DAFTAR PUSTAKA

A, M. A., & Suprianto, A. (2018). Penggunaan Algorithma AES-RIJNDAEL Pada Sistem Enkripsi Dan Dekripsi Untuk Komunikasi Data. *Sainstech: Jurnal Penelitian dan Pengkajian Sains dan Teknologi*, *25*(2), 31–39. https://doi.org/10.37277/stch.v25i2.94

Aedy. (2016). *Fitur dan Arsitektur Software Sistem Operasi Android*. BacaMedi.com. https://www.bacamedi.com/fitur-dan-arsitektur-software-sistem-operasi-android/

Basri. (2016). Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*, *2*(2), 17–23. http://ejournal.fikom-unasman.ac.id

Dian Widyawan, I. (2021). *Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite*. *4*(1), 15–22.

Fitriansyah, F., Safrianti, E., Teknik, M., Universitas, E., Jurusan, D., Elektro, T., Riau, U., & Jaringan, L. (2019). *Aplikasi Android Untuk Pengaman Teks Menggunakan Kriptografi Berlapis Dengan Algoritma Caesar , Blowfish*. *6*(1), 1–8.

H. Kridalaksana, A., Arriyanti, E., & Widodo, W. (2018). Aplikasi Pengaman Sms Dengan Metode Kriptografi Advanced Encryption Standard (Aes) 128 Berbasis Android. *Sebatik*, *10*(1), 8–14. https://doi.org/10.46984/sebatik.v10i1.59

Harahap, J. L. (2013). Mobile Searching Aplikasi Panduan Belanja Pada Factory Outlet Black And White. *Jurnal Ilmiah Komputer Informatika (KOMPUTA)*, 1–7.

J, S. (2006). Implementasi Kriptografi untuk Keamanan Data dengan menggunakan metode Andvanced Encryption Standart (AES) 128.

Universitas Komputer Indonesia.

Juansyah, A. (2015). Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-GPS) Dengan Platform Android. *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, *1*(1), 1–8. elib.unikom.ac.id/download.php?id=300375

Kharisma, R. S., Aziz, M., & Rachman, F. (2017). *Pembuatan Aplikasi Notes Menggunakan Substitution Cipher Kombinasi Kode Ascii Dan Operasi Xor Berbasis Android*. *XII*, 1–7.

Liksha, P. D. (2018). *APLIKASI AKUNTANSI PENGOLAHAN DATA JASA SERVICE*. *1*(1), 1–14.

Lubis, J. H. (2018). Implementasi Keamanan Data Dengan Metode Kriptografi XOR. *Jurnal Sistem Informasi Kaputama (JSIK)*, *2*(2), 1–4.

Miansyah, V., & Laipaka, R. (2017). Perancangan Aplikasi Kriptografi Simetris Menggunakan Algoritma Hill Cipher dan Advanced Encryption Standard. *Jurnal TISI*, *1*, 63–77. http://www.sisfotenika.stmikpontianak.ac.id/index.php/TISI/article/view/922

Nasution, Y. R., & Furqan, M. (2020). Aplikasi Mobile Media Pembelajaran Dasar Algoritma dan Pemrograman Berbasis Android. *Syntax : Journal of Software Engineering, Computer Science and Information Technology*, *1*(1), 45–51. https://doi.org/10.46576/syntax.v1i1.791

Nuari, R., & Ratama, N. (2020). Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping. *JOAIIA: Journal of Artificial …*, *1*(2), 37–44. http://openjournal.unpam.ac.id/index.php/JOAIIA/article/view/5146

Riyowati, B., & Fadlilah, N. I. (2019). Rancang Bangun Aplikasi Ensiklopedia Batik Indonesia Berbasis Android. *EVOLUSI - Jurnal Sains dan Manajemen*, *7*(1), 341–348. https://doi.org/10.31294/evolusi.v7i1.5584

Santoso, S., Sutrisno, & Hardiyanto, G. (2017). *Implementasi Kriptografi Algoritma AES Serta Algoritma Kompresi Huffman Dengan Menggunakan Pemograman PHP*. *2*(1), 225–230.

Sibarani, N. S., Munawar, G., & Wisnuadhi, B. (2018). Analisis Performa Aplikasi Android Pada Bahasa Pemrograman Java dan Analisis Performa Aplikasi Android Pada Bahasa Pemrograman Java dan Kotlin. *9th Industrial Research Workshop and Natiomal Seminar (IRONS), Juli*, 319–324.

Simarmata, J. (2019). *KRIPTOGRAFI* (M. Kika (ed.); 1 ed.).

Winarno, A., Tulus, E., Cahyanto, B., Tinggi, S., & Negara, S. (2012). *T-4 POLYNOMIAL FUNCTIONS DAN IMPLEMENTASINYA DALAM ALGORITMA ADVANCED ENCRYPTION STANDARD PADA*. *November*, 978–979.

Yuniati, V., Indriyanta, G., & Rachmat C., A. (2011). Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File. *Jurnal Informatika*, *5*(1). https://doi.org/10.21460/inf.2009.51.69

Zufria, I., & Indonesia, M. (2016). *SISTEM PENGAMAN DATA MENGGUNAKAN ALGORITMA ENKRIPSI AES (ADVANCE ENCRYPTION STANDARD). November 2015*.

Zunaidi, M., & Suharsil, S. (2018). Pengamanan Citra Digital Menggunakan Kombinasi Antara Algoritma AES Dan Metode LSB. *J-SISKO TECH (Jurnal Teknologi …*, *1*(2), 36–50. https://ojs.trigunadharma.ac.id/index.php/jsk/article/view/29

LAMPIRAN

1. Listing Program AES (*Advanced Encryption Standard*) Rijndael

```
package com.example.newmynotesapp;
import android.util.Log;
import java.io.UnsupportedEncodingException;
import java.security.GeneralSecurityException;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
public class AESCryptt {
   private static final String TAG = "AESCrypt";
   private static final String AES_MODE = "AES"; //equals
"AES/ECB/PKCS5Padding"
   private static final String CHARSET = "UTF-8";
   public static String encrypt(final String password, String message)
         throws GeneralSecurityException {
      try {
         Log.e("message", message);
         Log.e("password", password);
         final SecretKeySpec key = new
SecretKeySpec(password.getBytes(CHARSET), "AES");
         byte[] cipherText = encrypt(key, message.getBytes(CHARSET));
         String encoded = bytesToHex(cipherText);
         Log.e("Encrypt pertama", "byte to hex : " + encoded);
         return encoded;
      } catch (UnsupportedEncodingException e) {
         Log.e(TAG, "UnsupportedEncodingException ", e);
         throw new GeneralSecurityException(e);
      }
   }
```

```
    public static byte[] encrypt(final SecretKeySpec key, final
byte[]message)
            throws GeneralSecurityException {
        final Cipher cipher = Cipher.getInstance(AES_MODE);
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] cipherText = cipher.doFinal(message);
        //log("cipherText", cipherText);
        Log.e("Encrypt kedua", "Chiper Text : " + cipherText);
        return cipherText;
    }
    public static String decrypt(final String password, String textBiasa)
            throws GeneralSecurityException {
        try {
            final SecretKeySpec key = new
SecretKeySpec(password.getBytes(CHARSET), "AES");
            Log.e("textBiasa", textBiasa);
            //change string to byte[]
            byte[] textByte = hexToBytes(textBiasa);
            //byte[] decryptedBytes = decrypt(key, ivBytes, textByte);
            byte[] decryptedBytes = decrypt(key, textByte);
            Log.e("decryptedBytes", "" + decryptedBytes);
            String message = new String(decryptedBytes, CHARSET);
            Log.e("message", message);
            return message;
        } catch (UnsupportedEncodingException e) {
            Log.e(TAG, "UnsupportedEncodingException ", e);
            throw new GeneralSecurityException(e);
        }
    }
    public static byte[] decrypt(final SecretKeySpec key, final byte[]
decodedCipherText)
```

```
            throws GeneralSecurityException {
        final Cipher cipher = Cipher.getInstance(AES_MODE);
        cipher.init(Cipher.DECRYPT_MODE, key);
        byte[] decryptedBytes = cipher.doFinal(decodedCipherText);
        Log.e("decryptedBytes", "" + decryptedBytes);
        return decryptedBytes;
    }
    private static String bytesToHex(byte[] bytes) {
        final char[] hexArray = {'0', '1', '2', '3', '4', '5', '6', '7', '8',
                '9', 'A', 'B', 'C', 'D', 'E', 'F'};
        char[] hexChars = new char[bytes.length * 2];
        int v;
        for (int j = 0; j < bytes.length; j++) {
            v = bytes[j] & 0xFF;
            hexChars[j * 2] = hexArray[v >>> 4];
            hexChars[j * 2 + 1] = hexArray[v & 0x0F];
        }
        return new String(hexChars);
    }
    public static byte[] hexToBytes(String s) {
        int len = s.length();
        byte[] data = new byte[len / 2];
        for (int i = 0; i < len; i += 2) {
            data[i / 2] = (byte) ((Character.digit(s.charAt(i), 16) << 4)
                    + Character.digit(s.charAt(i + 1), 16));
        }
        return data;
    }
    private AESCryptt() {
    }
}
```

2. Tabel Pengujian black-box

Tabel Pengujian black-box pada Implementasi Algoritma Kriptografi AES *(Advanced Encrytion Standard)* Rijndael Dalam Keamanan Teks Catatan Berbasis Android

No.	Skenario Pengujian	Hasil yang diharapkan	Kesimpulan
1.	Panjang kunci hanya bisa di input dengan 128 bit,192 bit, dan 256 bit	Dapat menentukan panjang kunci sesuai dengan tipe AES yaitu 128 bit,192 bit, dan 256 bit	Berhasil [✓]
			Gagal [ ]
2.	Perhitungan manual dengan aplikasi memiliki output yang sama pada saat di enkripsi dan di dekripsi.	Hasil output dari perhitungan dengan aplikasi yaitu sama. Hanya saja di aplikasi lebih panjang dikarenakan menggunakan PKCS5 *Padding*	Berhasil [✓]
			Gagal [ ]
3.	Aplikasi yang dibangun seperti pada umumnya dapat di edit,di hapus,dan di tambah	Aplikasi berjalan seperti pada umumnya hanya dapat di edit, di hapus dan di tambah	Berhasil [✓]
			Gagal [ ]
4.	Teks yang di input tidak terbatas dan ouputnya berupa 128 bit, 192 bit, dan 256 bit	Menggunakan PKCS5 *padding* agar jumlah teks yang ingin di enkripsi tidak terbatas	Berhasil [✓]
			Gagal [ ]

Medan, 09 Februari 2022

Dr. M. Fakhriza, ST, M.Kom
NIB. 1100000115

3. Kode ASCII

DEC	OCT	HEX	BIN	CHAR
1	1	1	00000001	
2	2	2	00000010	┐
3	3	3	00000011	└
4	4	4	00000100	┘
5	5	5	00000101	│
6	6	6	00000110	─
7	7	7	00000111	•
8	10	8	00001000	◘
9	11	9	00001001	
10	12	A	00001010	
11	13	B	00001011	♂
12	14	C	00001100	♀
13	15	D	00001101	
14	16	E	00001110	♫
15	17	F	00001111	☼
16	20	10	00010000	┼
17	21	11	00010001	◄
18	22	12	00010010	↕
19	23	13	00010011	‼
20	24	14	00010100	¶
21	25	15	00010101	┴
22	26	16	00010110	┬
23	27	17	00010111	┤
24	30	18	00011000	↑
25	31	19	00011001	├
26	32	1A	00011010	→
27	33	1B	00011011	←
28	34	1C	00011100	
29	35	1D	00011101	
30	36	1E	00011110	
31	37	1F	00011111	
32	40	20	00100000	
33	41	21	00100001	!
34	42	22	00100010	"
35	43	23	00100011	#
36	44	24	00100100	$
37	45	25	00100101	%
38	46	26	00100110	&
39	47	27	00100111	'
40	50	28	00101000	(
41	51	29	00101001	)
42	52	2A	00101010	*
43	53	2B	00101011	+
44	54	2C	00101100	,
45	55	2D	00101101	-
46	56	2E	00101110	.
47	57	2F	00101111	/
48	60	30	00110000	0
49	61	31	00110001	1
50	62	32	00110010	2
51	63	33	00110011	3
52	64	34	00110100	4
53	65	35	00110101	5
54	66	36	00110110	6
55	67	37	00110111	7
56	70	38	00111000	8
57	71	39	00111001	9
58	72	3A	00111010	:
59	73	3B	00111011	;
60	74	3C	00111100	<
61	75	3D	00111101	=
62	76	3E	00111110	>
63	77	3F	00111111	?
64	100	40	01000000	@
65	101	41	01000001	A
66	102	42	01000010	B
67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T
85	125	55	01010101	U
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\
93	135	5D	01011101	]
94	136	5E	01011110	^
95	137	5F	01011111	_
96	140	60	01100000	`
97	141	61	01100001	a
98	142	62	01100010	b
99	143	63	01100011	c
100	144	64	01100100	d
101	145	65	01100101	e
102	146	66	01100110	f
103	147	67	01100111	g
104	150	68	01101000	h
105	151	69	01101001	i
106	152	6A	01101010	j
107	153	6B	01101011	k
108	154	6C	01101100	l
109	155	6D	01101101	m
110	156	6E	01101110	n
111	157	6F	01101111	o
112	160	70	01110000	p
113	161	71	01110001	q
114	162	72	01110010	r
115	163	73	01110011	s
116	164	74	01110100	t
117	165	75	01110101	u
118	166	76	01110110	v
119	167	77	01110111	w
120	170	78	01111000	x
121	171	79	01111001	y
122	172	7A	01111010	z
123	173	7B	01111011	{
124	174	7C	01111100	|
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	⌂
128	200	80	10000000	€
129	201	81	10000001	
130	202	82	10000010	‚
131	203	83	10000011	ƒ
132	204	84	10000100	„
133	205	85	10000101	…
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	ˆ
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–
151	227	97	10010111	—
152	230	98	10011000	˜
153	231	99	10011001	™
154	232	9A	10011010	š
155	233	9B	10011011	›
156	234	9C	10011100	œ
157	235	9D	10011101	
158	236	9E	10011110	ž
159	237	9F	10011111	Ÿ
160	240	A0	10100000	
161	241	A1	10100001	¡
162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	ª
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	-
174	256	AE	10101110	®
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³
180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	·
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	º
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾
191	277	BF	10111111	¿
192	300	C0	11000000	À
193	301	C1	11000001	Á
194	302	C2	11000010	Â
195	303	C3	11000011	Ã
196	304	C4	11000100	Ä
197	305	C5	11000101	Å
198	306	C6	11000110	Æ
199	307	C7	11000111	Ç
200	310	C8	11001000	È
201	311	C9	11001001	É
202	312	CA	11001010	Ê
203	313	CB	11001011	Ë
204	314	CC	11001100	Ì
205	315	CD	11001101	Í
206	316	CE	11001110	Î
207	317	CF	11001111	Ï
208	320	D0	11010000	Ð
209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ
223	337	DF	11011111	ß
224	340	E0	11100000	à
225	341	E1	11100001	á
226	342	E2	11100010	â
227	343	E3	11100011	ã
228	344	E4	11100100	ä
229	345	E5	11100101	å
230	346	E6	11100110	æ
231	347	E7	11100111	ç
232	350	E8	11101000	è
233	351	E9	11101001	é
234	352	EA	11101010	ê
235	353	EB	11101011	ë
236	354	EC	11101100	ì
237	355	ED	11101101	í
238	356	EE	11101110	î
239	357	EF	11101111	ï
240	360	F0	11110000	ð
241	361	F1	11110001	ñ
242	362	F2	11110010	ò
243	363	F3	11110011	ó
244	364	F4	11110100	ô
245	365	F5	11110101	õ
246	366	F6	11110110	ö
247	367	F7	11110111	÷
248	370	F8	11111000	ø
249	371	F9	11111001	ù
250	372	FA	11111010	ú
251	373	FB	11111011	û
252	374	FC	11111100	ü
253	375	FD	11111101	ý
254	376	FE	11111110	þ
255	377	FF	11111111	ÿ

4. Daftr Riwayat Hidup

(CURRICULUME VITAE)

Nama	: Siti Fatimah
NIM	: 0701173206
Tempat, Tanggal Lahir	: Sei Rampah, 05 Juni 1999
Jenis Kelamin	: Perempuan
Alamat	: Kp. Ibus Dusun IX
Kel/Desa	: Kp. Ibus
Kecamatan	: Sei Rampah
Kabupaten	: Serdang Bedagai
Agama	: Islam
No. Hp	: 081533753095
Nama Orang Tua	
Ayah	: Sugiono
Ibu	: Nurhayati
Alamat Email	: Sftmah99@gmail.com
Pendidikan Formal	
-SD/MI	: SDN 104303 Kp.Ibus
-SMP/MTS	: SMP N 1 Sei Rampah
-SLTA/MA	: SMAS Kartini Utama

5. Kartu Bimbingan Dkripsi

KARTU BIMBINGAN SKRIPSI

Semester Gasal/Genap Tahun Akademik 2021 / 2022

Nama	: Siti Fatimah	Pembimbing I	: Ilka Zufria, M.KOM
NIM	: 0701173206	Pembimbing II	: Yusuf Ramadhan Nasution, M.KOM
Prog. Studi	: Ilmu komputer	SK Pembimbing	:

Judul Skripsi :
Implementasi Algoritma kriptografi AES (Advanced Encryption standard) Rijndael dalam keamanan Teks Catatan Berbasis Android

PERT	PEMBIMBING I			PEMBIMBING II		
	Tgl.	Materi Bimbingan	Tanda Tangan	Tgl.	Materi Bimbingan	Tanda Tangan
I	20/sept/2021	- Cover proposal - tabel penelitian terdahulu - tabel waktu penelitian - penulisan proposal		23/Agst/2021	- Menambahkan teori flowchart - Redaksi tabel dan gambar	
II	21/sept/2021	- Persetujuan untuk revisi judul		14/sept/2021	- Daftar pustaka - flowchart	
III	27/sept/2021	- Memakai mendeley		16/sept/2021	- Perbaiki judul sesuai dengan metode	
IV	30/sept/2021	Acc Seminar		20/9/20	Acc. Seminar Proposal	
V	17 Jan 2022	Konfirmasi soal Judul. agar sinkron yang akan dibangun		24/01/2022	Melanjutkan Bab 4. Perhitungan dan Program harus sama dulunya	

VI	7 Feb 2022	- Menambahkan black box - Perbaiki flowchart - Plaintext diubah		31 Jan 2022	Plaintext /awal kata harus dibuat	
VII	10 Feb. 2022	lenskapi Projam & print Berita		9/2/22	Acc - Sidang	
VIII	14 Feb 2022	Acc Sidang Munaqasyah				
IX						
X						

Medan, 14 Februari 2022
An. Dekan
Ketua Jurusan/Program Studi
Ilmu Komputer

Ilka Zufria, M.Kom
NIP. 198506042015031006

Catatan: *Pada saat bimbingan, kartu ini harus diisi dan ditandatangani oleh pembimbing*