Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

Implementasi Algoritma Camellia Dalam Penyandian Pesan SMS Pada Telepon Seluler

Halimah Ani, Surya Darma Nasution

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: [1]halimahani85@gmail.com

Abstrak−Teknologi SMS juga tidak menjamin keamanan dan kerahasian pesan yang dikirim. Pendisbutrian isi pesan sangat rentan dengan gangguan atau pencurian oleh pihak-pihak yang tidak bertanggung jawab, karena isi pesan yang bersifat plainteks (teks-terang) dapat dibaca oleh siapa saja,untuk mengurangi resiko yang ditimbulkan salah satu cara penanggulangnya adalah dengan menerapkan suatu algoritma kriptografi pada pesan yang dikirimkan. Algoritma kriptografi yang digunakan adalah algoritma kriptografi Camellia dengan panjang kunci 128-bit. Camellia merupakan block cipher yang dirancang oleh ahli-ahli dalam riset dan pengembangan dalam teknik kriptografik. Dengan terenkripsinya pesan yang dikirim maka seseorang yang berhasil mencuri informasi pesan SMS yang dikirim, maka seseorang yang berhasil mencuri informasi pesan teks yang dikirim tersebut akan kesulitan untuk mengetahui isi dari pesan tersebut. Dirancang dan dibangun suatu program aplikasi menggunakan android dengan sistem android minimal versi 2.2 untuk mempermudah pengguna dalam menyandikan pesan SMS.

Kata Kunci: Kriptografi, Keamanan Pesan, Algoritma Camellia.

Abstract−SMS technology also does not guarantee the security and confidentiality of messages sent. The distribution of message content is very vulnerable to interference or theft by irresponsible parties, because the message content that is plaintext (text-light) can be read by anyone, to reduce the risk caused by one way of overcoming it is to implement a cryptographic algorithm on the message sent. The cryptographic algorithm used is the Camellia cryptographic algorithm with a 128-bit key length. Camellia is a block cipher designed by experts in research and development in cryptographic techniques. With the encrypted message sent then someone who managed to steal information about the SMS message sent, then someone who succeeded in stealing information from the text message sent would find it difficult to know the contents of the message. Designed and built an application program using Android with an Android system of at least version 2.2 to facilitate users in encoding SMS messages.

Keywords: Cryptography, Message Security, Camellia Algorithm.

1. PENDAHULUAN

Pesan SMS (*Short Message Service)* adalah tulisan *electronic* yang prakteknya membuat atau mengirim singkat suatu isi pesan dari dua ponsel atau lebih dengan tujuan untuk bermunikasi dan saling bertukar informasi. Penggunaan SMS saat ini sangat popular digunakan sebagai salah satu alat komunikasi yang mudah dan cepat, namun pendistribusian isi pesan sangat rentan dengan gangguan atau pencurian oleh pihak-pihak yang tidak bertanggung jawab.

Dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS dan pesan yang dikirimkan perlu pengamanan yang ekstra lebih untuk menghindari terjadinya pencurian atau pengeditan isi pesan sebelum sampai kepenerima pesan, karena isi pesan yang bersifat *plainteks* (teks-terang) dapat dibaca oleh siapa saja, untuk mengurangi resiko yang ditimbulkan dari kelemahan yang terdapat pada layanan SMS tersebut salah satu cara penanggulangannya adalah dengan menerapkan suatu algoritma Camellia pada pesan yang dikirimkan. Dengan terenkripsinya pesan yang di kirim maka seseorang yang berhasil mencuri informasi pesan teks yang dikirim tersebut akan kesulitan untuk mengetahui isi dari pesan tersebut.

Berdasarkan penelitian sebelumnya yang dilakukan Budi Rahardjo, menyatakan bahwa ketika kita berbicara tentang keamanan informasi, maka yang kita bicarakan adalah tiga hal: Kerahasiaan dan keamanan (*Confidentiality)*, data tidak boleh berubah (*Integrity*), dan dapat diakses ketika dibutuhkan (*Availability*). Ketiganya sering disebut dengan istilah CIA, yang merupakan gabungan huruf depan dari kata-kata tersebut. Selain ketiga hal tersebut ,masih ada aspek keamanan lainnya [1].

Kriptografi (*cryptography*) berasal dari dua kata dalam Bahasa Yunani, yaitu "*cryptos*" yang berarti rahasia, dan "*graphein*" yang berarti tulisan.Kriptografi adalah ilmu mempelajari teknik-teknik matematika. Dalam kriptpgrafi, banyak metode yang dapat digunakan untuk mengamankan data. Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun yang menjadi penghalang utama dalam memilih metode kriptografi yang cocok adalah bagaimana mengetahui dan memahami cara kerja algoritma dan metode kriptografi tersebut [2]. Salah satu metode kriptografi yang ada adalah metode Camellia. Camellia dikembangkan oleh NTT (Nippon Telegraph and Telephone Corporation) dan Mitsubishi Electric Corporation pada tahun 2000. Camellia merupakan *block cipher* yang dirancang oleh ahli-ahli dalam riset dan pengembangan dalam teknik kriptografik. Camellia mempunyai *interface* yang sama dengan *Advanced Encrytion Standard* (AES). Algoritma enkripsi dan dekripsi Camellia diputar dengan menggunakan *secret key* yang panjang 128/192/256-bit dan dengan blok data sebesar 128-bit [3].

2. METODOLOGI PENELITIAN

2.1 SMS *(Short Message Service)*

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

Short Message Service (SMS) merupakan sebuah layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel, memungkinkan dilakukannya pengiriman pesan dalam bentuk *alphanumeric* antara terminal pelanggan atau antara terminal pelanggan dengan sistem ekternal seperti *email, paging, voice mail* dan lain lain. Disebut pesan teks pendek karena pesan yang dikirimkan hanya berupa karakter [9].

2.2 Kriptografi

Kriptografi adalah ilmu mengenai teknik *enkripsi* dimana data diacak menggunakan suatu kunci *dekripsi. Dekripsi* menggunakan kunci dekripsi mendapatkan kembali data asli. Proses *enkripsi* dilakukan menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan *enkripsi* yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi itulah yan harus dirahasiakan (parameter menjadi *ekuivalen* dengan kunci) [12].

2.3 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*) [14].

Algoritma Camellia pada umumnya digunakan untuk pengamanan jaringan Algoritma Camellia juga memiliki tingkat keamanan yang tinggi. Algoritma ini memiliki keistimewaan yang berbeda dari algoritma lainnya, yang mana algoritma Camellia memiliki variasi kunci yang banyak mulai dari yang berukuran paling kecil 128 bit, 192 bit dan 256 bit sebagai variasi kunci terbesar [15].

Algoritma Camellia menggunakan struktur Feistel dengan 18-*round* untuk kunci 128-bit, dan struktur Feistel dengan 24-*round* untuk kunci 192-dan 256-bit, dengan tambahan *input*/*outputwhitenings* dan fungsi-fungsi logis yang disebut fungsi FL dan FL $^{-1}$. Fungsi FL dimasukkan disetiap 6 putaran yaitu sebelum lanjut putaran ketujuh dan ketigabelas.

Adapun langkah-langkah penjadwalan kunci pada algoritma Camellia [15] sebagai berikut:

1. Kunci masukkan dibagi menjadi dua bagian variabel, yaitu K_L dan K_R. Masing-masing variabel berukuran 128 bit. Khusus kunci berukuran 128 bit, K_R=0.
2. Variabel K_L dan K_R di-XORkan, kemudian dienkripsikan dengan nilai konstanta $\sum_1$ dan $\sum_2$.
3. Hasil enkripsi sebelumnya di-XOR kan dengan K_L dan kemudian diekripsikan dengan nilai konstanta $\sum_3$ dan $\sum_4$. Hasil dari enkripsi ini adalah K_A.
4. Kemudian K_A di-XOR dengan K_R dan kemudian diekripsikan dengan nilai konstanta $\sum_5$ dan $\sum_6$.Hasil dari enkripsi ini adalah K_B.

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Ketika SMS dikirimkan, SMS tidak akan langsung terkirim kenomor tujuan, namun akan masuk terlebih dahulu ke Short Message Service Center (SMSC) yaitu operator telepon yang anda gunakan. SMSC sendiri dapat diartikan sebagai sebuah server yang bertanggung jawab pada proses pengiriman SMS dalam suatu operator. SMS yang dikirimkan dari suatu ponsel akan masuk kedalam SMSC ini, Kemudian baru diteruskan kenomor tujuan SMS tersebut. Bila nomor yang dituju ternyata sedang mati/*offline*, SMSC ini akan menyimpan SMS ini untuk sementara waktu, hingga nomor tujuan tersebut hidup kembali. Nomor yang telah menerima SMS akan mengirimkan laporan ke SMSC bahwa SMS telah diterima. Laporan tersebut kemudian akan diteruskan lagi kenomor pengirim SMS, dalam proses pengiriman pesan yang dikirim adalah teks yang sudah tersandikan yang disebut *ciphertext*. *Ciphertext* merupakan hasil dari enkripsi dengan menggunakan algoritma Camellia.Sebelum pesan sampai kepenerima, pesan harus melewati SMSC terdahulu, dengan terjadinya proses enkripsi pada pesan ini, maka pesan tidak akan bisa dibacaoleh operator karena pesan sudah tersandikan.

3.2 Penerapan Algoritma Camellia

Tahap ini merupakan proses penerapan penyandian teks dengan menggunakan kunci 128 bit.
Plaintext : Budi Darma Medan
Kunci : Halimah-AniHTB18

1. Kunci masukkan dibagi menjadi dua bagian variabel, yaitu $K_L$dan K_R. Masing-masing variable berukuran 128 bit. Khusus kunci berukuran 128 bit, K_R=0.
2. Variabel $K_L$dan K_R di-XOR kan, kemudian dienkripsikan dengan nilai konstanta $\sum_1$dan $\sum_2$.
3. Hasil enkripsi sebelumnya di-XOR kan dengan K_L dan kemudian diekripsikan dengan nilai konstanta $\sum_3$ dan $\sum_4$. Hasil dari enkripsi ini adalah K_A.
4. Kemudian K_A di-XOR dengan K_R dan kemudian diekripsikan dengan nilai konstanta $\sum_5$ dan $\sum_6$. Hasil dari enkripsi ini adalah K_B.

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

Tabel 1. Kunci Algoritma Camellia

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

Key = Halimah-AniHTB18
= 4861 6C69 6D61 682D 416E 6948 5442 3138

1. Penjadwalan Kunci
   a. K_L= 4861 6C69 6D61 682D 416E 6948 5442 3138
   KL_L = 4861 6C69 6D61 682D
   KL_R = 416E 6948 5442 3138
   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 = $KL_L \oplus \sum_1$
=4861 6C69 6D61 682D$\oplus$ A09E 6673 FBCC 908B
= E8FF 0A1A 96AD F8A6

P(S($A_{8(8)}$))	= E8	=S_1(232)	=54
P(S($A_{7(8)}$))	= FF	=S_4(255)	=158
P(S($A_{6(8)}$))	= 0A	=S_3(10)	=171
P(S($A_{5(8)}$))	= 1A	=S_2(26)	=158
P(S($A_{4(8)}$))	= 96	=S_4(150)	=197
P(S($A_{3(8)}$))	= AD	=S_3(173)	=191
P(S($A_{2(8)}$))	= F8	=S_2(248)	=42
P(S($A_{1(8)}$))	= A6	=S_1(166)	=144

A =369E AB9E C5BF 2A90
A’ = **A** $\oplus$ KL_R
=369E AB9E C5BF 2A90$\oplus$416E 6948 5442 3138
= 77F0 C2D6 91FD 1BA8

B = A’$\oplus\sum_2$
= 77F0 C2D6 91FD 1BA8$\oplus$B67A E858 4CAA 73B2
= C18A 2A8E DD57 681A

P(S($B_{8(8)}$))	=C1	=S_1(193)	=121
P(S($B_{7(8)}$))	= 8A	=S_4(138)	=25
P(S($B_{6(8)}$))	= 2A	=S_3(42)	=110
P(S($B_{5(8)}$))	= 8E	=S_2(142)	=200
P(S($B_{4(8)}$))	= DD	=S_4(221)	=75
P(S($B_{3(8)}$))	= 57	=S_3(87)	=130
P(S($B_{2(8)}$))	= 68	=S_2(104)	=100
P(S($B_{1(8)}$))	= 1A	=S_1(26)	=79

B =7919 6EC8 4B82 644F
B’ =**B**$\oplus$ KL_L
=7919 6EC8 4B82 644F$\oplus$4861 6C69 6D61 682D
= 3178 02A1 26E3 0C62
B’$\oplus$ KL_L = B
A’$\oplus$ KL_R = A

C =P(S(B$\oplus\sum_3$))
=7919 6EC8 4B82 644F$\oplus$C6EF 372F E94F 82BE
= BFF6 59E7 A2CD E6F1

P(S($B_{8(8)}$))	= BF	=S_1(191)	=46

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

$P(S(B_{7(8)}))$ = F6 $=S_4(246)$ =56
$P(S(B_{6(8)}))$ = 59 $=S_3(89)$ =219
$P(S(B_{5(8)}))$ = E7 $=S_2(231)$ =20
$P(S(B_{4(8)}))$ = A2 $=S_4(162)$ =204
$P(S(B_{3(8)}))$ = CD $=S_3(205)$ =254
$P(S(B_{2(8)}))$ = E6 $=S_2(230)$ =89
$P(S(B_{1(8)}))$ = F1 $=S_1(241)$ =40

C = 2E38 DB14 CCFE 5928
C' =**C**⊕ A
=2E38 DB14 CCFE 5928⊕369E AB9E C5BF 2A90
= 18A6 708A 0941 73B8

D $=P(S(C' \oplus \sum_4))$
=18A6 708A 0941 73B8⊕54FF 53A5 F1D3 6F1C
= 4C59 232F F892 1CA4

$P(S(B_{8(8)}))$ = 4C $=S_1(76)$ =240
$P(S(B_{7(8)}))$ = 59 $=S_4(89)$ =216
$P(S(B_{6(8)}))$ = 23 $=S_3(35)$ =199
$P(S(B_{5(8)}))$ = 2F $=S_2(47)$ =52
$P(S(B_{4(8)}))$ = F8 $=S_4(248)$ =40
$P(S(B_{3(8)}))$ = 92 $=S_3(146)$ =0
$P(S(B_{2(8)}))$ = 1C $=S_2(28)$ =58
$P(S(B_{1(8)}))$ = A4 $=S_1(164)$ =205

D = F0D8 C734 2800 3ACD
D' =**D**⊕ B
= F0D8 C734 2800 3ACD⊕7919 6EC8 4B82 644F
= 89C1 A9FC 6382 5E82
K_A = C' || D'
K_A =18A6 708A 0941 73B8 89C1 A9FC 6382 5E82

Tabel 2. Hasil Tabel Kunci

	Sub kunci	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	$Kw_{3(64)}$	$(KA<<<111)_{L(64)}$
	$Kw_{4(64)}$	$(KA<<<111)_{R(64)}$

$Kw_{1(64)}$ = $(KL <<< 0)_{L(64)}$ =4861 6C69 6D61 682D
$Kw_{2(64)}$ = $(KL <<< 0)_{R(64)}$ =L9
$k_{1(64)}$ = $(KA <<< 0)_{L(64)}$ =**18A6 708A 0941 73B8**

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

$k_{2(64)}$ = $(KA <<< 0)_{R(64)}$ =**89C1 A9FC 6382 5E82**
$k_{3(64)}$ = $(KL <<< 15)_{L(64)}$ =B634 B6B0 B416 A0B7
$k_{4(64)}$ = $(KL <<< 15)_{R(64)}$ =34A4 2A21 189C 2430
$k_{5(64)}$ = $(KA <<< 15)_{L(64)}$ = 3845 04A0 B9DC 44E0
$k_{6(64)}$ = $(KA <<< 15)_{R(64)}$ = D4FE 31C1 2F41 0C53
$kl_{1(64)}$ = $(KA <<< 30)_{L(64)}$ = 8250 5CEE 2270 6A7F
$kl_{2(64)}$ = $(KA <<< 30)_{R(64)}$ = 18E0 97A0 8629 9C22
$k_{7(64)}$ = $(KL <<< 45)_{L(64)}$ = 2D05 A82D CD29 0A88
$k_{8(64)}$ = $(KL <<< 45)_{R(64)}$ = 4627 090C 2D8D 2DAC
$k_{9(64)}$ = $(KA <<< 45)_{L(64)}$ = 2E77 1138 353F 8C70
$k_{10(64)}$ = $(KL <<< 60)_{R(64)}$ = 8486 16C6 96D6 1682
$k_{11(64)}$ = $(KA <<< 60)_{L(64)}$ = 889C 1A9F C638 25E8
$k_{12(64)}$ = $(KA <<< 60)_{R(64)}$ = 218A 6708 A094 173B
$kl_{3(64)}$ = $(KL <<< 77)_{L(64)}$ = CD29 0A88 4627 090C
$kl_{4(64)}$ = $(KL <<< 77)_{R(64)}$ = 2D8D 2DAC 2D05 A82D
$k_{13(64)}$ = $(KL <<< 94)_{L(64)}$ = 1510 8C4E 1218 5B1A
$k_{14(64)}$ = $(KL <<< 94)_{R(64)}$ = 5B58 5A0B 505B 9A52
$k_{15(64)}$ = $(KA <<< 94)_{L(64)}$ = 18E0 97A0 8629 9C22
$k_{16(64)}$ = $(KA <<< 94)_{R(64)}$ = 8250 5CEE 2270 6A7F
$k_{17(64)}$ = $(KL <<< 111)_{L(64)}$ = 189C 2430 B634 B6B0
$k_{18(64)}$ = $(KL <<< 111)_{R(64)}$ = B416 A0B7 34A4 2A21
$Kw_{3(64)}$ = $(KA <<< 111)_{L(64)}$ = 2F41 0C53 3845 04A0
$Kw_{4(64)}$ = $(KA <<< 111)_{R(64)}$ = B9DC 44E0 D4FE 31C1

1. Proses Enkripsi

Plaintext = Budi Darma Medan
$M_{(128)}$ = 4275 6469 2044 6172 6D61 204D 6564 616E

a. $M_{L(64)}$ = 4275 6469 2044 6172
$M_{R(64)}$ = 6D61 204D 6564 616E
L_0 = $M_{L(64)} \oplus kw_1$
= 4275 6469 2044 6172 ⊕4861 6C69 6D61 682D
=0A14 0800 4D25 095F
R_0 = $M_{R(64)} \oplus kw_2$
= 6D61 204D 6564 616E⊕416E 6948 5442 3138
=2C0F 4905 3126 5056

b. Round →1

L_1 = $R_0 \oplus F(L_0, k_1)$
R_1 = L_0
L_1 = $R_0 \oplus F(L_0, k_1)$
= 2C0F 4905 3126 5056⊕F (L_0, k_1)
R_1 = 0A14 0800 4D25 095F
k_1 = 18A6 708A 0941 73B8

$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)}$ = P(S ($X_{(64)} \oplus k_{(64)}$))

P(S($X_{8(8)} \oplus k_{1(8)}$))	**=0A⊕18**	= 12	= P(S_1(18))	= Y(107)
P(S($X_{7(8)} \oplus k_{1(8)}$))	**=14 ⊕ A6**	=B2	= P(S_4(178))	= Y(27)
P(S($X_{6(8)} \oplus k_{1(8)}$))	**= 08⊕70**	= 78	= P(S_3(120))	= Y(18)
P(S($X_{5(8)} \oplus k_{1(8)}$))	**= 00 ⊕8A**	= 8A	= P(S_2(138))	= Y(60)
P(S($X_{4(8)} \oplus k_{1(8)}$))	**= 4D⊕09**	= 44	= P(S_4(68))	= Y(84)
P(S($X_{3(8)} \oplus k_{1(8)}$))	**= 25⊕41**	= 64	= P(S_3(100))	= Y(111)
P(S($X_{2(8)} \oplus k_{1(8)}$))	**= 09⊕73**	= 7A	= P(S_2(122))	= Y(209)
P(S($X_{1(8)} \oplus k_{1(8)}$))	**= 5F⊕B8**	= E7	= P(S_1(231))	= Y(10)

z'_1= z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	**=10⊕111⊕84⊕18⊕27⊕107**	**=83**
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	**=10⊕209⊕84⊕60⊕27⊕107**	**=195**
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	**=10⊕209⊕111⊕60⊕18⊕107**	**=241**
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	**=209⊕111⊕84⊕60⊕18⊕27**	**=223**
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	**=10⊕209⊕18⊕27⊕107**	**=185**
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	**=209⊕111⊕60⊕27⊕107**	**=242**
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	**=111⊕84⊕60⊕18⊕107**	**=126**
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	**=10⊕84⊕60⊕18⊕27**	**=107**

$z'_{(64)}$ = 53C3 F1DF B9F2 7E6B

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

$L_1 = R_0 \oplus F(L_0, k_1)$
$= 2C0F\ 4905\ 3126\ 5056V \oplus \mathbf{53C3\ F1DF\ B9F2\ 7E6B}$
$= 7FCC\ B8DA\ 88D4\ 2E3D$
$R_1 = \mathbf{0A14\ 0800\ 4D25\ 095F}$

c. Round →2

$L_2 = R_1 \oplus F(L_1, k_2)$
$R_2 = L_1$
$L_2 = R_1 \oplus F(L_1, k_2)$
$= \mathbf{0A14\ 0800\ 4D25\ 095F} \oplus F(L_1, k_2)$
$R_2 = 7FCC\ B8DA\ 88D4\ 2E3D$
$k_2 = \mathbf{89C1\ A9FC\ 6382\ 5E82}$

$\mathbf{(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))}$
$X_{(64)} \oplus k_{2(64)} = 7FCC\ B8DA\ 88D4\ 2E3D \oplus \mathbf{89C1\ A9FC\ 6382\ 5E82}$
$= \mathbf{F60D\ 1126\ EB56\ 70BF}$

$\mathbf{P(S(X_{8(8)} \oplus k_{2(8)}))}$	=F6	$= P(S_1(246))$	$= Y(67)$
$\mathbf{P(S(X_{7(8)} \oplus k_{2(8)}))}$	= 0D	$= P(S_4(13))$	$= Y(79)$
$\mathbf{P(S(X_{6(8)} \oplus k_{2(8)}))}$	= 11	$= P(S_3(17))$	$= Y(247)$
$\mathbf{P(S(X_{5(8)} \oplus k_{2(8)}))}$	= 26	$= P(S_2(38))$	$= Y(62)$
$\mathbf{P(S(X_{4(8)} \oplus k_{2(8)}))}$	= EB	$= P(S_4(235))$	$= Y(186)$
$\mathbf{P(S(X_{3(8)} \oplus k_{2(8)}))}$	= 56	$= P(S_3(86))$	$= Y(59)$
$\mathbf{P(S(X_{2(8)} \oplus k_{2(8)}))}$	= 70	$= P(S_2(112))$	$= Y(253)$
$\mathbf{P(S(X_{1(8)} \oplus k_{2(8)}))}$	= BF	$= P(S_1(191))$	$= Y(46)$

$\mathbf{z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8}$	$\mathbf{=46 \oplus 59 \oplus 186 \oplus 247 \oplus 279 \oplus 67}$	**=268**
$\mathbf{z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8}$	$\mathbf{=46 \oplus 253 \oplus 186 \oplus 62 \oplus 79 \oplus 67}$	**=91**
$\mathbf{z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8}$	$\mathbf{=46 \oplus 253 \oplus 59 \oplus 62 \oplus 247 \oplus 67}$	**=98**
$\mathbf{z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7}$	$\mathbf{=253 \oplus 59 \oplus 186 \oplus 62 \oplus 247 \oplus 79}$	**=250**
$\mathbf{z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8}$	$\mathbf{=46 \oplus 253 \oplus 247 \oplus 79 \oplus 67}$	**=40**
$\mathbf{z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8}$	$\mathbf{=253 \oplus 59 \oplus 62 \oplus 79 \oplus 67}$	**=244**
$\mathbf{z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8}$	$\mathbf{=59 \oplus 186 \oplus 62 \oplus 247 \oplus 67}$	**=11**
$\mathbf{z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7}$	$\mathbf{=46 \oplus 186 \oplus 62 \oplus 247 \oplus 79}$	**=18**

$\mathbf{z'_{(64)} = 0C5B\ 62FA\ 28F4\ 0B12}$

$L_2 = R_1 \oplus F(L_1, k_2)$
$= \mathbf{0A14\ 0800\ 4D25\ 095F} \oplus \mathbf{0C5B\ 62FA\ 28F4\ 0B12}$
$= 064F\ 6AFA\ 65D1\ 024D$
$R_2 = 7FCC\ B8DA\ 88D4\ 2E3D$

d. Round→3

$L_3 = R_2 \oplus F(L_2, k_3)$
$R_3 = L_2$
$L_3 = R_2 \oplus F(L_2, k_3)$
$= 7FCC\ B8DA\ 88D4\ 2E3D \oplus F(L_2, k_3)$
$R_3 = 064F\ 6AFA\ 65D1\ 024D$
$k_3 = B634\ B6B0\ B416\ A0B7$
$\mathbf{(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))}$
$X_{(64)} \oplus k_{3(64)} = 064F\ 6AFA\ 65D1\ 024D \oplus B634\ B6B0\ B416\ A0B7$
$= \mathbf{B07B\ DC4A\ D1C7\ A2FA}$

$\mathbf{P(S(X_{8(8)} \oplus k_{2(8)}))}$	=B0	$= P(S_1(176))$	$= Y(82)$
$\mathbf{P(S(X_{7(8)} \oplus k_{2(8)}))}$	= 7B	$= P(S_4(123))$	$= Y(67)$
$\mathbf{P(S(X_{6(8)} \oplus k_{2(8)}))}$	= DC	$= P(S_3(220))$	$= Y(68)$
$\mathbf{P(S(X_{5(8)} \oplus k_{2(8)}))}$	= 4A	$= P(S_2(74))$	$= Y(86)$
$\mathbf{P(S(X_{4(8)} \oplus k_{2(8)}))}$	= D1	$= P(S_4(209))$	$= Y(2)$
$\mathbf{P(S(X_{3(8)} \oplus k_{2(8)}))}$	= C7	$= P(S_3(199))$	$= Y(71)$
$\mathbf{P(S(X_{2(8)} \oplus k_{2(8)}))}$	= A2	$= P(S_2(162))$	$= Y(7)$
$\mathbf{P(S(X_{1(8)} \oplus k_{2(8)}))}$	= FA	$= P(S_1(250))$	$= Y(173)$

$\mathbf{z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8}$	$\mathbf{=173 \oplus 71 \oplus 2 \oplus 68 \oplus 67 \oplus 82}$	**=189**
$\mathbf{z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8}$	$\mathbf{=173 \oplus 7 \oplus 2 \oplus 86 \oplus 67 \oplus 82}$	**=239**
$\mathbf{z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8}$	$\mathbf{=173 \oplus 7 \oplus 71 \oplus 86 \oplus 68 \oplus 82}$	**=173**
$\mathbf{z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7}$	$\mathbf{=7 \oplus 71 \oplus 2 \oplus 86 \oplus 68 \oplus 67}$	**=19**

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8 =173⊕7⊕68⊕67⊕82 =255
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8 =7⊕71⊕86⊕67⊕82 =7
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8 =71⊕2⊕86⊕68⊕82 =5
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7 =173⊕2⊕86⊕68⊕67 =254
$z'_{(64)}$ = BDEF AD13 FF07 05FE
L_3 = R_2 ⊕F(L_2, k_3)
= 7FCC B8DA 88D4 2E3D⊕**BDEF AD13 FF07 05FE**
= C223 15C9 77D3 2BC3
R_3 = 064F 6AFA 65D1 024D

e. Round→18
L_{18} = R_{17}⊕F(L_{17}, k_{18})
R_{18} = L_{17}
L_{18} = R_{17}⊕F(L_{17}, k_{18})
=3EAF B329 4BB4 6236⊕F (L_{17}, k_{18})
R_{18} = 30A9 C107 00F1 E4E5
k_{18} = B416 A0B7 34A4 2A21
($X_{(64)}$, $k_{(64)}$) →$Y_{(64)}$ = P(S ($X_{(64)}$⊕$k_{(64)}$))
$X_{(64)}$ ⊕$k_{18(64)}$ =30A9 C107 00F1 E4E5⊕B416 A0B7 34A4 2A21
= 84BF 61B0 3455 CEC4

P(S($X_{8(8)}$⊕$k_{2(8)}$) =84 = P(S_1(132)) = Y(161)
P(S($X_{7(8)}$⊕$k_{2(8)}$)) = BF = P(S_4(191)) = Y(80)
P(S($X_{6(8)}$⊕$k_{2(8)}$)) = 61 = P(S_3(97)) = Y(44)
P(S($X_{5(8)}$⊕$k_{2(8)}$)) = B0 = P(S_2(176)) = Y(164)
P(S($X_{4(8)}$⊕$k_{2(8)}$)) = 34 = P(S_4(52)) = Y(50)
P(S($X_{3(8)}$⊕$k_{2(8)}$)) = 55 = P(S_3(85)) = Y(63)
P(S($X_{2(8)}$⊕$k_{2(8)}$)) = CE = P(S_2(206)) = Y(105)
P(S($X_{1(8)}$⊕$k_{2(8)}$)) = C4 = P(S_1(196)) = Y(159)

z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8 =159⊕63⊕50⊕44⊕80⊕161 =79
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8 =159⊕105⊕50⊕164⊕80⊕161 =145
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8 =159⊕105⊕63⊕164⊕44⊕161 =224
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7 =105⊕63⊕50⊕164⊕44⊕80 =188
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8 =159⊕105⊕44⊕80⊕161 =43
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8 =105⊕63⊕164⊕80⊕161 =3
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8 =63⊕50⊕164⊕44⊕161 =36
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7 =159⊕50⊕164⊕44⊕80 =117
$z'_{(64)}$ = 4F91 E0BC 2B03 2475
L_{18} = R_{17}⊕F(L_{17}, k_{18})
= 3EAF B329 4BB4 6236⊕**4F91 E0BC 2B03 2475**
=713E 5395 60B7 4643
R_{18} = 30A9 C107 00F1 E4E5
$C_{(128)}$ =($R_{18(64)}$ || $L_{18(64)}$) ⊕($kw_{3(64)}$||$kw_{4(64)}$)
= ($R_{18(64)}$ ⊕$kw_{3(64)}$|| $L_{18(64)}$⊕$kw_{4(64)}$)
= (30A9 C107 00F1 E4E5⊕2F41 0C53 3845 04A0) ||
= (713E 5395 60B7 4643⊕B9DC 44E0 D4FE 31C1)
= 1FE8 CD54 38B4 E045C8E2 1775 B449 7782

2. Proses Dekripsi
Cipherteks =
$C_{(128)}$ = 1FE8 CD54 38B4 E045C8E2 1775 B449 7782
$C_{(128)}$⊕($kw_{3(64)}$||$kw_{4(64)}$) = $R_{18(64)}$||$L_{18(64)}$
1FE8 CD54 38B4 E045C8E2 1775 B449 7782⊕(2F41 0C53 3845 04A0||B9DC 44E0 D4FE 31C1)= 30A9 C107 00F1 E4E5||713E 5395 60B7 4643
$R_{18(64)}$ = 30A9 C107 00F1 E4E5
$L_{18(64)}$ = 713E 5395 60B7 4643

a. 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})
=713E 5395 60B7 4643⊕F (R_{18}, k_{18})

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

L_{17}= 30A9 C107 00F1 E4E5
k_{18} = B416 A0B7 34A4 2A21
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{18(64)}$ = 30A9 C107 00F1 E4E5 ⊕ B416 A0B7 34A4 2A21
= 84BF 61B0 3455 CEC4

$P(S(X_{8(8)} \oplus k_{2(8)})$	=84	= $P(S_1(132))$	= Y(161)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= BF	= $P(S_4(191))$	= Y(80)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= 61	= $P(S_3(97))$	= Y(44)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= B0	= $P(S_2(176))$	= Y(164)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= 34	= $P(S_4(52))$	= Y(50)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= 55	= $P(S_3(85))$	= Y(63)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= CE	= $P(S_2(206))$	= Y(105)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= C4	= $P(S_1(196))$	= Y(159)

z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	**=159⊕63⊕50⊕44 ⊕80⊕161**	**=79**
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	**=159⊕105⊕50⊕164⊕80⊕161**	**=145**
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	**=159⊕105⊕63⊕164⊕44⊕161**	**=224**
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	**=105⊕63⊕50⊕164⊕44⊕80**	**=188**
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	**=159⊕105⊕44⊕80⊕161**	**=43**
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	**=105⊕63⊕164⊕80⊕161**	**=3**
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	**=63⊕50⊕164⊕44⊕161**	**=36**
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	**=159⊕50⊕164⊕44⊕80**	**=117**

$z'_{(64)}$ = 4F91 E0BC 2B03 2475
$R_{17} = L_{18} \oplus F(R_{18}, k_{18})$
= 713E 5395 60B7 4643⊕**4F91 E0BC 2B03 2475**
= 3EAF B329 4BB4 6236
L_{17}= 30A9 C107 00F1 E4E5

b. Round →2
$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$
$L_{16} = R_{17}$
$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$
=30A9 C107 00F1 E4E5⊕F (R_{18}, k_{18})
L_{16}= 3EAF B329 4BB4 6236
k_{17} = 189C 2430 B634 B6B0
$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}))$
$X_{(64)} \oplus k_{17(64)}$ =3EAF B329 4BB4 6236⊕ 189C 2430 B634 B6B0
= 2633 9719 FD80 D486

$P(S(X_{8(8)} \oplus k_{2(8)})$	=26	= $P(S_1(38))$	= Y(31)
$P(S(X_{7(8)} \oplus k_{2(8)}))$	= 33	= $P(S_4(51))$	= Y(17)
$P(S(X_{6(8)} \oplus k_{2(8)}))$	= 97	= $P(S_3(151))$	= Y(237)
$P(S(X_{5(8)} \oplus k_{2(8)}))$	= 19	= $P(S_2(25))$	= Y(28)
$P(S(X_{4(8)} \oplus k_{2(8)}))$	= FD	= $P(S_4(253))$	= Y(244)
$P(S(X_{3(8)} \oplus k_{2(8)}))$	= 80	= $P(S_3(128))$	= Y(85)
$P(S(X_{2(8)} \oplus k_{2(8)}))$	= D4	= $P(S_2(212))$	= Y(207)
$P(S(X_{1(8)} \oplus k_{2(8)}))$	= 86	= $P(S_1(134))$	= Y(98)

z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	**=98⊕85⊕244⊕237 ⊕17⊕31**	**=32**
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	**=98⊕207⊕244⊕28⊕17⊕31**	**=75**
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	**=98⊕207⊕85⊕28⊕237⊕31**	**=22**
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	**=207⊕85⊕244⊕28⊕237⊕17**	**=142**
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	**=98⊕207⊕237⊕17⊕31**	**=78**
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	**=207⊕85⊕28⊕17⊕31**	**=136**
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	**=85⊕244⊕28⊕237⊕31**	**=79**
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	**=98⊕244⊕28⊕237⊕17**	**=118**

$z'_{(64)}$ = 204B 168E 4E88 4F76

$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$
= 30A9 C107 00F1 E4E5⊕**204B 168E 4E88 4F76**
= 10E2 D789 4E79 AB93
L_{16}= 3EAF B329 4BB4 6236

c. Round →3
$R_{15} = L_{16} \oplus F(R_{16}, k_{16})$
$L_{15} = R_{16}$

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

Journal of Information Sistem Research (JOSH)
Volume 2, No. 1, October 2020
ISSN 2686-228X (media online)
Hal: 61-70

R_{15}= L_{16}⊕F(R_{16}, k_{16})
=3EAF B329 4BB4 6236⊕F (R_{16}, k_{16})
L_{15}= 10E2 D789 4E79 AB93
k_{16} = 8250 5CEE 2270 6A7F
(X $_{(64)}$, k $_{(64)}$) →Y$_{(64)}$ = P(S (X $_{(64)}$⊕k $_{(64)}$))
$X_{(64)}$ ⊕$k_{16(64)}$ =10E2 D789 4E79 AB93⊕8250 5CEE 2270 6A7F
= 92B2 8B67 6C09 C1EC

P(S($X_{8(8)}$⊕$k_{2(8)}$)	=92	= P(S_1(146))	= Y(0)
P(S($X_{7(8)}$⊕$k_{2(8)}$))	= B2	= P(S_4(178))	= Y(27)
P(S($X_{6(8)}$⊕$k_{2(8)}$))	= 8B	= P(S_3(139))	= Y(202)
P(S($X_{5(8)}$⊕$k_{2(8)}$))	= 67	= P(S_2(103))	= Y(56)
P(S($X_{4(8)}$⊕$k_{2(8)}$))	= 6C	= P(S_4(108))	= Y(212)
P(S($X_{3(8)}$⊕$k_{2(8)}$))	= 09	= P(S_3(9))	= Y(194)
P(S($X_{2(8)}$⊕$k_{2(8)}$))	= C1	= P(S_2(193))	= Y(242)
P(S($X_{1(8)}$⊕$k_{2(8)}$))	= EC	= P(S_1(236))	= Y(60)

z'_1 = z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	**=60⊕194⊕212⊕202 ⊕27⊕0**	**=251**
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	**=60⊕242⊕212⊕56⊕27⊕0**	**=57**
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	**=60⊕242⊕194⊕56⊕202⊕0**	**=254**
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	**=242⊕194⊕212⊕56⊕202⊕27**	**=13**
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	**=60⊕242⊕202⊕27⊕0**	**=31**
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	**=242⊕194⊕56⊕27⊕0**	**=19**
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	**=194⊕212⊕56⊕202⊕0**	**=228**
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	**=60⊕212⊕56⊕202⊕27**	**=1**

$z'_{(64)}$ = FB39 FE0D 1F13 E401
R_{15}= L_{16}⊕F(R_{16}, k_{16})
=3EAF B329 4BB4 6236⊕**FB39 FE0D 1F13 E401**
= C596 4D24 54A7 8637
L_{15}= 10E2 D789 4E79 AB93

d. Round →18
R_0 = L_1⊕F(R_1, k_1)
L_0 = R_1
R_0 = L_1⊕F(R_1, k_1)
=7FCC B8DA 88D4 2E3D⊕F (R_1, k_1)
L_0 = 0A14 0800 4D25 095F
k_1 = 18A6 708A 0941 73B8
(X $_{(64)}$, k $_{(64)}$) →Y$_{(64)}$ = P(S (X $_{(64)}$⊕k $_{(64)}$))
$X_{(64)}$ ⊕$k_{18(64)}$ =0A14 0800 4D25 095F⊕ **18A6 708A 0941 73B8**
= 12B2 788A 4464 7AE7

P(S($X_{8(8)}$⊕$k_{1(8)}$))	= 12	= P(S_1(18))	= Y(107)
P(S($X_{7(8)}$⊕$k_{1(8)}$))	= B2	= P(S_4(178))	= Y(27)
P(S($X_{6(8)}$⊕$k_{1(8)}$))	= 78	= P(S_3(120))	= Y(18)
P(S($X_{5(8)}$⊕$k_{1(8)}$))	= 8A	= P(S_2(138))	= Y(60)
P(S($X_{4(8)}$⊕$k_{1(8)}$))	= 44	= P(S_4(68))	= Y(84)
P(S($X_{3(8)}$⊕$k_{1(8)}$))	= 64	= P(S_3(100))	= Y(111)
P(S($X_{2(8)}$⊕$k_{1(8)}$))	= 7A	= P(S_2(122))	= Y(209)
P(S($X_{1(8)}$⊕$k_{1(8)}$))	= E7	= P(S_1(231))	= Y(10)

z'_1= z1⊕z3⊕z4⊕z6⊕ z7⊕ z8	**=10⊕111⊕84⊕18⊕27⊕107**	**=83**
z'_2 = z1⊕z2⊕z4⊕z5⊕ z7⊕ z8	**=10⊕209⊕84⊕60⊕27⊕107**	**=195**
z'_3 = z1⊕z2⊕z3⊕z5⊕ z6⊕ z8	**=10⊕209⊕111⊕60⊕18⊕107**	**=241**
z'_4 = z2⊕z3⊕z4⊕z5⊕ z6⊕ z7	**=209⊕111⊕84⊕60⊕18⊕27**	**=223**
z'_5 = z1⊕z2⊕z6⊕ z7⊕ z8	**=10⊕209⊕18⊕27⊕107**	**=185**
z'_6 = z2⊕z3⊕z5⊕ z7⊕ z8	**=209⊕111⊕60⊕27⊕107**	**=242**
z'_7 = z3⊕z4⊕z5⊕ z6⊕ z8	**=111⊕84⊕60⊕18⊕107**	**=126**
z'_8 = z1⊕z4⊕z5⊕ z6⊕ z7	**=10⊕84⊕60⊕18⊕27**	**=107**

$z'_{(64)}$ = 53C3 F1DF B9F2 7E6B
R_0= L_1⊕F(R_1, k_1)
=7FCC B8DA 88D4 2E3D⊕**53C3 F1DF B9F2 7E6B**
= 2C0F 4905 3126 5056
L_0= 0A14 0800 4D25 095F
$Kw_{1(64)}$ = 4861 6C69 6D61 682D
$Kw_{2(64)}$ = 416E 6948 5442 3138

Submitted: **02/10/2020**; Accepted: **09/10/2020**; Published: **26/10/2020**

$M_{(128)}$ $=(L_{0(64)} \| R_{0(64)}) \oplus (kw_{1(64)} \| kw_{2(64)})$
$= (0A14\ 0800\ 4D25\ 095F \oplus 4861\ 6C69\ 6D61\ 682D) \|$
$(2C0F\ 4905\ 3126\ 5056 \oplus 416E\ 6948\ 5442\ 3138)$
$=4275\ 6469\ 2044\ 61726D61\ 204D\ 6564\ 616E$
= Budi Darma Medan

4. KESIMPULAN

Dengan adanya kesimpulan dan saran ini, maka dapatlah diambil suatu perbandingan yang akhirnya dapat memberikan perbaikan-perbaikan pada masa yang akan datang. Adapun kesimpulan yang peulis peroleh adalah sebagai berikut:

1. Algritma Camellia dapat di implementasikan pada aplikasi pengamanan pesan teks SMS.
2. Aplikasi ini dapat menyandikan isi teks SMS hanya capital saja agar informasi yang dikirim tidak dapat dibaca oleh orang lain.
3. Dengan menggunakan bahasa pemograman *Java* dan *eclipse* sebagai aplikasinya dapat membuat aplikasi pengamanan pesan teks menggunakan agoritma camellia.

REFERENCES

[1] BUDI RAHARDJO, keamanan informasi berbasis Internet. jakarta, 2002.
[2] Azanuddin, "Penyandian Short Message Service (SMS) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfeld," Pelita Informatika Budi Darma, vol. IV, p. 49, Agustus 2013.
[3] Leo Willyanto Santoso, Gregorius Satia Budhi, Lanny Susanto, "Perbandingan Aplikasi Menggunakan Metode Camellia 128 Bit Key Dan 256 Bit Key," Jurnal Informatika, vol. 12, pp. 113-130, November 2014.
[4] Budi Rahardjo, Keamanan Sistem Informasi Berbasis Internet. Jakarta, 2002.
[5] Cangara. (2013, mei) Defenisi Pesan Menurut Ahli. [Online]. http://defenisiahli.blogspot.co.id/2013/05/defenisi-pesan-menurut-ahli-html
[6] Luxemburg. (2016, Oktober) Pengertianmu.Com. [Online]. http://www.pengertianmu.com/2016/10/pengertian-teks-menurut-paraahli.html
[7] Iwan Binanto, Multimedia Digital-Dasar Teori Dan Pengembangannya. Yogyakarta, 2010.
[8] Yakub,Irwan Limiady Tri Puji Rahayu, "Aplikasi Enkripsi Pesan Teks(SMS) Pada Perangkat Handphone Dengan Algoritma Caesar Chiper," Sentika 2012, vol. 143, pp. 2089-9815, Maret 2012.
[9] Romzi Imron Rozidi, Membuat Sendiri SMS Gateway Berbasis Protocol SMPP., 2004.
[10] Dini Lestari Tresnani, "Kode Huffman Untuk Kompresi Sms," Program Studi Teknik Informatika, pp. 1-7, 2009.
[11] Dony Ariyus, Pengantar Ilmu Kriptografi Teori Analisis dan Informasi. Yogyakarta, 2008.
[12] Sentot Kromodimoejo, Teori dan Aplikasi Kriptografi.: SPK IT Consulting, 2010.
[13] Rinaldi Munir, Kritografi. Bandung: Informatika Bandungg, 2006.
[14] B. S. W. Poetro and R. Wardoyo, "Perbandingan Efisiensi, Efektifitas dan Kualiatas Algoritma Rijndael dengan Algoritma Camellia pada Citra Digital," J.Math.Nat.Sci, vol. 24, pp. 281-291, 2014.
[15] L. Susanto, G. S. Budhi, and L. W. Santoso, "Perbandingan Menggunakan Metode Camellia 128 Bit Key dan 256 Bit Key," J. Inform, vol. 12, pp. 109-116, 2014.
[16] K. Aoki et al, "Camelia A 128-Bit Block Cpiher Suitable for Multiple Platform-Design and Analysis Structure of Camelia," Springer-Verlag Berlin Heidelb , pp. 39-56, 2001.
[17] Ahmad Rifqi Hadiyanto, "Algoritma Kunci Simetris Camelia," EC-510, pp. 3-15, 2004.
[18] Nazruddin Safaat H, Pemograman Aplikasi Mobile Smartphone dan Tablet Pc Berbasis Android. Bandung, 2015.
[19] Yuniar Supardi, Semua Bisa Menjadi Programmer Java. Jakarta, 2010.
[20] Rosa A.S, M. Shalahuddin, Rekayasa Perangkat Lunak. Bandung, 2013.