Jurnal CyberTech

Vol.x. No.x, Januari 2019, pp. xx~xx
P-ISSN : 1978-6603

E-ISSN : 2615-3475

Implementasi Kriptografi Menggunakan Metode RSA Pada Laporan Hasil Pengujian di UPT Perlindungan Tanaman Pangan Dan Hortikultura

Vivi Ayu Mahdina *, Hendryan Winata, S.Kom, M.Kom., Milfa Yetri, S.Kom., M.Kom****

* Program Studi Mahasiswa, STMIK Triguna Dharma

** Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info

Article history:

Keyword:

ABSTRACT

Laporan hasil pengujian ini diperoleh dari hasil pengujian laboratorium baik secara kualitatif dan kuantitatif sebagai dasar

pembuatan sertifikat hasil uji. Data hasil uji ini biasanya digunakan untuk mengetahui bagaimana kondisi sample dari masing-masing daerah.

Implementasi merupakan sebuah tahapan penting pada suatu program yang telah ditetapkan agar tercapainya tujuan yang Laporan hasil Pengujian diinginkan serta dapat dirasakan dampaknya.Secara etimologi, Implementasi menurut Kamus Webster yang dikutip oleh Solichin Abdul Wahab kriptografi tentang pengertian implementasi yang berasal dari bahasa inggris yakni *to implement.* Dalam kamus besar Webster menyatakan bahwa *to implement* (mengimplementasikan) itu berarti menyediakan sarana untuk melaksanakan sesuatu (*to provide the means for carrying out),* untuk menimbulkan dampak/akibat terhadap sesuatu *(to give practical effect to).*

kriptografi adalah ilmu yang mempelajari tentang teknik-teknik pada matematika yang berhubungan dengan aspek keamanan data berupa kerahasiaan, integritas, serta otentikasi suatu data.

Corresponding Author: Nama : **Vivi Ayu Mahdina**

Program Studi : Sistem Informasi STMIK Triguna Dharma

Email : viviayumahdina95@gmail.com

***Journal homepage**: https://ojs.trigunadharma.ac.id/*

1. PENDAHULUAN

Ada berbagai macam algoritma kriptografi yang dapat diimplementasikan untuk pengamanan data yaitu algoritma kriptografi *Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman(RSA).*RSA merupakan proses penyandian *asymmetric key algoritma* yang mana dalam proses enkripsi dan dekripsinya menggunakan kunci yang berbeda. Dimana untuk kunci umum *(Public key)* digunakan untuk proses enkripsi, sedangkan untuk kunci rahasia/pribadi *(private key)* digunakan untuk proses dekripsi. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus *n* yang sangat besar[5].Sehingga algoritma kriptografi RSA ini sangat cocok digunakan untuk enkripsi dan dekripsi pada data laporan hasil pengujian.

Berdasarkan latar belakang tersebut maka diangkat judul yaitu **"Implementasi Kriptografi Menggunakan Metode RSA Pada Laporan Hasil Pengujian di UPT Perlindungan Tanaman Pangan Dan Hortikultura"**

2. METODE PENELITIAN

Di dalam melakukan risert atau penelitian terdapat beberapa cara dalam pengambilan data dengan cara sebagai berikut:

1. Pengumpulan Data (Data Collecting)

Dalam teknik pengumpulan datateradapat beberapa yang dilakukan yaitu dengan cara observasi dan wawancara. Pada bagian observasi ini merupakan teknik pencarian atau pengumpulan data dengan melakukan tinjauan langsung ke Laboratorium Pengujian Mutu dan Residu Pestisida di UPT Perlindungan Tanaman Pangan dan Hortikultura. Dimana untuk melakukan kegiatan observasi pra-riset terlebih dahulu, bertujuan untuk mencari tahu kendala dan masalah seperti apa yang dialami serta sejauh apa dampak yang terjadi dengan keamanan data di instansi tersebut. Berdasarkan hasil observasi tersebut kemudian ditemukan masalah terkait keamanan data pada hasil uji laboratorium. Melakukan kegiatan wawancara ini sebaiknya kepada kepala laboratorium langsung atau kepada pihak-pihak yang bersangkutan dengan data tersebut.

Studi Literatur

. Dari komposisi yang ada jumlah literature yang digunakan sebanyak 20 sumber referensi.Diharapkan dengan literatur tersebut dapat membantu peneliti dalam menyelesaikan permasalahan pengamanan data yang terjadi pada data laporan hasil pengujian.

Tabel 1 Keterangan kunci yang akan digunakan

No. Seri														
2	1	.	L	H	P	.	R	.	0	5	.	0	1	8

Tabel 2 Merubah No.Seri menjadi *Plaintext* ASCII

No. Seri	***Plaintext* ASCII**
2	50
1	49

.	46
L	76
H	72
P	80
.	46
R	82
.	46
0	48
5	53
.	46
0	48
1	49
8	56

K = (17,143)

$C = P^e \bmod n$

Maka : $C_1 = 50^{17} mod\ 143 = 85$

$C_2 = 49^{17} mod\ 143 = 69$

$C_3 = 46^{17} mod\ 143 = 128$

$C_4 = 76^{17} mod\ 143 = 98$

$C_5 = 72^{17} mod\ 143 = 63$

$C_6 = 80^{17} mod\ 143 = 97$

$C_7 = 46^{17} mod\ 143 = 128$

$C_8 = 82^{17} mod\ 143 = 36$

$C_9 = 46^{17} mod\ 143 = 128$

$C_{10} = 48^{17} mod\ 143 = 16$

$C_{11} = 53^{17} mod\ 143 = 92$

$C_{12} = 46^{17} mod\ 143 = 128$

$C_{13} = 48^{17} mod\ 143 = 16$

$C_{14} = 49^{17} mod\ 143 = 69$

$C_{15} = 56^{17} mod\ 143 = 23$

Tabel 3 Hasil enkripsi

No. Seri	***Plaintext* ASCII**	***Enkripsi***
2	50	85
1	49	69

.	46	128
L	76	98
H	72	63
P	80	97
.	46	128
R	82	36
.	46	128
0	48	16
5	53	92
.	46	128
0	48	16
1	49	69
8	56	23

Tabel 4 Hasil *ciphertext* yang akan dikembalikan ke bentuk *plaintext*

No. Seri	***Plaintext*ASCII**	***Enkripsi (ciphertext)***
2	50	85
1	49	69
.	46	128
L	76	98
H	72	63
P	80	97
.	46	128
R	82	36
.	46	128
0	48	16
5	53	92
.	46	128
0	48	16
1	49	69
8	56	23

K = (113,143)

$P = C^d \bmod n$

Maka : $P_1 = 85^{113} mod\ 143 = 50$

$P_2 = 69^{113} mod\ 143 = 49$

$P_3 = 128^{113} mod\ 143 = 46$

$P_4 = 98^{113} mod\ 143 = 76$

$P_5 = 63^{113} mod\ 143 = 72$

$P_6 = 97^{113} mod\ 143 = 80$

$P_7 = 128^{113} mod\ 143 = 46$

$P_8 = 36^{113} mod\ 143 = 82$

$P_9 = 128^{113} mod\ 143 = 46$

$P_{10} = 16^{113} mod\ 143 = 48$

$P_{11} = 92^{113} mod\ 143 = 53$
$P_{12} = 128^{113} mod\ 143 = 46$
$P_{13} = 16^{113} mod\ 143 = 48$
$P_{14} = 69^{113} mod\ 143 = 49$
$P_{15} = 23^{113} mod\ 143 = 56$

Maka hasil *ciphertext* yang telah didekripsi kedalam bentuk *plaintext*, maka hasilnya yaitu sebagai berikut :

Tabel 3.4 Hasil dekripsi

No. Seri	*Plaintext* ASCII	*Enkripsi (ciphertext)*	*Dekripsi (Plaintext)*
2	50	85	50
1	49	69	49
.	46	128	46
L	76	98	76
H	72	63	72
P	80	97	80
.	46	128	46
R	82	36	82
.	46	128	46
0	48	16	48
5	53	92	53
.	46	128	46
0	48	16	48
1	49	69	49
8	56	23	56

3. ANALISA DAN HASIL

2.1 Laporan Hasil Pengujian

Laporan hasil pengujian ini diperoleh dari hasil pengujian laboratorium baik secara kualitatif dan kuantitatif sebagai dasar pembuatan sertifikat hasil uji. Data hasil uji ini biasanya digunakan untuk mengetahui bagaimana kondisi sample dari masing-masing daerah. Factor cuaca dan siklus tanam pada sample yang akan diuji sangat mempengaruhi hasil akhir yang berbeda.Fungsi hasil uji laboratorium sendiri digunakan sebagai bahan dasar pembuatan sertifikat hasil uji laboratorium yang nantinya sangat berpengaruh pada kinerja laboratorium. Sebab jika hasil uji laboratorium tidak akurat, maka laboratorium bisa dituntut oleh petani dan dinas pertanian.

2.2 Implementasi

Implementasi merupakan sebuah tahapan penting pada suatu program yang telah ditetapkan agar tercapainya tujuan yang diinginkan serta dapat dirasakan dampaknya[3].

2.3 Kriptografi kriptografi adalah ilmu yang mempelajari tentang teknik-teknik pada matematika yang berhubungan dengan aspek keamanan data berupa kerahasiaan, integritas, serta otentikasi suatu data. Menurut Stinson sistem kriptografi merupakan suatu kumpulan yang terdiri dari *plaintext, ciphertext, enkripsi dan dekripsi.*Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentukyang tidak dapat dimengerti lagi maknanya. Kriptografi terdiri dari 2 buah proses yang akan dilalui yaitu enkripsi (proses penyandian *plaintext* menjadi *ciphertext)* dan dekripsi (proses kebalikan dari enkripsi yaitu proses mengembalikan *ciphertext* menjadi *plaintext*)[6].

a. Proses pembangkitan kunci

Besaran yang digunakan dalam algoritma kriptografi RSA dalam pembangkitan kunci ini adalah sebagai berikut[11] :

1. Menentukan *p* dan*q*, dimana *p* dan *q* bilangan prima, dimana p ≠ q. Misal nilai *p*= 11 dan *q* = 13. Jadi nilai *p* dan *q* ini harus dirahasiakan.
2. Menghitung nilai modulus*(n) : n = p.q.* Misal :*n = p.q n* = 11.13 = 143. Maka nilai *n* ini boleh dipublikasikan(tidak rahasia).
3. Menghitung *Ø*(n), dimana *Ø*(n) ini merupakan banyaknya bilangan bulat positif yang lebih kecil atau sama dengan *n* danrelative prima terhadap*n.* Dengan begitu dapat dicari dengan persamaan *Ø*(n) = (p – 1)(q – 1) dengan cara sebagai berikut :
   Ø(n) = (p – 1)(q – 1)
   Ø(n) = (11 – 1)(13 – 1)
   Ø(n) = 120. Jadi nilai *Ø*(n) = (p – 1)(q – 1) = 120 (harus dirahasiakan).
4. *e* (kunci enkripsi, dimana 1< e < Ø, e ko prima (bilangan yang tidak bisa saling membagi) Ø), dimana untuk memntukan nilai bilangan bulat *e* sebagai kunci public. Missal nilai *e* relative prima terhadap 120 kita misalkan *e* = 17. *e* = 17
   17 relatif prima terhadap 120
   fpb (17,120) = 1 (kuncinya tidak rahasia)
5. Membangkitkan kunci rahasia *d* dengan persamaan (dimana *d* × *e mod Ø =1*, atau *d = (1 + (k* × *Ø))/e).* kita misalkan dengan *d = (1 + (k* × *Ø))/e)*
   d = (1 + (k × *120))/17)* pada bagian ini, nikai *k* merupakan sembarangan angka yang digunakan untuk menghasilkan suatu nilai integer atau bulat. Dengan mencoba nilai dari 1,2,3… dan seterusnya hingga diperoleh nilai *d* yang bulat. Jadi disini kita misalkan nilai *k* = 16.
   d = (1 + (16× *120))/17)* = 113.
   Jadi diperoleh nilai *d* = 113, sebab *d* × *e mod Ø =1*
   113 × 17 = 1921
   1 (mod120) (maka kuncinya harus dirahasiakan).

Dari hasil algoritma diatas maka dapat disimpulkan bahwa:

1. Proses Enkripsi adalah pasangan dari *(e,n).*
2. Proses Dekripsi adalah pasangan dari *(d,n).*

b. Proses Enkripsi

Proses enkripsi dengan algoritma RSA ini bertujuan untuk menghitung *exponent plaintext* dalam operasi modulus *n* (modulus = sisa pembagian) untuk setiap blok data sehingga menghasilkan ciphertext. Eksponen yang digunakan adalah public exponent *e*. Proses enkripsi ini menggunakan kode ASCII. Dan kunci enkripsi ini menggunakan kunci public cari pasangan *(e,n).* Maka dapat dituliskan persamaan sebagai berikut :

$$C = P^e \bmod n$$

C = ciphertext
P = plaintext e = public exponent
n = modulus

c. Proses Dekripsi

Proses deksripsi yang dilakukan hampir sama dengan enkripsi akan tetapi eksponen yang digunakan adalah private exponent *d* untuk mengembalikan pesan kebentuk asli seperti semula. Maka dapat dituliskan persamaan sebagai berikut [10] :

$$P = C^d \bmod n$$

P = plaintext *C* = ciphertext d = private exponent *n* = modulus

4. KESIMPULAN

Berdasarkan penelitian yang telah dilalui dalam setiap tahapan perancangan keamanan data pada laporan hasil pengujian dengan menggunakan metode RSA maka dapat disimpulkan bahwa :

1. Untuk mengamankan data laporan hasil pengujian di UPT Perlindungan Tanaman Pangan dan Hortikultura menggunakan metode RSA sebab data laporan hasil pengujian ini bersifat rahasia.
2. Berdasarkan pemodelan dan perancangan desain sisttem, metode Algoritma RSA ini dapat diaplikasikan ke dalam pengimplementasian kriptografi pada laporan hasil pengujian. Dimana algoritma RSA ini merupakan pengamanan data yang cukup terbilang rumit, karena dalam perhitungannya memerlukan ketelitian dan logika yang kuat. Sehingga Algoritma RSA ini sangat membantu mengurangi resiko penyalahgunaan pada data laporan hasil pengujian. Dengan pengamanan data berbasis *website* yang telah dibangun, sehingga dapat memudahkan admin dalam menginput data secara aman.

UCAPAN TERIMA KASIH

Terima kasih kepada dosen pembimbing Bapak Hendryan Winata, S.Kom., M.KOM. dan Ibu Milfa Yetri, S.Kom., M.Kom beserta pihak–pihak lainnya yang mendukung penyelesaian jurnal skripsi ini.

REFERENSI

[3] J. T. Informatika, F. Sains, and D. A. N. Teknologi, “Implementasi Kombinasi Algoritma Asimetris Rivest Shamir Adleman Dan Algoritma Simetris Advanced Encryption Standard Pada Aplikasi Pesan Singkat,” 2017.

[5] P. D. Atika, “DIGITAL SIGNATURE DENGAN ALGORITMA SHA-1 DAN RSA SEBAGAI,” vol. XVI, 2018.

[6] W. Chandra, “Kriptografi Dan Algoritma RSA,” no. 13509094, 2011.

[11] “Pendahuluan,” pp. 1–15.

BIBLIOGRAFI PENULIS

	Data Diri
	Nama : Vivi Ayu Mahdina
	Tempat/Tanggal Lahir : Sei Glugur, 17 Maret 1998
	Jenis Kelamin : Perempuan
	Agama : Islam
	Status : Belum Menikah

Pendidikan Terakhir : Sekolah Menengah Atas

Kewarganegaraan : Indonesia

E-mail : viviayumahdina95@gmail.com

Pendidikan Formal

1. Tahun 2003 - 2004 : TK Mentari
2. Tahun 2004 - 2010 : SDN 101829
3. Tahun 2010 - 2013 : SMPN 3 Pancur Batu
4. Tahun 2013 - 2016 : SMAN 1 Sunggal
5. Tahun 2016 - 2020 : STMIK Triguna Dharma

Hendryan Winata, S.Kom., M.kom
Dosen pengajar tetap STMIK TRIGUNADHARMA

	Milfa Yetri, S.Kom., M.Kom Dosen pengajar tetap STMIK TRIGUNADHARMA