Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2019
ISBN: 978-602-52720-1-1
Januari 2019
Hal: 898 - 902

Implementasi Algoritma Paillier Cryptosystem Pengamanan Audio

Juni Ade Nawer Purba, Debora Sinaga, Saima Ronita Purba

Prodi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338, Medan, Indonesia

Abstrak

Sistem keamanan data sangat dibutuhkan untuk meminimalisir penyalahgunaan data yang bersifat penting dan rahasia. Pemalsuan data menjadi salah satu permasalahan yang sering terjadi pada era teknologi saat ini terutama dalam kegiatan distribusi pesan, sehingga dibutuhkannya pengamanan yang sangat akurat. Salah satu jenis data yang umum digunakan sebagai media dalam bertukar infromasi adalah audio. Salah satu solusi yang dapat mengamankan permasalahan tersebut adalah mengimplementasikan algoritma *paillier cryptosystem* dalam pengamanan audio. Proses kerja dari metode *paillier* terdiri dari proses pembentukan kunci, proses enkripsi dan proses dekripsi. Proses pembentukan kunci akan menghasilkan kunci *privat* dan kunci *public*. Kunci *privat* pada algoritma ini digunakan untuk proses enkripsi dan kunci *public* digunakan untuk melakukan proses dekripsi. Implementasi algoritma ini dapat meminimalisir tindakan-tindakan penyalagunaan atau tindakan untuk memanipulasi audio.

Kata Kunci: Kriptografi, Paillier Cryptosystem, Enkripsi, Dekripsi, Audio

1. PENDAHULUAN

Keamanan informasi merupakan hal yang sangat penting. Informasi yang sudah dirahasiakan tidak boleh diberitahu ke publik atau kepada orang yang tidak berkepentingan dalam informasi tersebut. Jika hal itu terjadi maka akan merugikan suatu pihak atau negara. Salah satunya adalah audio. Audio yang bersifat rahasia perlu dijaga keasliannya dan keutuhannya bila ingin dikirim karena data tersebut dapat disadap dan diketahui oleh pihak ketiga selama proses pengiriman. Berdasarkan penelitian sebelumnya mengungkapkan bahwa untuk mengirimkan data yang bersifat penting maupun rahasia perlu dilakukan pengamanan agar tidak diketahui oleh pihak ketiga[1][2].

Algoritma *paillier cryptosystem* merupakan salah satu algoritma *privat key dan public key* yang populer dipakai dan bahkan hingga saat ini algoritma *paillier cryptosystem* masih dianggap aman karena *public key* akan digunakan pada proses enkripsi dan *privat key* digunakan pada proses dekripsi[3]. Sekuritas dari algoritma *Paillier* ini bergantung pada problema perhitungan n-*residue class* yang dipercaya sangat sulit untuk dikomputasi. Problema ini dikenal dengan asumsi *Composite Residuosity* (CR) dan merupakan dasar dari kriptosistem *Paillier* ini.

Skema ini merupakan *additive homomorphic cryptosystem*, yang berarti bahwa diberikan kunci publik dan enkripsi dari m_1 dan m_2, seseorang akan mampu menghitung enkripsi dari m_1 yang digabungkan dengan m_2. Enkripsi *probabilistic*, menyebabkan seorang *crypanalyst* tidak dapat lagi mengenkripsi *plaintext* acak untuk mencari *ciphertext* yang benar. Penelitian ini menguraikan bagaimana proses penerapan algoritma *paillier cryptosystem* untuk mengamankan pesan penting berjenis audio.

Tabel 1. Penelitian Terkait

No	Penulis	Judul	Kesimpulan
1	Kristoforus Jawa Bendi dan Titus Andika Rizki	Sistem Kriptografi DES pada Media Audio [4]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa perlunya penerapan teknik kriptografi untuk mengamankan komunikasi dalam bentuk audio, sehingga informasi yang ada di dalam audio dapat terjaga dengan baik
2	Utami Putri Setyaningrum	Algoritma Paillier Cryptosystem Untuk Mengamankan Citra Digital[5]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa keamanan yang diberikan oleh *paillier cryptosystem* berdasarkan hasil histogram dan analisis menghasilkan koefisien korelasi cukup baik
3	Aji Setiyo Sukarno dan Theresia Natalia	Pemanfaatan Paillier Cryptosystem untuk Low Cost Secure Direct-Recording Electronic (DRE)[6]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa implementasi algoritma paillier dapat menjaga otentikasi dan mencegah manipulasi data asli.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (*cryptography*) berarti *secret writing* (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat dan mata-mata. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *nonrepudiation*[7][8].

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 898 - 902

2.2 Audio

File audio adalah suara atau getaran yang dihasilkan oleh getaran suatu benda. Audio terbentuk melalui beberapa tahap pengambilan atau penangkapan suara, sambungan transmisi yang membawa bunyi, ampilifer dan lain-lain[9]**.** Agar dapat didengar telinga manusia ,getaran tersebut harus cukup kuat yaitu minimal 20 kali per detik. Bila kurang dari jumlah tersebut, telinga manusia tidak akan mendengarnya sebagai suatu bunyi. Banyaknnya getaran suatu benda diukur dengan satuan *cycles per second* atau cps. Pengukuran ini dikenal dengan sebutan Hertz (Hz). Daya tangkap pendengaran manusia secara teoritis adalah mulai dari 20Hz sampai 20 kHz. File audio disebut juga merupakan salah satu elemen yang penting, karena ikut berperan dalam membangun sebuah sistem komunikasi dalam bentuk suara, ilah suatu sinyal elektrik yang akan membawa unsur unsur bunyi didalamnya.

2.3 Algoritma Paillier Cryptosystem

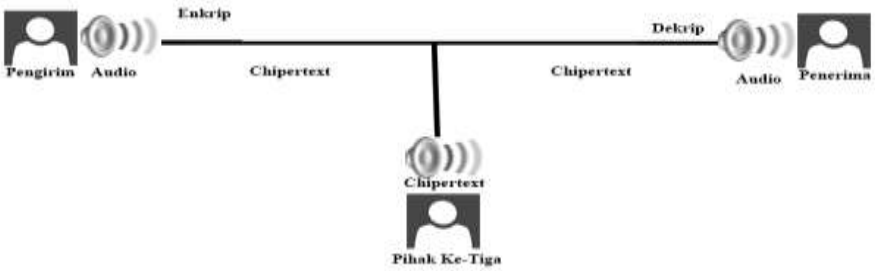
Paillier Cryptosystem yang ditemukan oleh Pascal Paillier pada tahun 1999 yang merupakan sebuah sistem yang berbasis algoritma asimetris probabilistikgrafi untuk kriptografi kunci publik. Sekuritas dari algoritma *paillier* ini bergantung pada problema perhitungan n-residuue class yang dipercaya sangat sulit untuk komputasi. Algoritma enkripsi yang digunakan adalah sebuah algoritma kriptografi kunci publik. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis.

Paillier adalah jenis kriptografi berbasis *keypair* .Berarti setiap pengguna mendapatkan kunci publik dan pribadi, dan pesan yang dienkripsi dengan kunci publik mereka hanya dapat didekripsi dengan kunci pribadi mereka. *Paillier* tidak banyak digunakan sebagai algoritma lain seperti RSA, dan ada beberapa implementasi yang tersedia secara *online*. Kelebihan dari *paillier cryptsystem* tidak seperti banyak *cryptosystem* lainnya *keypair*, *paillier* menyediakan *homomorfisme aditif*. Ini berarti bahwa pesan dapat ditambahkan bersama ketika dienkripsi, dan pihak lain tidak akan mendekripsi dengan benar. Khususnya, bila pengirim memiliki dua pesan (x dan y) yang dienkripsi dengan kunci publik penerima (membuat cx dan cy), maka pengirim dapat menambahkannya bersama-sama dan mengirimkannya ke penerima. Ketika penerima mendekripsi pesannya, penerima akan mendapatkan hasil x + y [3][5][6].

3. ANALISA DAN PEMBAHASAN

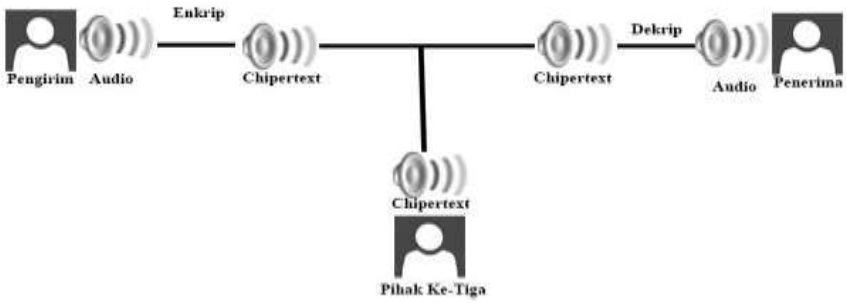
3.1 Analisis

Permasalahan dalam penelitian ini adalah implementasi algoritma *paillier cryptosystem* untuk mengamankan audio dengan ekstensi mp3. Pengamanan ini dilakukan karena mudahnya pengaksesan pada audio oleh semua orang, sehingga rentan terhadap manipulasi *value* ataupun informasi dari audio. Kerentanan yang dimaksud adalah dalam pendistribusian atau dalam perjalanan dari pengirim kepada penerima, ilustrasi dapat dilihat pada pada gambar 1.



Gambar 1. Ilustrasi Pengiriman Tanpa Enkripsi

Pengenkripsian atau pengamanan dilakukan karena data tersebut bersifat sangat rahasia, sehingga harus tahan terhadap pembajakan oleh pihak ketiga. Algoritma *paillier cryptosystem* merupakan salah satu metode pengamanan kriptografi dalam menyelesaikan masalah pembajakan tersebut, hal tersebut dapat digambarkan pada gambar 2.



Gambar 2. Ilustrasi Pengiriman Setelah Enkripsi

Agar kemampuan maksimal yang dihasilkan dalam menerapkan algoritma *paillier cryptosystem*, maka dilakukan pengujian enkripsi dan dekripsi dengan melakukan pencobaan terhadap data yang tertera di bawah ini. pengkodean pada audio dilakukan terlebih dahulu agar memudahkan dalam pengujian. Berikut adalah nilai bit dari audio:

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 898 - 902

3.2 Pembahasan

Penelitian ini menggunakan algoritma *paillier cryptosystem* yang berkonsep *symmetric cryptosystem*. *Symmetric cryptosystem* sangat mengedepankan kerahasiaan kunci untuk enkripsi dan dekripsi. Proses enkripsi terhadap audio dengan format mp3 dapat dilakukan dengan melakukan langkah-langkah berikut :

1. Mengambil nilai hexadesimal dari audio.
   49 6E 66 6F 0F 01 FB 03 3D 62 00 03 06 08 0B 0D 10 12 15 17 1A 1C 1F 21 24 26 29 2C 2E 31 33 36 38 3B 3D 40 42 45 47 4A 4C 4F 51 54 57 59 5C 5E 61 63 67 69 6C 6E 71 73 76 78 7B 7D 80 83 85 88 8A 8D 8F 92 94 97 99 9C 9E A1 A3 A6 A8 AB AE B0 B3 B5 B8 BA BD BF C2 C4 C7 C9 CD CF D2 D4 D7 DA DC DF E1 E4 E6 E9 EB EE F0 F3 F5 F8 FA FD 00 00 00 39 4C 41 4D 45 33 2E 39 37 20 01 AA 00 00 00 00 2E 5E 00 00 14 80 24 06 C0 4E 00 00 80 00 03 3D 62 2A 50 40 28 00 00 00 00 00 00 00 00 68 2C 08 B8 61 74 A8 6B E0 41 E9 87 05 9F FF FC 91 8F EE EA 15 17 0F FF FF FF A4 00 62 00 07 D5 69 87 00 61 81 38 27 98 88 24 C1 C5 90 9A 98 1C 0A B9 A3 45 C7 99 D8 8A 99 85 0A 40 19 03 25 E9 82 50 57 18 0C 8F 79 30 10 90 80 28 D1 A6 07 0C 69 DB 32 FA 2B E1 37 28 2F F8 13 F8 63 46 73 4D 63 93 24 22 06 97 CB AA D3 CB BF EA EA 81 7D BB B7 A0 0F 0D DF DB 40 44 4D 43 25 07 93 CE 2C CA 94 B7 7B F9 7D E7 16 AC 01 80 29 AC C3 6B 04 61 AA 27 BE 16 18 16 6A 78 C1 C7 82 05 53 9F C3 61 57 4A 41 B5 22 D8 10 4C E5 02 50 DD FF FF FF FF F6 57 FF FB D1 74 33 94 AA D1 15 01 90 03 00 5C 02 A1 10 08 A6 00 08 10 C0 80 4F CC 08 E3 D0 8C 60 21 46 CC 09 90 EA 8C 89 C5 E4 8C 36 30 54 8C 23 B0 AE 0D 5B 30 FC 4C 36 30 2C 0C 15 60 DF CA 04 37 30 1A 80 05 32 72 22 22 D1 E1 74 B7 2A 00 1C 07 FD 3D 77 ED F4 2C E9 9C 2B 86 A6 8A 80 50 FF 5F 45 0A 22 EE 64 D4 30 0C CD 8E 4A 57 E3 C6 60 E0 94 FF FB 92 64 D7 0C C3 A3 32 49 13 DC 5A E0 31 61 C8 F2 6C EC 64 0D A0 C9 24 6F 69 4 EF EB 7D EE 6E 93 9B 83 E6 2F D8 45 36 2D 33 74 93 41 1B 14 25 B0 A2 EF 2F 5E A6 B7 36 F9 97 5C 49 CF 24 B4 AA 99 12 34 C4 CA ED 3C A5 00 2C 20 01 29 5A 6D 25 62 7B AC F7
4. Pengenkripsian dilakukan pada masing-masing nilai bit hexadesimal audio
3. Setelah setiap bagian bit di enkripsi, maka kemudian menyatukan kembali hasil bit decimal sehingga akan menhasilkan audio yang telah terenkripsi.

3.2.1 Proses Enkripsi

Proses enkripsi dari metode Paillier *cryptosystem* untuk file audio kita ambil 8 digit hexadesimal dari audio yang akan di enkripsi = ’ 49 6E 66 6F 0F 01 FB 03’ dapat dirincikan sebagai berikut:

Langkah 1 : Input File Audio

Pesan = 8
‘49’ = 73 = 01001001
‘6E’ = 110 = 01101110
‘66’ = 102 = 01100110
‘6F’ = 111 = 01101111
‘0F’ = 15 = 00001111
‘01’ = 01 = 00000001
‘FB’ = 251 = 11111011
‘03’ = 03 = 00000011

Langkah 2 : Kelompokkan pesan menjadi subblok bit Hitung nilai b sedemikian sehingga 2^b <= n, n = 2911 ; nilai b yang dipilih = 11.

M(1) = 01001001011 = 587
M(2) = 01110 011001= 921
M(3) = 10011011110 = 1246
M(4) = 00011110000 = 240
M(5) = 00011111101 = 253
M(6) = 10000001100 = 1036
M(7) = 10000001011 = 1035
M(8) = 10100101110 = 1326
M(9) = 00100000011 = 259
M(10) = 10011010011 = 1235
M(11) = 01010011011 = 667
M(12) = 10000100100 = 1060
M(13) = 11110100110 = 1958
M(14) = 00100111100 = 316
M(15) = 00111000001 = 449

Langkah 3 : Input nilai r, r = 87

Langkah 4 : Hitunglah nilai Ci

Temp2 = (r^n) mod n^2)
Temp2 = (87^2911 mod 8473921)

Cara Kerja :

2911 = 2048 + 512 + 256 + 64 + 16 + 8 + 4 + 2 + 1
Pangkat 1 : 87 mod 8473921 = 87 [*]
Pangkat 2 : 87 mod 8473921 = 7569 [*]
Pangkat 4 : 7569 mod 8473921 = 6446235 [*]

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 898 - 902

Pangkat 8 : 6446235 mod 8473921 = 1671182 [*]
Pangkat 16 : 1671182 mod 8473921 = 1936540 [*]
Pangkat 32 : 1936540 mod 8473921 = 3425713 [*]
Pangkat 64 : 3425713 mod 8473921 = 4739743[*]
Pangkat 128 : 4739743 mod 8473921 = 4284887
Pangkat 256 : 4284887 mod 8473921 = 4814690 [*]
Pangkat 512 : 4814690 mod 8473921 = 2814690 [*]
Pangkat 1024 : 8059468 mod 8473921 = 3910539
Pangkat 2048 : 4910539 mod 8473921 = 63672921[*]

Cara Kerja :
316 = 256 + 32 + 16 + 8 + 4
Pangkat 1 : 7481^2 mod 8473921 = 7481 [*]
Pangkat 2 : 7481^2 mod 8473921 = 5121835
Langkah 5 : Gabungkan semua nilai Ci menjadi cipher value
C(1) = 2389830 = 2389830
C(2) = 4006911 = 4006911
C(3) = 5236568 = 5236568
C(4) = 2325533 = 2325533
C(5) = 4663494 = 4663494
C(6) = 8201801 = 8201801
C(7) = 6283603 = 6283603
C(8) = 6035247 = 6035247
C(9) = 3861074 = 3861074
C(10) = 1280085 = 1280085
C(11) = 8397737 = 8397737
C(12) = 514784 = 0514784
C(13) = 4650977 = 4650977
C(14) = 4815123 = 4815123
C(15) = 7299551 = 7299551

Cipheraudio = 238983040069115236568232553346634948201801628360360352473861074128008583977370514784465097748151237299551

3.2.2 Proses Deskripsi

Proses dekripsi untuk cipher teks yang diperoleh pada proses enkripsi di atas dapat dirincikan sebagai berikut:
Langkah 1 : Input Cipher value
Cipheraudio = 238983040069115236568232553346634948201801628360360352473861074128008583977370514784465097748151237299551

Langkah 2 : Kelompokkan cipher value menjadi subblok
n^2 = 2911^2 = 8473921, jadi : B1 = 7
C(1) = 2389830 = 2389830
C(2) = 4006911 = 4006911
C(3) = 5236568 = 5236568
C(4) = 2325533 = 2325533
C(5) = 4663494 = 4663494
C(6) = 8201801 = 8201801
C(7) = 6283603 = 6283603
C(8) = 6035247 = 6035247
C(9) = 3861074 = 3861074
C(10) = 1280085 = 1280085

Langkah 3 : Hitung nilai Ui dan L(Ui)
U(1) = M(1)^h mod n^2
U(1) = 2389830^280 mod 8473921

Cara Kerja :
280 = 256 + 16 + 8
Pangkat 2 : 2389830^2 mod 8473921 = 257636
Pangkat 4 : 257636^2 mod 8473921 = 85303
Bit pesan yang diperoleh =
01001001,01101110,01100110,01101111,00001111,00000001,11111011,00000011001000000100110100101110001000000101001101001001010011010100001001001111010011000100111101001110000000

Langkah 4 : Gabungkan semua nilai Mi dan konversikan ke karakter

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 898 - 902

Bit pesan yang diperoleh =
01001001011011100110011001101111000011110000000111111011000000110010000001001101001011100010000000101001101001001011010000100100111101001100010011111010011100000
Karakter ke-1 = 01001001 = 73 = '49'
Karakter ke-2 = 01101110 = 110 = '6E'
Karakter ke-3 = 01100110 = 102 = 66'
Karakter ke-4 = 01101111 = 111 = '6F'
Karakter ke-5 = 00001111 = 15 = '0F'
Karakter ke-6 = 00000001 = 01 = '01'
Karakter ke-7 = 11111011 = 251 = 'FB'
Karakter ke-8 = 00000011 = 03 = '03'

4. KESIMPULAN

Berdasarkan hasil implementasi yang telah dilakukan, maka disimpulkan bahwa algoritma *paillier cryptosystem* dapat mengenkripsi audio, sehingga lebih meningkatkan keamanan dari audio itu sendiri dan menekan kemungkinan diambil oleh pihak ketiga. Algoritma *paillier cryptosystem* pada audio enkripsi sangat bergantung pada ukuran dari audio itu sendiri, semakin besar ukuran audio maka semakin lama pula waktu yang dibutuhkan untuk enkripsi.

REFERENCES

[1] R. Anderson, E. Biham, and L. Knudsen, "Serpent : A proposal for the advanced encryption standard," *NIST AES Propos.*, pp. 1–23, 1998.
[2] T. Zebua, "Pengamanan Data Teks Dengan Kombinasi Cipher Block Chaining dan LSB-1," in *Seminar Nasional Inovasi dan Teknologi (SNITI)*, 2015, pp. 85–89
[3] R. M. Simbolon, "Perancangan Perangkat Lunak Enkripsi Pesan Dengan Metode Paillier Cryptosystem," *Pelita Inform. Budi Darma*, vol. 5, no. 3, pp. 23–30, 2013.
[4] K. Jawa Bendi and T. Andika Rizki, "Sistem Kriptografi DES pada Media Audio," in *Seminar Nasional Teknologi Terapan SV UGM*, 2016, pp. 640–644.
[5] A. S. Sukarno and T. Natalia, "Pemanfaatan Paillier Cryptosystem untuk Low Cost Secure Direct-Recording Electronic (DRE)," *bptt*, 2014.
[6] U. P. Setyaningrum, "Algoritma Paillier Cryptosystem untuk Mengamankan Citra Digital," UNISSULA, 2017.
[7] D. Br Tarigan, K. Kunci, and K. Hill Cipher, "Implementasi Algoritma Kriptografi Hill Cipher Dalam Penyandian Data Gambar," no. 0911610, pp. 76–81, 2014.
[8] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," *J. Sains Komput. Inform.*, vol. 2, no. 1, pp. 12–22, 2018.
[9] H. Santoso and M. Fakhriza, "PERANCANGAN APLIKASI KEAMANAN FILE AUDIO FORMAT WAV (WAVEFORM) MENGGUNAKAN ALGORITMA RSA," vol. 6341, no. April, pp. 47–54, 2018.