Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2625

Perancangan Aplikasi Pengamanan File Menggunakan Algoritma Paillier Berbasis Android

Yazirwan

Fakultas Ilmu Komputer dan Teknologi Informasi, Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: yazirwanmz63@gmail.com
Submitted: **03/12/2020**; Accepted: **04/01/2021**; Published: **24/01/2021**

Abstrak–Masalah Keamanan dan kerahasiaan data merupakan salah satu aspek penting dalam hal pertukaran informasi. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada file adalah dengan teknik penyandian sebagai kunci enkripsi dan dekripsi.Penelitian ini memaparkan mengenai pengembangan kriptografi (enkripsi dan dekripsi) yang menerapkan algoritma Paillier. Tujuan Algoritma paillier dipilih karena merupakan dari algoritma caesar dimana algoritma paillier menggunakan dua kunci. Penelitian ini menghasilkan sebuah program aplikasi bertujuan untuk peningkatan keamanan file. Dalam pembuatan aplikasi ini, metode yang digunakan adalah Algoritma Paillier, karena sangat cocok untuk keamanan file yang menghasilkan penyelesian proses enkripsi dan deskripsi. Aplikasi ini dibuat dengan bahasa pemograman Android dan pembuatan aplikasi keamanan file dengan proses enkripsi dan deskripsi menggunakan algoritma Paillier, diharapkan untuk mengatasi permasalahan tersebut.

Kata Kunci: Kriptografi; File; Algoritma Paillier; Android

Abstract–Data security and confidentiality issues are one of the important aspects in terms of information exchange. One solution to maintaining the security and confidentiality of files is an encryption technique as an encryption and decryption key. This research describes the development of cryptography (encryption and decryption) that implements the Paillier algorithm. The purpose of Paul's algorithm was chosen because it is a Caesarean algorithm, where Paul's algorithm uses two keys. This research produces an application program that aims to increase file security. In making this application, the method used is Paillier's Algorithm, because it is very suitable for file security that results in completing encryption processes and descriptions. This application is made with the Android programming language and the creation of a file security application with an encryption and description process using the Paillier algorithm, which is expected to solve this problem.

Keywords: Cryptography; Files; Paillier's Algorithm; Android

1. PENDAHULUAN

Pesatnya perkembangan komputer dan kelebihan-kelebihan menjadi pemicu berbagai bidang untuk memanfaatkan hal tersebut dengan penggunaan sistem informasi berbasis komputer khususnya bagi perusahaan guna menghasilkan informasi berbasis komputer yang aktual. Lingkungan perusahaan menempatkan komputer sebagai alat bantu yang mutlak diperlukan. Sistem informasi pun menjadi bagian yang tak kalah pentingnya dalam perusahaan, karena penerapan sistem informasi pada perusahaan tersebut dapat menjadi teknologi yang tepat guna dan berfungsi sebagaimana mestinya untuk menerima dan mengolah data menjadi informasi yang unggul dan kompetitif, sehingga mendapat prioritas yang tinggi dalam mendukung pelaksanaan operasional perusahaan.

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) graphia berarti writing (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan akan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital. Pada zaman Romawi kuno dikisahkan tentang Julius Caesar yang ingin mengirimkan satu pesan rahasia kepada seorang jenderal dimedan perang. Pesan tersebut harus dikirimkan melalui seorang kurir, tetapi karena pesan tersebut mengandung pesan rahasia, Julius Caesar tak ingin pesan tersebut terbuka ditengah jalan. Dari ilustrasi tersebut apa yang dilakukan Julius Caesar dengan cara mengacak pesannya disebut dengan encryption dan saat sang jenderal merapikan pesan yang teracak disebut decryption. Pesan awal yang belum diacak dan yang telah dirapikan disebut plaintext, sedangkan pesan yang telah diacak disebut chipertext.

Data rahasia yang bersifat pribadi dan sangat penting merupakan data yang wajib kita jaga dan lindungi dari orang yang tidak bertanggung jawab. Supaya data tersebut tidak jatuh ketangan yang tidak diinginkan dan data tersebut lebih terjamin keamananannya dari para pencuri yang bisa menyalahgunakan data-data penting tersebut, maka dibutuhkan suatu sistem keamanan. Sistem keamanan sangat penting untuk melindungi data tersebut dari orang-orang yang tidak memiliki hak untuk mengakses. Sistem enkripsi file merupakan salah satu cara untuk mengamankan file dari orang – orang yang tidak bertanggung jawab. Sistem tersebut dapat mengenkripsi file. Oleh karena itu, dibutuhkan suatu metode yang bisa mengenkripsi file tersebut. Salah satunya dengan menerapkan teknik kriptografi.

Algoritma Paillier merupakan sebuah algoritma untuk kriptografi kunci publik. Algoritma paillier bekerja dengan proses pembentukan kunci enkripsi dan dekripsi.. Enkripsi adalah suatu proses mengubah pesan asli menjadi pesan acak (ciphertext). Sedangkan untuk mengembalikan pesan tersembunyi ke bentuk asli disebut Dekripsi. Aplikasi pengamanan data ditujukan untuk membantu mengatasi masalah keamanan data yang dibuat

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2625

atau disimpan menggunakan file yang berformat pdf, dari pencurian file baik yang tidak penting maupun yang penting dan rahasia. Sehingga orang lain tidak dapat mengetahui isi dari file tersebut.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu *kripto* dan *graphia*. *Kripto* berarti *secret* (rahasia) *graphia* berarti *writing* (tulisan). Menurut terminologinya *kriptografi* adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan akan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint*)[2].

2.2 File

Dokumen adalah sebuah bentuk data-data tertulis yang dimiliki seseorang yang diangkap penting. Dokumen juga menjadi sebuah kumpulan data baik berupa gambar, tulisan atau *file* lainnya. Itu menjadi sebuah bentuk pemahaman dan pengertian dari dokumen secara umum[3].

2.3 Algoritma Paillier

Algoriitma paillier adalah sebuah system yang berbasis algoritma asimetris probalistik. *Algoritma enkripsi* yang digunakan adalah sebuah algoritma kriptografi kunci public. Sistem ini ditemuka oleh *pascal paillier* pada tahun 1999. System algoritma paillier dibuat berdasarkan pemikiran bahwa untuk menghitung kelas residu yang ke-n, hal ini dikenal sebagai asumsi *composite residuosity (CR)*[9].

Memilih dua bilangan prima secara random dimana p dan q. Karna diperlukan nilai n. sehingga n = pq. Selain itu, juga perlu dideklarasikan fungsi Totient dari Euler, φ(n) = (p – 1)(q – 1) dan fungsi Carmichael, λ(n) = lcm(p – 1, q – 1). Asumsikan Z_{n2}^{*} = φ(n2) = nφ(n) maka untuk semua w ∈ berlaku :

wλ = 1 mod n

wnλ = 1 mod n2

Teorema ini dinamakan teorema Carmichael.

Sedangkan, sebuah bilangan z dikatakan sebagai residu modulo ke-n dari n2 jika terdapat sebuah bilangan y ∈ sedemikian sehingga : Z_{n2}^{*} z = yn mod n2 Teorema ini dikenal dengan teorema *Composite Residuosity* (CR) yang menjadi dasar dari algoritma *Paillier*. Sementara itu, jika diambil sebuah set Sn = {u < n2 | u = 1 mod n} yang merupakan sebuah subgrup perkalian dari integer modulo n2 melalui sebuah fungsi L, maka persamaan berikut :

∀u ∈ Sn L(u) = (u – 1) / n

pasti akan dapat terdefinisikan dengan baik.[9].

Kunci public dan kunci privat yang digunakan dalam *algoritma paillier* dibangkitkan dengan mekanisme sebagai berikut [13]:

1. Memilih dua bilangan prima berukuran besar sembarangan secara acak, dua bilangan tersebut yang umum disebut *p* dan *q*.
2. Menghitung nilai n, dimana n adalah hasil perkalian antara p dan nilai q (n = p.q).
3. Menghitung nilai ג = lcm (p – 1, q – 1).

Memilih bilangan bulat acak g.

3. HASIL DAN PEMBAHASAN

Analisa *file* merupakan tahapan dimana dilakukannya análisa terhadap *file-file* apa saja yang diolah dalam sistem atau prosedur sebuah rancangan, dalam hal ini *file* yang akan *dienkripsi* dan *dekripsi* pada kriptografi adalah file yang berbentuk file text dan berformat pdf. Solusi dalam mengamankan file dengan menerapkan teknik kriptografi yaitu dengan menggunakan kunci metode diantaranya algoritma *Paillier*. Karena proses *file* dari *Kunci Pailler* dibutuhkan input *plainteks* atau penyandian menggunakan proses pembentukan kunci akan menghasilkan kunci privat dan kunci publik. Kunci publik akan digunakan pada proses *enkripsi* dan kunci privat digunakan pada proses *dekripsi*. Alasan karena tekni kriptografi *Paillier* merupakan salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Berdasarkan teknik penyandian *Paillier* dalam mengamankan *file*, diantaranya untuk menjaga suatu *file* agar *file* tidak bisa dipahami oleh orang yang tidak mengetahui kunci dekripsi dari file tersebut. Hasil proses enkripsi *file* akan menjadi sebuah *cipherteks* yang berbentuk word txt. sehingga *file* tersebut tidak dapat terbaca.

3.1 Penerapan Algoritma Paillier

Permasalahan yang akan diangkat dari penerapan ini adalah bagaimana proses pembentukan kunci dari algoritma *paillier* untuk *enkripsi file*.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2625

1. Pembentukan kunci :
   a. Memilih dua bilangan prima p dan q secara acak
      p = 7
      q = 11
   b. Menghitung nilai n
      n = p x q
      n = 7 x 11
      n = 77
   c. Memilih bilangan bulat acak g
      g = 16

Dimisalkan contoh kasus teks atau *plainteks* dengan nama"YAZIRWAN" menggunakan algoritma *Paillier* sebelum melakukan proses enkripsi, ubah terlebih dahulu plainteks dan kunci ke bilangan *decimal* ke *biner* pada ASCII.

Plaintext : YAZIRWAN
Kunci : p = 7
q = 11
Y = 89 = 01011001
A = 65 = 01000001
Z = 90 = 01011010
I = 73 = 01001001
R = 82 = 01010010
W = 87 = 01010111
A = 65 = 01000001
N = 78 = 01001110
Kelompokkan pesan menjadi subblok
M(1) = 01011001 = 89
M(2) = 01000001 = 65
M(3) = 01011010 = 90
M(4) = 01001001 = 73
M(5) = 01010010 = 82
M(6) = 01010111 = 87
M(7) = 01000001 = 65
M(8) = 01001110 = 78
Input nilai r, r = 4
c = $g^m.r^n$ mod n^2
c(1) = $16^{89}.4^{77}\ mod\ 77^2$ = 5.653486
c(2) = $16^{65}.4^{77}\ mod\ 77^2$ = 7.135702
c(3) = $16^{90}.4^{77}\ mod\ 77^2$ = 9.045577
c(4) = $16^{73}.4^{77}\ mod\ 77^2$ = 3.064761
c(5) = $16^{82}.4^{77}\ mod\ 77^2$ = 2.106087
c(6) = $16^{87}.4^{77}\ mod\ 77^2$ = 2.208393
c(7) = $16^{65}.4^{77}\ mod\ 77^2$ = 7.135702
c(8) = $16^{78}.4^{77}\ mod\ 77^2$ = 3.213634
Cipher teks = 565348671357029045577306476121060872208393713570232136 34

Proses *dekripsi* untuk *cipherteks* yang diperoleh pada proses *enkripsi* di atas dapat dirincikan sebagai berikut:

Cipher teks = 565348671357029045577306476121060872208393713570232136 34
m = c. mod n^2mod n
Kunci : p = 7
q = 11
Kelompokkan *cipher value* menjadisubblok :
m(1) = 5.653486 mod 77^2mod 77 = 5.653486
m(2) = 7.135702 mod 77^2mod 77 = 7.135702
m(3) = 9.045577 mod 77^2mod 77 = 9.045577
m(4) = 3.064761 mod 77^2mod 77 = 3.064761
m(5) = 2.106087 mod 77^2mod 77 = 2.106087
m(6) = 2.208393 mod 77^2mod 77 = 2.208393
m(7) = 7.135702 mod 77^2mod 77 = 7.135702
m(8) = 3.213634 mod 77^2mod 77 = 3.213634
Bit file yang diperoleh = 01011001010000010101101001001001010100100101011101000001010011 10
Karakter ke-1 = 01011001 = 89 = Y

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 2, Januari 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i2.2625

Karakter ke-2 = 01000001 = 65 = A
Karakter ke-3 = 01011010 = 90 = Z
Karakter ke-4 = 01001001 = 73 = I
Karakter ke-5 = 01010010 = 82 = R
Karakter ke-6 = 01010111 = 87 = W
Karakter ke-7 = 01000001 = 65 = A
Karakter ke-8 = 01001110 =78 = N

4. KESIMPULAN

Berdasarkan hasil yang didapat dalam penelitian dan penyusunan skripsi ini serta sesuaikan dengan tujuan, maka diperoleh kesimpulan *Kriptografi* merupakan suatu ilmu dan seni mengamankan *file* serta mampu menawarkan solusi pada setiap permasalahan *file* berdasarkan keamanan dan kerahasiaan. *Algoritma paillier* terbukti dapat mengamankan suatu *file*. Dimana *paillier* dapat mengenkripsikan dan mendekripsikan *file* yang akan diamankan. Hasil pengujian tersebut menyatakan bahwa sifat ini benar adanya. Dalam pengujian *algoritma paillier file* yang akan dienkripsikan melakukan proses pengacakan. Pada pengguna akan memasukkkan variasi kunci yang tidak sama. Setelah melakukan proses tersebut penulis akan melakukan proses *dekripsi* untuk mengembalikan *file* asli.

REFERENCES

[1] Safaat, Nazruddin, Pemrograman Aplikasi Mobile Smartphone Dan Table PC Berbasis Android, Informatika, Bandung 2012.
[2] Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, ANDI : Yogyakarta.
[3] Astuti, Kridalaksana & Pabokory, 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen Menggunakan Algoritma Advanced Encryption Standart. Jurnal Informatika
[4] Mutiara Rizky Parlindungan, 2017. Implementasi Super Enkripsi Menggunakan Algoritma RC4A Dan MDTM Chiper Pada Pengamanan File PDF Berbasis Android. Skripsi Universitas sumatera utara (USU), Medan.
[5] S. Hermawan. 2011. Mudah Membuat Aplikasi Android. ANDI : Yogyakarta
[6] Mulyadi, ST. 2010. Membuat Aplikasi Untuk Android. Multimedia Center Publishing, Yogyakarta.
[7] Shalahuddin, M. Belajar Pemprograman Dengan Bahasa C++ dan Java, Informatika, Bandung 2005.
[8] B. Haryanto. 2011. Esensi-esensi Bahasa Pemrograman Java. ANDI : Yogyakarta
[9] Reinhard M. Simbolon, 2013. Perancangan Aplikasi Lunak Enkripsi Pesan Dengan Metode Paillier Cryptosystem. Jurnal Informatika Budi darma, vol : 5, No : 3. ISSN : 2301-9425. STMIK Budi darma Medan
[10] Adi Nugroho, 2010, Rekayasa Perangkat Lunak Menggunakan UML dan Java. Penerbit ANDI : Yogyakarta
[11] Rosa A.S,M. Shalahuddin 2011, Rekayasa Perangkat Lunak. Penerbit ANDI : Yogyakarta
[12] Wina Novianti Fatimah, ST. Pengenalan Eclipse, p.15.February 2011
[13] Stevia Gionvanni, Dining Cryptographers Protocol Dan Paillier Cryptosystem. Jurnal Informatika Institut Teknologi Bandung.