F3	32	BE	4F	BE	03								
	EA	AB	27	1D	1D	EA	AB	27	DA	69	52	A9	D9	3B	AC	05	03	52	FE	AC								
Round 7	D9	C5	41	49	D9	C5	41	49	00	80	CA	D0	AC	75	48	E4	AC	F5	82	34	40							
	3A	45	F4	6A	45	F4	6A	3A	2F	66	4B	10	CC	D1	04	14	E3	B7	4F	04								
	14	9D	0D	23	0D	23	14	9D	3B	28	3E	FA	14	48	E0	27	2F	60	DE	DD								
	35	E2	91	6B	6B	35	E2	91	EE	E9	62	45	A3	F6	83	08	4D	1F	E1	4D								
Round 8	91	9D	52	69	91	9D	52	69	AA	EA	09	B1	74	C1	A0	2C	DE	2B	A9	9D	80							
	4B	3E	F2	FA	3E	F2	FA	4B	E5	27	EA	E5	C7	B2	30	3B	22	95	DA	DE								
	FA	52	E1	CC	E1	CC	FA	52	26	F2	81	A9	EA	5E	F3	06	CC	AC	72	AF								
	0A	42	EC	30	30	0A	42	EC	17	96	72	61	42	DC	D9	87	55	4A	AB	E6								
Round 9	92	78	E0	71	92	78	E0	71	7C	BF	E7	DE	A4	4C	BD	19	D8	F3	5A	C7	1B							
	C6	37	04	E2	37	04	E2	C6	FC	ED	2B	3B	A7	23	3F	F1	5B	CE	14	CA								
	87	58	0D	6F	0D	6F	87	58	86	D6	86	58	C4	38	1A	6B	42	EE	9C	33								
	2C	86	35	17	17	2C	86	35	B9	BB	49	67	B2	FA	A3	6B	0B	41	EA	0C								
Round 10	49	29	7A	D4	49	29	7A	D4					D3	40	49	20	9A	69	33	F4	36							
	5C	26	75	A1	26	75	A1	5C					BE	23	E3	D4	98	56	42	88								
	1C	07	A2	7F	A2	7F	1C	07					1E	2D	D2	FA	BC	52	CE	FD								
	37	2D	0A	7F	7F	37	2D	0A					B2	BB	4B	60	CD	8C	66	6A								
	SubBytes	ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant										

2. Dekripsi Pesan

String Representations	
Ciphertext:	D3BE1EB240232DBB49E3D24B20D4FA60
Key:	656C6C797468696E3132333435363738
Plaintext:	68616C6F0C0C0C0C0C0C0C0C0C0C0C

	SubBytes	ShiftRows	MixColumns	AddRoundKey	Key Schedule	Round Constant
Round 0				68 0C 0C 0C 61 0C 0C 0C 6C 0C 0C 0C 6F 0C 0C 0C	65 74 31 35 6C 68 32 36 6C 69 33 37 79 6E 34 38	
Round 1	0D 78 3D 39 0D 64 3E 3A 00 65 3F 3B 16 62 38 34	D7 BC 27 12 D7 BC 27 12 63 4D 75 E2 47 AA 07 18	D7 BC 27 12 43 B2 80 D7 75 E2 63 4D 18 47 AA 07	1D 0B 1C 0C D6 B9 33 77 56 18 84 56 64 01 C5 A2	61 15 24 11 F6 9E AC 9A 6B 02 31 06 EF 81 B5 8D	01
Round 2	7C 1E 38 1D 20 27 9F ED 3D 1A B5 50 8B 80 70 2F	10 72 07 A4 B7 CC DB 55 27 A2 D5 53 3D CD 51 15	10 72 07 A4 CC DB 55 B7 D5 53 27 A2 15 3D CD 51	AF FC 1B 62 E2 17 09 7D 52 48 50 BF 03 64 FA 40	DB CE EA FB 99 07 AB 31 36 34 05 03 6D EC 59 D4	02
Round 3	74 32 F1 99 7B 10 A2 4C 64 7C 55 BC 6E 88 A3 94	92 23 A1 EE 21 CA 3A 29 43 10 FC 65 9F C4 0A 22	92 23 A1 EE CA 3A 29 21 FC 65 43 10 22 9F C4 0A	A4 F2 A5 BE 20 67 F2 96 DD 69 59 F1 DF 1F 01 0C	18 D6 3C C7 E2 E5 4E 7F 7E 4A 4F 4C 62 8E D7 03	04
Round 4	BC 24 99 79 C2 82 BC E9 A3 23 16 BD BD 91 D6 0F	65 36 EE B6 25 13 65 1E 0A 26 47 7A 7A 81 F6 76	65 36 EE B6 13 65 1E 25 47 7A 0A 26 7A 81 F6 76	CE C3 6E C8 FC 08 4D 60 62 29 7C DE 17 B1 24 35	C2 14 28 EF CB 2E 60 1F 05 4F 00 4C A4 2A FD FE	08
Round 5	0C D7 46 27 37 27 2D 7F 67 66 7C 92 B3 9B D9 CB	FE 0E 5A CC 9A F7 D8 D2 85 33 10 4F 6D 14 35 1F	FE 0E 5A CC F7 D8 D2 9A 10 4F 85 33 1F 6D 14 35	EA 4D 48 30 24 19 65 83 08 FF A5 6F C0 5F 91 8C	12 06 2E C1 E2 CC AC B3 BE F1 F1 BD 7B 51 AC 52	10
Round 6	F8 4B 66 F1 C6 D5 C9 30 B6 0E 54 D2 BB 0E 3D DE	41 B3 33 A1 B4 03 DD 04 4E AB 20 B5 EA AB 27 1D	41 B3 33 A1 03 DD 04 B4 20 B5 4E AB 1D EA AB 27	BA 5E 8F 12 3A 3C 42 13 25 3A 4D 31 DA 69 52 A9	5F 59 77 B6 98 54 F8 4B BE 4F BE 03 03 52 FE AC	20
Round 7	E5 07 F8 A4 A2 68 BA 58 9B 75 F3 32 D9 3B AC 05	D9 C5 41 49 3A 45 F4 6A 14 9D 0D 23 E2 91 6B 6B	D9 C5 41 49 45 F4 6A 3A 0D 23 14 9D 6B 6B 35 E2	00 80 CA D0 2F 66 4B 10 3B 28 3E FA EE E9 62 45	AC F5 82 34 E3 B7 4F 04 2F 60 DE DD 4D 1F E1 4D	40
Round 8	AC 75 48 E4 CC D1 04 14 14 48 E0 27 A3 F6 83 08	91 9D 52 69 4B 3E F2 FA FA 52 E1 CC 0A 42 EC 30	91 9D 52 69 3E F2 FA 4B E1 CC FA 52 30 0A 42 EC	AA EA 09 B1 E5 27 EA E5 26 F2 81 A9 17 96 72 61	DE 2B A9 9D 22 95 DA DE CC AC 72 AF 55 4A AB E6	80
Round 9	74 C1 A0 2C C7 B2 30 3B EA 5E F3 06 42 DC D9 87	92 78 E0 71 C6 37 04 E2 87 58 0D 6F 2C 86 35 17	92 78 E0 71 37 04 E2 C6 0D 6F 87 58 2C 86 35 17	7C BF E7 DE FC ED 2B 3B 86 D6 86 58 B9 BB 49 67	D8 F3 5A C7 5B CE 14 CA 42 EE 9C 33 0B 41 EA 0C	1B
Round 10	A4 4C BD 19 A7 23 3F F1 C4 38 1A 6B B2 FA A3 6B	49 29 7A D4 5C 26 75 A1 1C 07 A2 7F 2D 0A 7F	49 29 7A D4 5C 26 75 A1 1C 07 A2 7F 2D 0A 7F	49 29 7A D4 26 75 A1 5C A2 7F 1C 07 7F 37 2D 0A	9A 69 33 F4 98 56 42 88 BC 52 CE FD CD 8C 66 6A	36

3. Ekspansi Kunci

	Key Schedule								
Round 0	65	74	31	35					
	6C	68	32	36					
	6C	69	33	37					
	79	6E	34	38					
Round 1	61	15	24	11	Round 6	5F	59	77	B6
	F6	9E	AC	9A		98	54	F8	4B
	6B	02	31	06		BE	4F	BE	03
	EF	81	B5	8D		03	52	FE	AC
Round 2	DB	CE	EA	FB	Round 7	AC	F5	82	34
	99	07	AB	31		E3	B7	4F	04
	36	34	05	03		2F	60	DE	DD
	6D	EC	59	D4		4D	1F	E1	4D
Round 3	18	D6	3C	C7	Round 8	DE	2B	A9	9D
	E2	E5	4E	7F		22	95	DA	DE
	7E	4A	4F	4C		CC	AC	72	AF
	62	8E	D7	03		55	4A	AB	E6
Round 4	C2	14	28	EF	Round 9	D8	F3	5A	C7
	CB	2E	60	1F		5B	CE	14	CA
	05	4F	00	4C		42	EE	9C	33
	A4	2A	FD	FE		0B	41	EA	0C
Round 5	12	06	2E	C1	Round 10	9A	69	33	F4
	E2	CC	AC	B3		98	56	42	88
	BE	F1	F1	BD		BC	52	CE	FD
	7B	51	AC	52		CD	8C	66	6A



Sekolah Tinggi Manajemen Informatika & Komputer
(STMIK) Atma Luhur
KARTU BIMBINGAN SKRIPSI

NIM : 1511500169
 Nama : Eli Patima
 Jurusan : Teknik Informatika
 No. Handphone : 0821 7880 7628
 Semester : VIII Tahun Akademik 2019 / 2019..
 Dosen Pembimbing : Laurentinus, M. Kom.
 Judul Skripsi : Penerapan Kriptografi Algoritma AES
 (Advanced Encryption Standard) Serta Kompresi
 Algoritma Huffman Pada Aplikasi Message



No	Tanggal	Uraian	Paraf Pembimbing
1	14/mar 2018	Bimbingan Judul	<i>Handwritten signature</i>
2	20/mar 2018	Bimbingan Proposal	<i>Handwritten signature</i>
3	9/apr 2018	Bimbingan Bab II	<i>Handwritten signature</i>
4	11/apr 2018	Revisi Bab II, bimbingan Bab III dan Bab IV	<i>Handwritten signature</i>
5	25/apr 2018	Revisi Bab III dan Bab IV	<i>Handwritten signature</i>
6	4/may 2018	Acc Bab II dan III, revisi Bab IV	<i>Handwritten signature</i>
7	15/may 2018	Bimbingan Program	<i>Handwritten signature</i>
8	23/may 2018	Bimbingan Program	<i>Handwritten signature</i>
9	28/may 2018	Bimbingan Program	<i>Handwritten signature</i>
10	30/5 - 5/6 2018	Bimbingan Program	<i>Handwritten signature</i>
11	6/juli 2018	Revisi Bab IV	<i>Handwritten signature</i>
12	9, 10/juli 2018	Revisi Bab IV	<i>Handwritten signature</i>
13	23/juli 2018	Bimbingan Keseluruhan laporan	<i>Handwritten signature</i>
14	27/juli 2018	Acc keseluruhan laporan	<i>Handwritten signature</i>

Mahasiswa diatas telah melakukan bimbingan dengan jumlah materi yang telah mencukupi untuk disidangkan.

Pangkalpinang, 27 Juli 2018

Mahasiswa

Dosen Pembimbing

(Eli Patima)

(Laurentinus)

BIODATA PENULIS SKRIPSI



Pendadaran / Lulus Tanggal : 10 Agustus 2018

Wisuda Tanggal :

NIM : 1511500167
Nama : Eli Patima
Jenis Kelamin : ~~Laki-laki~~ / Perempuan
Tempat & Tanggal Lahir : Palembang, 26 September 1996
Status : ~~Nikah~~ / Belum Nikah
Agama : Kristen
Program Studi : Teknik Informatika
Pekerjaan Saat Ini : Mahasiswi
Alamat Rumah Asal : Kp. Menjelang Baru No : 98, Muntok, Bangka Barat, Prov. Kep. Bangka Belitung
No. Telpon / HP : 082178807628
Nama Ayah : Tjhin Hon Khun
Nama Ibu : Djie Siu Lan
Pekerjaan Ayah : Buruh Harian
Pekerjaan Ibu : Ibu Rumah Tangga
Alamat Orang Tua : Kp. Menjelang Baru No : 98, Muntok, Bangka Barat, Prov. Kep. Bangka Belitung
Judul Skripsi : Penerapan Kriptografi Algoritma AES (*Advanced Encryption Standard*) Serta Kompresi Algoritma *Huffman* Pada Aplikasi *Message*.
Dosen Pembimbing : Laurentinus, M.Kom

Pangkalpinang, 10 Agustus 2017

Penulis

(ELI PATIMA)