Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Implementasi Algoritma Camellia Pada Penyandian Record Database

Neti Rusri Yanti, Taronisokhi Zebua

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Email: [1]netiry95@mail.com

Abstrak−*Record database* dalam bentuk teks sangat banyak digunakan, sehingga sangat rentan terhadap pencurian data oleh pihak-pihak yang tidak berhak. Demi menjaga keamanan *record database* dapat dilakukan dengan pemanfaatan teknik kriptografi.Teknik kriptografi dapat menyandikan *record database* dengan mengenkripsikannya ke dalam bentuk sandi-sandi yang tidak dipahami. Algoritma Camellia adalah salah satu algoritma yang dapat diandalkan dalam mewujudkan teknik kriptografi. Algoritma simetri ini akan menghasilkan tingkat keamanan yang lebih tinggi terhadap *record database* karena dapat menyandikannya ke bentuk sandi dengan proses yang cukup rumit sehingga akan mempersulit kriptanalis untuk mengakses *database* tersebut. Penelitian ini akan menggunakan Algoritma Camellia 128 bit untuk proses enkripsi dan dekripsinya, sehingga dalam prosesnya perlu melalui beberapa tahap yang panjang agar dapat menghasilkan *cipher* akhirnya. Algoritma ini memerlukan 18 ronde dimana setiap enam ronde harus memasuki Fungsi F dan Fungsi FL^{-1} dan juga memerlukan sebanyak 26 subkunci yaitu kw, k dan kl. Penelitian ini menguraikan proses pengamanan *record database* dengan menyandikannya berdasarkan algoritma Camellia, sehingga dihasilkan teks *record database* dalam bentuk sandi yang sulit dipahami dan dimengerti oleh orang lain. Hal ini dilakukan sebagai upaya untuk meminimalisir tindakan-tindakan penyalahgunaan *record database.*

Kata Kunci: Kriptografi, Record, Database, Camellia

Abstract−Database records in the form of text are very widely used, so it is very vulnerable to data theft by unauthorized parties. In order to maintain the security of database records, it can be done by using cryptographic techniques. Cryptographic techniques can encode database records by encrypting them in the form of passwords that are not understood. The Camellia algorithm is one algorithm that can be relied upon to realize cryptographic techniques. This symmetry algorithm will produce a higher level of security against the database record because it can encode it into a password with a fairly complex process that will make it difficult for cryptanalysts to access the database. This research will use the 128 bit Camellia algorithm for the encryption and decryption process, so that in the process it is necessary to go through several long steps in order to produce the final cipher. This algorithm requires 18 rounds where every six rounds must enter Function F and Function FL-1 and also require as many as 26 subkeys, namely kw, k and kl. This study describes the process of securing a database record by encoding it based on the Camellia algorithm, so that it produces a text record database in the form of a password that is difficult for others to understand and understand. This is done in an effort to minimize acts of misuse of database records.

Keywords: Cryptography, Record, Database, Camellia

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat dapat mempermudah instansi dan organisasi untukberkomunikasi dan saling bertukar informasi atau data secara jarak jauh tanpa adanya kendala.Seiring dengan itu, tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna yang tidak ingin informasi yang disampaikannya diketahui oleh pihak-pihak lain.

Keamanan dalam penjagaan kerahasiaan suatu data dalam organisasi merupakan aspek yang sangat penting[1]. Agar data yang akandipertukarkan ataupun disimpan benar-benar aman secara fisik maupun sistem, maka perlu dibentuk suatu sistem penyimpanan atau pengirimanya agar tidak dapat dibaca atau dilacak oleh pihak-pihak yang tidak bertanggung jawab.

Berdasarkan penelitian yang dilakukan oleh Hondro, menyatatakan bahwa *database* merupakan himpunan kelompok data operasional yang lengkap dari suatu organisasi yang saling berhubungan sehingga dijadikan sebagai sumber dari setiap sistem informasi yang sedang berjalan dan mampu memenuhi kebutuhan para pengguna yang mana dapat disimpan dalam suatu media penyimpanan[2].Ada beberapa *software* yang dapat membuat sebuah *database* seperti perangkat lunak MySQL, Microsoft Access, Navicate, dBase dan banyak perangkat lainnya.

Zebua juga menyatakan dalam penelitiannya, bahwa r*ecord database* masih sering ditampilkan dalam bentuk teks sebagai informasi bagi pengguna, sehingga dapat mempermudah kriptanalis maupun pihak-pihak lain untuk mengakses isi dati *database*[3]. Agar keamanan dan kerahasian *record database* dapat dilindungi, maka diperlukan suatu metode keamanan yang bisa menjaga keamanan dan kerahasiaan suatu data dengan akurat.

Berdasarkan penelitian lainnya yang dilakukan oleh Rusdianto, bahwa kriptografi dapat memelihara dan mejaga suatu data agar tetap terpelihara kerahasiaan dan keasliannya[4]. Metode kriptografi memiliki banyak kemampuan dalam menjaga dan merahasiakan suatu data dengan cara menyandikan data sehingga tidak diketahui makna asli dati data tersebut.

Salah satu metode kriptografi yang akan digunakan untuk mengamankan *record database*ini adalah algoritma Camellia, dimana algoritma ini termasuk salah satu teknik kriptografi modern yang dapat menyelesaikan proses enkripsi dan dekripsi dengan cepat. Proses pengamanan data akan diterapkan dalam algoritma Camellia yang mana dapat mempersulit kriptanalis untuk mengakses dan mengetahui makna asli dari data yang disandikan dan mempermudah pengguna untuk menyandikan data yang terjamin kerahasiaannya.

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Proses enkripsi dan dekripsi pada algoritma Camellia memasuki dua fungsi yaitu FL dan FL^{-1} pada setiap enam tahapnya yaitu sebelum putaran ketujuh dan ketigabelas[5]. Salah satu keunggulan lain dari algoritma Camellia yaitu memiliki sub-kunci yang sangat banyak sehingga sangat sukar untuk ditembus. Algoritma Camellia juga menggunakan beberapa notasi operator seperti operasi XOR, penjumlahan, dan substitusi yang lebih kompleks.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kata kriptografi berasal dari bahasa Yunani yaitu *cryptos* yang artinya *secret* (rahasia) dan *graphein* yang artinya *writing* (tulisan), sehingga secara keseluruhan kriptografi dalam diartikan sebagai "secret *writing*" (tulisan rahasia). Beberapa definisi lain menyatakan bahwa kriptografi merupakan ilmu dan seni yang dapat menjaga suatu rahasia dengan menyandikan suatu pesan sehingga makna asli dari pesan tidak dipahami oleh orang lain[10].

2.2 Algoritma Camellia

Algoritma Camellia merupakan salah satu algoritma kriptografi modren yang termasuk ke dalam kunci simetrik dan juga blok*cipher* dengan jumlah blok 128 bit. Algoritma ini dikembangkan oleh NTT (*Nippon Telegraph and Telephone Corporation*) yang bekerja samadengan Mitsubishi Electric Corporation pada tahun 2000. Algoritma Camellia ini merupakan salah satu perkembangan dari metode AES (*Advanced Encryption Standard*)[12].

2.3 Database

Database atau basis data secara umum diartikan sebagai kumpulan data yang saling berhubungan yang tersimpan dalam suatu media komputer.*Database* terdiri dari beberapa *table*, *field*, entitas dan *record*. *Record database* dapat sangat mudah diakses oleh pihak-pihak yang lain, dikarenakan *record database* masih sering diitampilkan dalam bentuk teks yang mana dapat memberi peluang besar pada kriptanalis untuk mengakses ataupun memodifikasi *record database* tersebut[7].

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Pengamanan informasi merupakan suatu pengamanan dalam bentuk penyandian pesan atau informasi itu sendiri, agar informasi tersebut tidak dapat dicuri oleh pihak-pihak yang tidak berkepentingan. Pengembangan ilmu teknologi jaman sekarang menemukan berbagai cara untuk dapat mencuri informasi yang telah dirahasiakan. Seiring dengan itu, dibutuhkan suatu pengaman yang lebih kuat seperti melakukan penyembunyian atau penyandian pesan. Penyandian pesan atau informasi ini diharapkan mampu memperkuat pengamanan informasi melalui media seperti pengaman *record database* .

Langkah pertama dalam penyandian *record database* ini dimulai di saat *user* mengakses suatu *database* yang kemudian memilih salah satu tabel dari *database* tersebut dan dienkripsi berdasarkan algoritma kriptografi ke dalam bentuk sandi-sandi yang tidak dipahami. Setelah *record* terenkripsi, maka *record* kembali tersimpan ke dalam *database* tersebut dalam bentuk sandi-sandi yang dihasilkan dari proses enkripsi tadi

Disaat pengguna lain ingin mengakses *database* tersebut, maka pengguna tersebut harus menginputkan kata kunci (*primary key*) dari *database* tersebut. Kata kunci (*primary key*) yang diinputkan terlebih dahulu diproses dengan mengenkripsi kata kunci tersebut ke dalam bentuk sandi yang kemudian akan dicocokkan apakah sandi dari kata kunci yang diinputkan ada di dalam *database*. Bila sandi dari kata kunci yang diinputkan cocok dengan sandi yang tersimpan dalam *database*, maka data-data yang berhubungan dengan kata kunci akan didekripsi dan kemudian hasil dekripsi akan ditampilkan.

3.2 Penerapan Algoritma Camellia

Database yang akan diamankan yaitu DB_Nilai_Mahasiswa yang dibuat menggunakan MySQL. Sampel penyandian *record database* yang akan dilakukan diambil dari salah satu *record* DB_Nilai_Mahasiswa dari tabel Nilai. *Record database* akan dipilih dan kemudian dienkripsikan berdasarkan algoritma Camellia beserta dengan kunci yang menghasilkan *cipher*, kemudian *cipher* dari hasil enkripsi inilah yang akan ditampilkan.

Proses enkripsi pada algoritma Camellia dilakukan perblok.Setiap blok *plainteks* terdiri dari 128 bit. Kunci yang digunakan terdiri dari beberapa variasi yautu 128 bit, 192 bit dan 256 bit. Proses enkripsi dan dekripsi menggunakan kunci 128 bit dilakukan sebanyak 18 putran dengan menggunakan 26 subkunci yang dihasilkan dari kunci dasar K_L dan K_A yang terdiri dari 18 k, 4 kl dan 4 kw.

Terdapat nilai Mahasiswa yang tersimpan di dalam suatu *database* yang dibuat menggunakan MySQL dengan nama DB_Nilai_Mahasiswa tabel Nilai. Dimana *record database* ini akan diamankan menggunakan teknik kriptografi agar kerahasiaan data lebih terjamin. *Record database* diamankan dengan mengekripsikan *record* ke dalam bentuk sandi menggunakan algoritma Camellia dengan kunci 128 bit.

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

*Record*sampel : Neti Rusri Yanti
Key : Skripsi2018-NETI

Nilai konstanta yang digunakan dalam pembangkitan kunci ada enam yaitu $\sum_1$ hingga $\sum_6$. Nilai konstanta dapat dilihat pada tabel dibawah.

Tabel 1. Nilai konstanta pembangkitan kunci

$\sum_1$	0xA09E6673FBCC908B
$\sum_2$	0xB67AE8584CAA73B2
$\sum_3$	0xC6EF372FE94F82BE
$\sum_4$	0x54FF53A5F1D36F1C
$\sum_5$	0x10E527FADE682D1D
$\sum_6$	0xB05688C2B3E6C1FD

Key = Skripsi2018-NETI
= 536B 7269 7073 6932 3031 382D 4E45 5449

1. Penjadwalan Kunci

a. K_L= 536B 7269 7073 6932 3031 382D 4E45 5449
KL_L = 536B 7269 7073 6932
KL_R = 3031 382D 4E45 5449

b. Misalkan $P(S(KL_L \oplus \sum_1))$= A
$A \oplus KL_R$ = A'
$P(S(A' \oplus \sum_2))$ = B
$B \oplus KL_L$ = B'
$P(S(B \oplus \sum_3))$ = C
$C \oplus A$ = C'
$P(S(C' \oplus \sum_4))$ = D
$D \oplus B$ = D'
D' || C' = K_A

A = $KL_L \oplus \sum_1$
= 536B 7269 7073 6932 ⊕ A09E6673FBCC908B
= F3F5 141A 8BBF F9B9

$P(S(A_{8(8)}))$	= F3	$=S_1(243)$	=123
$P(S(A_{7(8)}))$	= F5	$=S_4(245)$	=104
$P(S(A_{6(8)}))$	= 14	$=S_3(20)$	=162
$P(S(A_{5(8)}))$	= 1A	$=S_2(26)$	=158
$P(S(A_{4(8)}))$	= 8B	$=S_4(139)$	=33
$P(S(A_{3(8)}))$	= BF	$=S_3(191)$	=23
$P(S(A_{2(8)}))$	= F9	$=S_2(249)$	=199
$P(S(A_{1(8)}))$	= B9	$= S_1(185)$	=91

A =7B68 A29E 2117 C75B
A' = A ⊕ KL_R
= 7B68 A29E 2117 C75B ⊕ 3031 382D 4E45 5449
= 4B59 9AB3 6F52 9312
B = $A' \oplus \sum_2$
= 4B59 9AB3 6F52 9312⊕ B67AE8584CAA73B2
= FD23 72EB 23F8 E0A0

$P(S(B_{8(8)}))$	= FD	$=S_1(253)$	=199
$P(S(B_{7(8)}))$	= 23	$=S_4(35)$	=176
$P(S(B_{6(8)}))$	= 72	$=S_3(114)$	=231
$P(S(B_{5(8)}))$	= EB	$=S_2(235)$	=52
$P(S(B_{4(8)}))$	= 23	$=S_4(35)$	=176
$P(S(B_{3(8)}))$	= F8	$=S_3(248)$	=138
$P(S(B_{2(8)}))$	= E0	$=S_2(224)$	=228
$P(S(B_{1(8)}))$	= B0	$=S_1(160)$	=135

B =C7B0 E734 B08A E487
B' = B ⊕ KL_L
= C7B0 E734 B08A E487 ⊕ 536B 7269 7073 6932
=94DB 955D C0F9 8DB5
B' ⊕ KL_L = B
A' ⊕ KL_R = A
C =$P(S(B \oplus \sum_3))$

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

= C7B0 E734 B08A E487 ⊕ C6EF372FE94F82BE
= 015F D01B 59C5 6639

$P(S(C_{8(8)}))$ = 01 $=S_1(1)$ =130
$P(S(C_{7(8)}))$ = 5F $=S_4(95)$ =99
$P(S(C_{6(8)}))$ = D0 $=S_3(208)$ =60
$P(S(C_{5(8)}))$ = 1B $=S_2(27)$ =156
$P(S(C_{4(8)}))$ = 59 $=S_4(89)$ =216
$P(S(C_{3(8)}))$ = C5 $=S_3(197)$ =55
$P(S(C_{2(8)}))$ = 66 $=S_2(102)$ =34
$P(S(C_{1(8)}))$ = 39 $=S_1(57)$ =2

C = 8263 3C9C D837 2202
C' = C ⊕ A
= 8263 3C9C D837 2202 ⊕ 7B68 A29E 2117 C75B
=F90B 9E02 F920 E559
D =P(S(C'⊕$\sum_4$))
= F90B 9E02 F920 E559⊕ 54FF53A5F1D36F1C
= ADF4 CDA7 08F3 8A45

$P(S(D_{8(8)}))$ = AD $=S_1(173)$ =127
$P(S(D_{7(8)}))$ = F4 $=S_4(244)$ =187
$P(S(D_{6(8)}))$ = CD $=S_3(205)$ =254
$P(S(D_{5(8)}))$ = A7 $=S_2(167)$ =102
$P(S(D_{4(8)}))$ = 08 $=S_4(8)$ =35
$P(S(D_{3(8)}))$ = F3 $=S_3(243)$ =189
$P(S(D_{2(8)}))$ = 8A $=S_2(138)$ =60
$P(S(D_{1(8)}))$ = 45 $=S_1(69)$ =204

D = 7FBB FE66 23BD 3CCC
D' =D⊕ B
= 7FBB FE66 23BD 3CCC⊕C7B0 E734 B08A E487
= B80B 1952 9337 D84B
K_A = C' || D'
K_A = F90B 9E02 F920 E559 B80B 1952 9337 D84B

Tabel 2. Subkunci algoritma Camellia

	Subkunci	**Nilai**
Prewhitening	$Kw_{1(64)}$	$(KL<<<0)_{L(64)}$
	$Kw_{2(64)}$	$(KL<<<0)_{R(64)}$
F (Tahap 1)	$k_{1(64)}$	$(KA<<<0)_{L(64)}$
F (Tahap 2)	$k_{2(64)}$	$(KA<<<0)_{R(64)}$
F (Tahap 3)	$k_{3(64)}$	$(KL<<<15)_{L(64)}$
F (Tahap 4)	$k_{4(64)}$	$(KL<<<15)_{R(64)}$
F (Tahap 5)	$k_{5(64)}$	$(KA<<<15)_{L(64)}$
F (Tahap 6)	$k_{6(64)}$	$(KA<<<15)_{R(64)}$
FL	$kl_{1(64)}$	$(KA<<<30)_{L(64)}$
FL^{-1}	$kl_{2(64)}$	$(KA<<<30)_{R(64)}$
F (Tahap 7)	$k_{7(64)}$	$(KL<<<45)_{L(64)}$
F (Tahap 8)	$k_{8(64)}$	$(KL<<<45)_{R(64)}$
F (Tahap 9)	$K_{9(64)}$	$(KA<<<45)_{L(64)}$
F (Tahap 10)	$k_{10(64)}$	$(KL<<<60)_{R(64)}$
F (Tahap 11)	$k_{1164)}$	$(KA<<<60)_{L(64)}$
F (Tahap 12)	$k_{12(64)}$	$(KA<<<60)_{R(64)}$
FL	$kl_{3(64)}$	$(KL<<<77)_{L(64)}$
FL^{-1}	$kl_{4(64)}$	$(KL<<<77)_{R(64)}$
F (Tahap 13)	$k_{13(64)}$	$(KL<<<94)_{L(64)}$
F (Tahap 14)	$k_{14(64)}$	$(KL<<<94)_{R(64)}$
F (Tahap 15)	$k_{15(64)}$	$(KA<<<94)_{L(64)}$
F (Tahap 16)	$k_{16(64)}$	$(KA<<<94)_{R(64)}$
F (Tahap 17)	$k_{17(64)}$	$(KL<<<111)_{L(64)}$
F (Tahap 18)	$k_{18(64)}$	$(KL<<<111)_{R(64)}$
Postwhitening	$Kw_{3(64)}$	$(KA<<<111)_{L(64)}$
	$Kw_{4(64)}$	$(KA<<<111)_{R(64)}$

Berdasarkan tabel pembangkitan subkunci di atas, maka didapatkan 24 subkunci yang akan digunakan pada

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

proses enkripsi dan dekripsi, yaitu:

$Kw_{1(64)}$ = $(KL <<< 0)_{L(64)}$ = 536B 7269 7073 6932
$Kw_{2(64)}$ = $(KL <<< 0)_{R(64)}$ = 3031 382D 4E45 5449
$k_{1(64)}$ = $(KA <<< 0)_{L(64)}$ = F90B 9E02 F920 E559
$k_{2(64)}$ = $(KA <<< 0)_{R(64)}$ = B80B 1952 9337 D84B
$k_{3(64)}$ = $(KL <<< 15)_{L(64)}$ = B934 B839 B499 1818
$k_{4(64)}$ = $(KL <<< 15)_{R(64)}$ = 9C16 A722 AA24 A9B5
$k_{5(64)}$ = $(KA <<< 15)_{L(64)}$ = CF01 7C90 72AC DC05
$k_{6(64)}$ = $(KA <<< 15)_{R(64)}$ = 8CA9 499B EC25 FC85
$kl_{1(64)}$ = $(KA <<< 30)_{L(64)}$ = 2F92 0E55 9B80 B195
$kl_{2(64)}$ = $(KA <<< 30)_{R(64)}$ = 2933 7D84 BF90 B9E0
$k_{7(64)}$ = $(KL <<< 45)_{L(64)}$ = 6D26 4606 2705 A9C8
$k_{8(64)}$ = $(KL <<< 45)_{R(64)}$ = AA89 2A6D 6E4D 2E0E
$k_{9(64)}$ = $(KA <<< 45)_{L(64)}$ = 1CAB 3701 632A 5266
$k_{10(64)}$ = $(KL <<< 60)_{R(64)}$ = 9536 B726 9707 3693
$k_{11(64)}$ = $(KA <<< 60)_{L(64)}$ = 6E02 C654 A4CD F612
$k_{12(64)}$ = $(KA <<< 60)_{R(64)}$ = FE42 E780 BE48 3956
$kl_{3(64)}$ = $(KL <<< 77)_{L(64)}$ = 2705 A9C8 AA89 2A6D
$kl_{4(64)}$ = $(KL <<< 77)_{R(64)}$ = 6E4D 2E0E 6D26 4606
$k_{13(64)}$ = $(KL <<< 94)_{L(64)}$ = 5391 5512 54DA DC9A
$k_{14(64)}$ = $(KL <<< 94)_{R(64)}$ = 5C1C DA4C 8C0C 4E0B
$k_{15(64)}$ = $(KA <<< 94)_{L(64)}$ = 9337 D84B F90B 9E02
$k_{16(64)}$ = $(KA <<< 94)_{R(64)}$ = F920 E559 B80B 1952
$k_{17(64)}$ = $(KL <<< 111)_{L(64)}$ = AA24 A9B5 B934 B839
$k_{18(64)}$ = $(KL <<< 111)_{R(64)}$ = B499 1818 9C16 A722
$Kw_{3(64)}$ = $(KA <<< 111)_{L(64)}$ = B097 F217 3C05 F241
$Kw_{4(64)}$ = $(KA <<< 111)_{R(64)}$ = CAB3 7016 32A5 266F

2. Proses Enkripsi

Record sampel = Neti Rusri Yanti
$M_{(128)}$ = 4E65 7469 2052 7573 7269 2059 616E 7469

a. $M_{L(64)}$ = 4E65 7469 2052 7573
$M_{R(64)}$ = 7269 2059 616E 7469
L_0 = $M_{L(64)} \oplus kw_1$
= 4E65 7469 2052 7573 ⊕536B 7269 7073 6932
= 1D0E 0600 5021 1C41
R_0 = $M_{R(64)} \oplus kw_2$
= 7269 2059 616E 7469 ⊕3031 382D 4E45 5449
= 4258 1874 2F2B 2020

b. Round →1
L_1 = $R_0 \oplus F(L_0, k_1)$
R_1 = L_0
L_1 = $R_0 \oplus F(L_0, k_1)$
= 4258 1874 2F2B 2020 ⊕F (L_0, k_1)
R_1 = 1D0E 0600 5021 1C41
k_1 = F90B 9E02 F920 E559
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$

$P(S(X_{8(8)} \oplus k_{1(8)}))$ = 1D ⊕F9 = E4 = $P(S_1(228))$ = Y(248)
$P(S(X_{7(8)} \oplus k_{1(8)}))$ = 0E ⊕0B = 5 = $P(S_4(5))$ = Y(87)
$P(S(X_{6(8)} \oplus k_{1(8)}))$ = 06 ⊕9E = 98 = $P(S_3(152))$ = Y(69)
$P(S(X_{5(8)} \oplus k_{1(8)}))$ = 00 ⊕02 = 2 = $P(S_2(2))$ = Y(88)
$P(S(X_{4(8)} \oplus k_{1(8)}))$ = 50 ⊕F9 = A9 = $P(S_4(169))$ = Y(194)
$P(S(X_{3(8)} \oplus k_{1(8)}))$ = 21 ⊕20 = 1 = $P(S_3(1))$ = Y(65)
$P(S(X_{2(8)} \oplus k_{1(8)}))$ = 1C ⊕E5 = F9 = $P(S_2(249))$ = Y(199)
$P(S(X_{1(8)} \oplus k_{1(8)}))$ = 41 ⊕59 = 18 = $P(S_1(24))$ = Y(237)

$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8$ =237⊕65⊕194⊕69⊕87⊕248 =132
$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8$ =237⊕199⊕194⊕88⊕87⊕248 =31
$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8$ =237⊕199⊕65⊕88⊕69⊕248 =142
$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7$ =199⊕65⊕194 ⊕88⊕69⊕87 =14
$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8$ =237⊕199⊕69⊕87⊕248 =192
$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8$ =199⊕65⊕88⊕69⊕248 =99
$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8$ =65⊕194⊕88⊕69⊕248 =102

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 \quad = 237 \oplus 194 \oplus 88 \oplus 69 \oplus 87 \quad = 101$
$z'_{(64)}$ = 841F 8E0E C063 6665
$L_1 = R_0 \oplus F(L_0, k_1)$
= 4258 1874 2F2B 2020 ⊕841F 8E0E C063 6665
= C647 967A EF48 4645
R_1 = 1D0E 0600 5021 1C41
c. Round →2
$L_2 = R_1 \oplus F(L_1, k_2)$
$R_2 = L_1$
$L_2 = R_1 \oplus F(L_1, k_2)$
= 1D0E 0600 5021 1C41⊕F (L_1, k_2)
R_2 = C647 967A EF48 4645
k_2 = B80B 1952 9337 D84B
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{2(64)}$ = C647 967A EF48 4645 ⊕ B80B 1952 9337 D84B
= 7E4C 8F28 7C7F 9E0E

$P(S(X_{8(8)} \oplus k_{2(8)})$	= 7E	= $P(S_1(126))$	= Y(105)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= 4C	= $P(S_4(76))$	= Y(138)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= 8F	= $P(S_3(143))$	= Y(105)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= 28	= $P(S_2(40))$	= Y(124)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= 7C	= $P(S_4(124))$	= Y(21)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= 7F	= $P(S_3(127))$	= Y(40)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= 9E	= $P(S_2(158))$	= Y(187)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= 0E	= $P(S_1(14))$	= Y(174)

$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 \quad = 174 \oplus 40 \oplus 21 \oplus 105 \oplus 138 \oplus 105 \quad = 25$
$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 \quad = 174 \oplus 187 \oplus 21 \oplus 124 \oplus 138 \oplus 105 \quad = 159$
$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 \quad = 174 \oplus 187 \oplus 40 \oplus 124 \oplus 105 \oplus 105 \quad = 65$
$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 \quad = 187 \oplus 40 \oplus 21 \oplus 124 \oplus 105 \oplus 138 \quad = 25$
$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 \quad = 174 \oplus 187 \oplus 105 \oplus 138 \oplus 105 \quad = 159$
$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 \quad = 187 \oplus 40 \oplus 124 \oplus 138 \oplus 105 \quad = 12$
$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 \quad = 40 \oplus 21 \oplus 124 \oplus 105 \oplus 105 \quad = 65$
$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 \quad = 174 \oplus 21 \oplus 124 \oplus 105 \oplus 13 \quad = 36$
$z'_{(64)}$ = 199F 4119 9F0C 4124
$L_2 = R_1 \oplus F(L_1, k_2)$
= 1D0E 0600 5021 1C41⊕199F 4119 9F0C 4124
= 0491 4719 CF2D 5D65
R_2 = C647 967A EF48 4645
d. Round→3
$L_3 = R_2 \oplus F(L_2, k_3)$
$R_3 = L_2$
$L_3 = R_2 \oplus F(L_2, k_3)$
= C647 967A EF48 4645 ⊕F (L_2, k_3)
R_3 = 0491 4719 CF2D 5D65
k_3 = B934 B839 B499 1818
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{3(64)}$ = 0491 4719 CF2D 5D65 ⊕ B934 B839 B499 1818
= BDA5 FF20 7BB4 457D

$P(S(X_{8(8)} \oplus k_{2(8)})$	= BD	= $P(S_1(189))$	= Y(190)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= A5	= $P(S_4(165))$	= Y(32)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= FF	= $P(S_3(255))$	= Y(79)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= 20	= $P(S_2(32))$	= Y(13)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= 7B	= $P(S_4(123))$	= Y(67)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= B4	= $P(S_3(180))$	= Y(230)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= 45	= $P(S_2(69))$	= Y(153)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= 7D	= $P(S_1(125))$	= Y(252)

$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 \quad = 252 \oplus 230 \oplus 67 \oplus 79 \oplus 32 \oplus 190 \quad = 136$
$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 \quad = 252 \oplus 153 \oplus 67 \oplus 13 \oplus 32 \oplus 190 \quad = 181$
$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 \quad = 252 \oplus 153 \oplus 230 \oplus 13 \oplus 79 \oplus 190 \quad = 127$
$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 \quad = 153 \oplus 230 \oplus 67 \oplus 13 \oplus 79 \oplus 32 \quad = 94$
$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 \quad = 252 \oplus 153 \oplus 79 \oplus 32 \oplus 190 = 180$
$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 \quad = 153 \oplus 230 \oplus 13 \oplus 32 \oplus 190 = 236$
$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 \quad = 230 \oplus 67 \oplus 13 \oplus 79 \oplus 190 \quad = 89$

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7 =252⊕67⊕13⊕79⊕32 =221
$z'_{(64)}$ = 88B5 7F5E B4EC 59DD
L_3 = R_2 ⊕F(L_2, k_3)
= C647 967A EF48 4645⊕88B5 7F5E B4EC 59DD
= 4EF2 E924 5BA4 1F98
R_3 = 0491 4719 CF2D 5D65

Langkah round dilakukan sampai dengan round 18, Setelah *cipherteks* didapatkan dalam bentuk *hexadecimal*, kemudian *cipherteks* dikonversikan ke dalam karakter yaitu ●‹Œ©óqv_|àÕÃî#a⊥

3. Proses Dekripsi

Seorang pengguna ingin mengakses suatu *database* yang telah terekripsi. Agar dapat mengakses *database* tersebut, maka pengguna tersebut perlu mendekripsi terlebih dahulu sandi-sandi dari *record* tersebut.

Record Sampel = ●‹Œ©óqv_|àÕÃî#a⊥
$C_{(128)}$ = 078B 8CA9 F371 765F 7CE0 D5C3 EE23 6115
$C_{(128)}$ ⊕ ($kw_{3(64)}$ || $kw_{4(64)}$) = $R_{18(64)}$ || $L_{18(64)}$
078B 8CA9 F371 765F 7CE0 D5C3 EE23 6115 ⊕ (B097 F217 3C05 F241|| CAB3 7016 32A5 266F)= B71C 7EBE CF74 841E|| B653 A5D5 DC86 477A
$R_{18(64)}$ = B71C 7EBE CF74 841E
$L_{18(64)}$ = B653 A5D5 DC86 477A
Round →1
R_{r-1} = L_r⊕ F(R_r, k_r)
L_{r-1} = R_r
R_{17}= L_{18} ⊕F(R_{18}, k_{18})
L_{17}= R_{18}
R_{17}= L_{18} ⊕F(R_{18}, k_{18})
= B653 A5D5 DC86 477A⊕F (R_{18}, k_{18})
L_{17}= B71C 7EBE CF74 841E
k_{18} = B499 1818 9C16 A722
($X_{(64)}$, $k_{(64)}$) →$Y_{(64)}$ = P(S ($X_{(64)}$⊕$k_{(64)}$))
$X_{(64)}$ ⊕$k_{18(64)}$ = B71C 7EBE CF74 841E ⊕ B499 1818 9C16 A722
= 0385 66A6 5362 233C
P(S($X_{8(8)}$ ⊕$k_{2(8)}$) = 03 = P(S_1(3)) = Y(236)
P(S($X_{7(8)}$ ⊕$k_{2(8)}$)) = 85 = P(S_4(133)) = Y(53)
P(S($X_{6(8)}$ ⊕$k_{2(8)}$)) = 66 = P(S_3(102)) = Y(136)
P(S($X_{5(8)}$ ⊕$k_{2(8)}$)) = A6 = P(S_2(166)) = Y(33)
P(S($X_{4(8)}$ ⊕$k_{2(8)}$)) = 53 = P(S_4(83)) = Y(144)
P(S($X_{3(8)}$ ⊕$k_{2(8)}$)) = 62 = P(S_3(98)) = Y(29)
P(S($X_{2(8)}$ ⊕$k_{2(8)}$)) = 23 = P(S_2(35)) = Y(31)
P(S($X_{1(8)}$ ⊕$k_{2(8)}$)) = 3C = P(S_1(60)) = Y(81)
z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8 =81⊕29⊕144⊕136 ⊕53⊕236 =141
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8 =81⊕31⊕144⊕33⊕53⊕236 =38
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8 =81⊕31⊕29⊕33⊕136⊕236 =22
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7 =31⊕29 ⊕144⊕33⊕136⊕236 =215
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8 =81⊕31⊕136⊕53⊕236 =31
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8 =31⊕29⊕33⊕53⊕236 =250
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8 =29⊕144⊕33⊕136⊕236 =200
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7 =81⊕144⊕33⊕136⊕53 =93
$z'_{(64)}$ = 8D26 16D7 1FFA C85D
R_{17}= L_{18} ⊕F(R_{18}, k_{18})
= B653 A5D5 DC86 477A⊕8D26 16D7 1FFA C85D
= 3B75 B302 C37C 8F27
L_{17}= B71C 7EBE CF74 841E
Round →2
R_{16}= L_{17} ⊕F(R_{17}, k_{17})
L_{16}= R_{17}
R_{16}= L_{17} ⊕F(R_{17}, k_{17})
= B71C 7EBE CF74 841E⊕F (R_{18}, k_{18})
L_{16}= 3B75 B302 C37C 8F27
k_{17} = AA24 A9B5 B934 B839
($X_{(64)}$, $k_{(64)}$) →$Y_{(64)}$ = P(S ($X_{(64)}$⊕$k_{(64)}$))
$X_{(64)}$ ⊕$k_{17(64)}$ = 3B75 B302 C37C 8F27 ⊕ AA24 A9B5 B934 B839

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

= 9151 1AB7 7A48 371E

$P(S(X_{8(8)} \oplus k_{2(8)}) = 91 = P(S_1(145)) = Y(196)$
$P(S(X_{7(8)} \oplus k_{2(8)})) = 51 = P(S_4(81)) = Y(131)$
$P(S(X_{6(8)} \oplus k_{2(8)})) = 1A = P(S_3(26)) = Y(167)$
$P(S(X_{5(8)} \oplus k_{2(8)})) = B7 = P(S_2(183)) = Y(118)$
$P(S(X_{4(8)} \oplus k_{2(8)})) = 7A = P(S_4(122)) = Y(187)$
$P(S(X_{3(8)} \oplus k_{2(8)})) = 48 = P(S_3(72)) = Y(18)$
$P(S(X_{2(8)} \oplus k_{2(8)})) = 37 = P(S_2(55)) = Y(122)$
$P(S(X_{1(8)} \oplus k_{2(8)})) = 1E = P(S_1(30)) = Y(146)$

$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 146 \oplus 18 \oplus 187 \oplus 167 \oplus 131 \oplus 196 = 219$
$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 146 \oplus 122 \oplus 187 \oplus 118 \oplus 131 \oplus 196 = 98$
$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 146 \oplus 122 \oplus 18 \oplus 118 \oplus 167 \oplus 196 = 239$
$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 122 \oplus 18 \oplus 187 \oplus 118 \oplus 167 \oplus 131 = 129$
$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 146 \oplus 122 \oplus 167 \oplus 131 \oplus 196 = 8$
$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 122 \oplus 18 \oplus 118 \oplus 131 \oplus 196 = 89$
$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 18 \oplus 187 \oplus 118 \oplus 167 \oplus 196 = 188$
$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 146 \oplus 187 \oplus 118 \oplus 167 \oplus 131 = 123$

$z'_{(64)}$ = DB62 EF81 0859 BC7B
$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$
= B71C 7EBE CF74 841E⊕DB62 EF81 0859 BC7B
= 6C7E 913F C72D 3865
L_{16}= 3B75 B302 C37C 8F27
Round →3
$R_{15} = L_{16} \oplus F(R_{16}, k_{16})$
$L_{15} = R_{16}$
$R_{15} = L_{16} \oplus F(R_{16}, k_{16})$
= 3B75 B302 C37C 8F27 ⊕F (R_{16}, k_{16})
L_{15}= 6C7E 913F C72D 3865
k_{16} = F920 E559 B80B 1952
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{16(64)}$ = 6C7E 913F C72D 3865 ⊕ F920 E559 B80B 1952
= 955E 7466 7F26 2137

$P(S(X_{8(8)} \oplus k_{2(8)}) = 95 = P(S_1(149)) = Y(247)$
$P(S(X_{7(8)} \oplus k_{2(8)})) = 5E = P(S_4(94)) = Y(19)$
$P(S(X_{6(8)} \oplus k_{2(8)})) = 74 = P(S_3(116)) = Y(225)$
$P(S(X_{5(8)} \oplus k_{2(8)})) = 66 = P(S_2(102)) = Y(34)$
$P(S(X_{4(8)} \oplus k_{2(8)})) = 7F = P(S_4(127)) = Y(128)$
$P(S(X_{3(8)} \oplus k_{2(8)})) = 26 = P(S_3(38)) = Y(143)$
$P(S(X_{2(8)} \oplus k_{2(8)})) = 21 = P(S_2(33)) = Y(113)$
$P(S(X_{1(8)} \oplus k_{2(8)})) = 37 = P(S_1(55)) = Y(45)$

$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 45 \oplus 143 \oplus 128 \oplus 225 \oplus 19 \oplus 247 = 39$
$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 45 \oplus 113 \oplus 128 \oplus 34 \oplus 19 \oplus 247 = 26$
$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 45 \oplus 113 \oplus 143 \oplus 34 \oplus 225 \oplus 247 = 231$
$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 113 \oplus 143 \oplus 128 \oplus 34 \oplus 225 \oplus 19 = 174$
$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 45 \oplus 113 \oplus 225 \oplus 19 \oplus 247 = 89$
$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 113 \oplus 143 \oplus 34 \oplus 19 \oplus 247 = 56$
$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 143 \oplus 128 \oplus 34 \oplus 225 \oplus 247 = 59$
$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 45 \oplus 128 \oplus 34 \oplus 225 \oplus 19 = 125$

$z'_{(64)}$ = 271A E7AE 5938 3B7D
$R_{15} = L_{16} \oplus F(R_{16}, k_{16})$
= 3B75 B302 C37C 8F27⊕271A E7AE 5938 3B7D
= 1C6F 54AC 9A44 B45A
L_{15}= 6C7E 913F C72D 3865

Proses dekripsi dilakukan sampai dengan round 18, Setelah hasil *plainteks* didapatkan, *plainteks hexadecimal* dikonversikan ke dalam bentuk karakter yaitu Neti Rusri Yanti.

3.2 Pengujian

Tampilan program yang akan ditampilkan yaitu hasil dari perancangan yang telah dibuat pada bahasan sebelumnya. Tampilan ini telah dibuat menggunakan bahasa pemograman *Microsoft Visual Basic. NET 2008* yang berupa tampilan menu utama, enkripsi, dekripsi dan *about*.

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 3, May 2020, Page 107-116
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Tampilan form menu utama adalah tampilan yang pertama kali terbuka disaat aplikasi dijalankan oleh user. Form menu utama berisikan menu-menu berupa menu enkripsi, menu dekripsi, menu about dan menu keluar. Adapun tampilan menu utama aplikasi sebagai berikut.



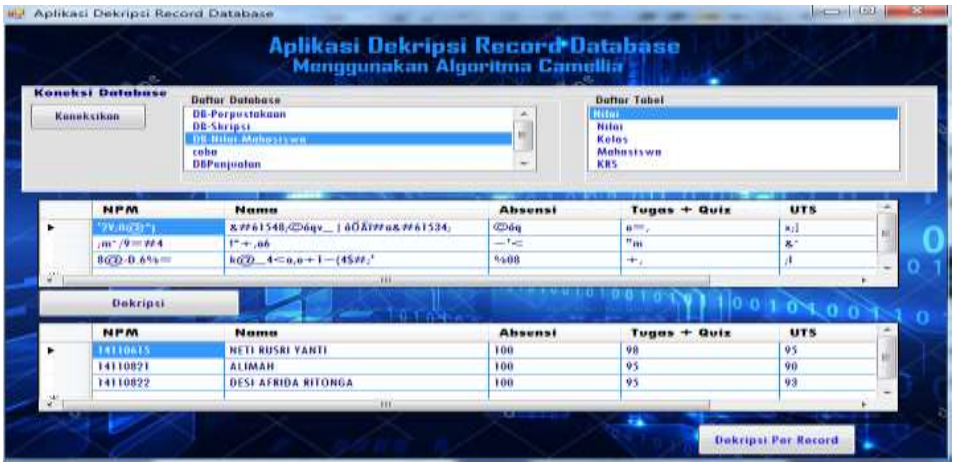
Gambar 1. Tampilan Menu Utama Aplikasi

Tampilan proses enkripsi adalah tampilan yang tampil disaat dipilihnya menu enkripsi pada menu utama aplikasi. Tampilan proses enkripsi berisikan langkah-langkah uintuk mengenkripsikan *record database*. Berikut ini tampilan dati form proses enkripsi *record database*.



Gambar 2. Tampilan Form enkripsi

Tampilan proses dekripsi adalah tampilan yang tampil diaat dipilihnya menu dekripsi pada menu utama. Tampilan form dekripsi berisikan langkah-langkah uintuk mendekripsikan *record database*. Berikut ini tampilan proses dekripsi *record database*.



Gambar 3. Tampilan Proses Dekripsi

4. KESIMPULAN

Berdasarkan hasil penerapan algoritma Camellia pada penyandian *record database* yang telah dilakukan, penulis dapat menarik kesimpulan sebagai berikut:

1. Penyandian *record database* berdasarkan algoritma Camellia mampu mempersulit pihak-pihak lain untuk mengerti dan memahami isi dari *record database.*
2. Tingkat keamanan yang dihasilkan sangat tinggi karena algoritma Camellia termasuk salah satu *cipher* blok dengan ukuran blok yang besar dan juga memiliki variasi kunci yang banyak. Variasi kunci terdiri dari 128 bit,

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**

192 bit dan 256 bit yang dapat membangkitkan 24 subkunci untuk kunci 128 bit dan 26 subkunci untuk 192 dan 256 bit.

3. Penyandian *record database* diawali dengan penentuan nama *database* dan pemilihan tabel yang memiliki *record* yang akan disandikan, dimana maasing-masing *record* pada tabel yang dipilih disandikan berdasarkan algoritma Camellia.

REFERENCES

[1] Y. Yanti, Munawir, Zulfan, and Erdiwansyah, "Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain," *Serambi Eng.*, vol. II, no. 4, pp. 172–175, 2017.
[2] R. K. Hondro and G. W. Nurcahyo, "ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA TRIANGLE CHAIN CIPHER (TCC) UNTUK ENKRIPSI RECORD TABEL DATABASE," *J. Teknol. Inf. dan Komput.*, vol. 3, no. Desember, pp. 118–127, 2014.
[3] T. Zebua, "TRIANGLE CHAIN PADA PENYANDIAN RECORD DATABASE ...," *Pelita Inform. Budi Darma*, vol. 3, no. April, pp. 37–49, 2013.
[4] Rusdianto and A. Qashlim, "IMPLEMENTASI ALGORITMA MD5 UNTUK KEAMANAN DOKUMEN," *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 10–16, 2016.
[5] L. Sutanto, G. S. Budhi, and L. W. Santoso, "PERBANDINGAN APLIKASI MENGGUNAKAN METODE CAMELLIA 128 BIT KEY DAN 256 BIT KEY," *J. Inform.*, vol. 12, no. 2, pp. 109–116, 2014.
[6] R. H. Zain, "Perancangan Dan Implementasi Cryptography Dengan Metode Algoritma Rc4 Pada Type File Document Menggunakan Bahasa Pemrograman Visual Basic 6 . 0," *J. Momentum*, vol. 12, no. 1, pp. 71–80, 2012.
[7] N. R. Yanti, Alimah, and D. A. Ritonga, "Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database," *J. Sains Komput. Inform.*, vol. 2, no. 1, pp. 23–32, 2018.
[8] D. Ariyus, *TEORI ILMU KRIPTOGRAFI Teori Analisis dan Implementasi*, I. Yogyakarta: ANDI, 2008.
[9] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan MATLAB*, I. Yogyakarta: ANDI, 2015.
[10] R. Munir, *Kriptografi*. Bandung: INFORMATIKA Bandung, 2006.
[11] R. Sadikin, *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Yogyakarta: ANDI, 2012.
[12] B. S. W. Poetro and R. Wardoyo, "Perbandingan Efisiensi , Efektifitas dan Kualitas Algoritma Rijndael dengan Algoritma Camellia pada Citra Digital," *J. Math. Nat. Sci.*, vol. 24, no. 3, pp. 281–291, 2014.
[13] K. Aoki *et al.*, "Camellia : A 128-Bit Block Cipher Suitable for Multiple Platforms – Design and Analysis Structure of Camellia," *Springer-Verlag Berlin Heidelb.*, pp. 39–56, 2001.
[14] P. B. Santoso, "Budi Akademika," 2012. [Online]. Available: http://pbsabn.lecture.ub.ac.id/2012/05/hierarki-data-data-hierarchy/. [Accessed: 19-Jul-2018].
[15] A. B. bin Ladjamuddin, *Konsep Sistem Basis Data dan Implementasinya*, I. Yogyakarta: Graha Ilmu, 2004.
[16] M. Shalahuddin and A. Rossa, *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*, I. B: Modula, 2011.
[17] P. Pudjo and H. Widodo, *Menggunakan UML*, I. Bandung: INFORMATIKA Bandung, 2011.
[18] J. Hartono M, *Analisi Desain*. Yogyakarta: ANDI, 2005.
[19] W. Komputer, *Panduan Aplikasi dan Solusi (PAS) Membuat Aplikasi Client Server dengan Visual Basic 2008*, I. Semarang: ANDI, 2010.
[20] A. Nugroho, *Mengembangkan Aplikasi Basis Data Menggunakan Visual Basic.NET dan Oracle*, I. Yogyakarta: ANDI, 2010.
[21] P. A. Aditya, *Perancangan & Pembangunan Sistem Informasi*, II. Yogyakarta: ANDI, 2006.

Submitted: **18/04/2020**; Accepted: **17/05/2020**; Published: **26/05/2020**