RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

Implementasi MD5 dan Paillier Cryptosystem Untuk Membuat Tanda Tangan Digital

Benny Sinaga, Muhammad Abdul Rohim, Efori Bu'ulolo

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338, Medan, Sumatera Utara, Indonesia
Email: [1]nagarinabolak@gmail.com

Abstrak-Dari beberapa manfaat dari teknik kriptografi adalah otentikasi data. Sebelum era digital tanda tangan digunakan sebagai sarana untuk membuktikan otentikasi dokumen cetak seperti surat, piagam, serifikat, ijazah, buku dan sebagainya. Dokumen-dokumen yang tidak memiliki tanda tangan akan diragukan keasliannya. Salah satu sifat dari tanda tangan tersebut adalah bahwa semua pola tanda tangan tersebut adalah sama, sehingga keadaan ini mudah dimanipulasi dengan pemalsuan tanda tangan, bila pihak terkait menggunakan tanda tangan yang berbeda pada setiap dokumen yang ditanda tangani juga akan berdampak perubahan pada keraguan pada pihak yang berhak memverifikasi. Untuk Mengatasi kebutuhan sebaiknya dokumen diberikan tanda tangan digital. Tanda tangan digital yang dimaksudkan bukanlah tanda tangan manual yang di*scan* kemudian disematkan pada dokumen digital. Tanda tangan digital akan dibangun dari teknik kriptografi. Dalam penelitian ini tanda tangan yang akan digunakan adalah tanda tangan dengan kombinasi algoritma fungsi *hash* dan kriptografi kunci-publik berbasis *web*. Adapun metode yang digunakan adalah algoritmai *MD5* dan *Paillier Cryptosystem*. *Paillier cryposystem* merupakan algoritma kriptografi kunci-publik yang diyakini sulit diserang karena menggunakan perhitungan *n-residue class* sehingga akan sangat sulit untuk menemukan pasangan kunci yang digunakan, ini dikenal dengan asumsi *Composite Residuosity* (CR).

Kata Kunci: Tanda Tangan Digital; MD5; *Paillier Cryptosystem*; *Web*.

Abstract-Of the several benefits of cryptographic techniques is data authentication. Before the digital era, signatures were used as a means to prove the authenticity of printed documents such as letters, certificates, certificates, books and so on. Documents that do not have a signature will be doubtful for their authenticity. One of the characteristics of these signatures is that all the signature patterns are the same, so this situation can easily be manipulated with signature forgery, if the related parties use a different signature on each document that is signed it will also have an impact on changing doubts on the parties who are signed. reserves the right to verify. To overcome the need, documents should be given a digital signature. The intended digital signature is not a manual signature that is scanned and then embedded in a digital document. Digital signatures will be built from cryptographic techniques. In this study, the signature that will be used is a signature with a combination of a hash function algorithm and a web-based public-key cryptography. The methods used are the MD5 algorithm and Paillier Cryptosystem. Paillier cryposystem is a public-key cryptographic algorithm which is believed to be difficult to attack because it uses n-residue class calculations so that it will be very difficult to find the key pair used, this is known as the Composite Residuosity (CR) assumption.

Keywords: Digital Signature; MD5; Paillier Cryptosystem; Web.

1. PENDAHULUAN

Teknologi digital telah mengubah peradaban dunia pada saat ini. Perkembangan ini membawa dampak positif dan juga dampak negatif. Salah satu dampak positif yang diperoleh melalui teknologi digital adalah mudahnya menyimpan data atau informasi di dalam komputer dan juga mudahnya melakukan transaksi data atau informasi melalui jaringan internet. Umumnya untuk mengamankan data atau informasi pada saat disimpan atau ditransmisikan digunakan teknik kriptografi enkripsi dan dekripsi. Namun pada kasus-kasus tertentu ada kalanya data atau informasi tidak perlu dienkripsi-dekripsi, tidak perlu dirahasiakan, yang dibutuhkan hanya kepastian apakah data atau informasi ini telah diubah atau tidak.

Untuk menandatangai secara digital digunakan teknik kriptografi. Secara garis besar ada dua cara menanda tangini secara digital yaitu menandatangani dengan cara mengekripsi pesan, dalam hal ini algoritma kunci simetri dan kunci publik dapat digunakan dalam membua tanda tangan, sedangkan cara yang kedua adalah dengan mengkombinasikan algoritma fungsi *hash* dan kriptografi kunci publik[1].

Dalam penelitian ini cara yang digunakan adalah kombinasi fungsi *hash* dan kriptografi kunci publik yaitu kombinasi Md5 dan *Paillier cryptosystem.* Algoritma Md5 akan digunakan untuk menghitung nilai *message digest* adalah berbasis *web*, karena dalam hal ini PHP telah menyediakan fungsi *built-in* MD5 yang siap pakai untuk mencari nilai *hash* dari sembarang *string*, selanjutnya untuk proses enkripsi dan akan diuraikan secara terurut[2]. Algoritma Md5 ini diciptakan oleh Ronald Rivest. Algoritma ini bekerja dengan menerima masukan berupa sembarang pesan (data atau informasi) dan menghasilkan *message digest* berukuran 128 *bit* (panjangnya tetap meskipun jumlah *string* berbeda)[3]. Setelah nilai *hash* diperoleh, nilai *hash* akan dienkripsi dengan menggunakan metode *pailleri cryptosystem.* Algoritma *pailler cryptosystem* adalah algoritma kriptografi kunci-publik. 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*[4]

2. METODOLOGI PENELITIAN

Metode Penelitian yang digunakan untuk mengumpulkan data sebagai berikut:

ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

1. Studi Pustaka
   Pencarian sumber dan bahan pustaka mengenai berbagai teori yang berkaitan dengan persoalan yang akan menjadi rujukan penulisan skripsi. Sumber yang akan dipakai adalah meliputi buku, jurnal, artikel, maupun situs internet.
2. Penyusunan Laporan
   Dalam tahapan ini akan dilaksanakan dengan mendokumentasikan hasil analisa dan menguji dengan tertulis yang berbentuk Laporan Kerja Praktek.

3. HASIL DAN PEMBAHASAN

Telah diuraikan di atas bahwa ada tahapan mendasar yang harus dilakukan untuk menandatangi secara digital yaitu *singing* (pembubuhan tanda tangan) dan *verifying* (verifikasi). Pembubuhan tanda tangan (*Singing*). Untuk membuat tanda tangan dibutuhkan pesan, kunci publik dan kunci rahasia.

1. Dokumen (p)=
   Rajin Membaca.
   Ilmu pengetahuan yang kita peroleh saat ini adalah hasil penelitan dari berbagai pihak selama bertahun-tahun. Ilmu pengetahun ini kemudian dituangkan dalam berbagai bentuk yang mudah diperoleh semua pihak. Ilmu dan pengetahuan ini selalu disebarluaskan semaksimalkan mungkin agar mudah diakses publik. Salah satu cara penyebaran ilmu pengetahuan ini adalah dengan menuangkannya dalam sebuah karya ilmiah buku. Jadi adalah sebuah kerugian yang besar bila masih ada insan yang tidak rajin membaca, karena penelitian bertahun-tahun dapat diperoleh dengan mudah dalam sebuah buku.
   Hash(h)=md5(p)
   Hash (h)= 96fc1dfd5a66fc4228c6d8db615ec462, nilai ini diperoleh dengan menggunakan fungsi *built-in* dengan PHP.
2. Langkah selanjutnya adalah membangkitkan kunci publik dan kunci rahasia *paillier cryptosystem.*
   a. Pilih dua buah bilangan prima besar p dan q
      p=17, q= 37
   b. Hitunglah nilai *n* dan λ
      $n=p*q$
      n = 17* 37
      n= 629
      $\lambda = LCM(p-1, q-1)$
      $\lambda = LCM(17-1, 37-1)$
      $\lambda = LCM(16, 36)$
      λ =*LCM*(2^2* 4, 2^2 *9)
      λ =*LCM*(2^2* 4*9)
      λ =144
   c. Pilih bilangan integer *g* lain secara acak, *g*=23
   d. Mencari nilai u dan L(u).
      $u = g^{\lambda} \ mod \ n^2$
      $u = 23^{144} \ mod \ 629^2$
      $u =$ 70896
      $144 = 128 + 16$
      X_1= 23 mod 692^2= 23
      X_2= $23^{2=}$ mod 692^2= 529
      X_4= 529^2 mod 692^2 = 279841
      X_8=279841^2 mod 692^2 = 41860
      X_{16}=41860^2 mod 692^2 =96224
      X_{32}=96224^2 mod 692^2 =222736
      X_{64}=222736^2 mod 692^2 = 57568
      X_{128}=57568^2 mod 692^2 = 335744
      X_{256}=335744^2 mod 692^2=405664
      Kemudian ambil nilai biner kelipatan dari 144 yaitu
      X_{16} dan X_{128} sehingga,
      u = (X_{128} * X_{16})
      u= (335744 * 96224) mod 692^2
      u = 70896
   e. L(u)= $(u-1)/n$
      $L(u) = (70897-1)/629$
      $L(u) = (70896)/629)$
      $L(u)$ =113
   f. μ= u^{-1} mod n

μ=113^{-1} mod 629
Untuk mencari invers dari modulo maka kedua bilangan harus relatif prima yaitu faktor pembagi bersama terbesar adalah satu (1).
FBB (113)=1, 113
FBB (629)=1, 17, 37, 629 , memenuhi syarat.
μ= 167

g. Kunci publik (*n*, *g*)=(629, 23)
h. Kunci privat $((\lambda, u) = (144, 167)$

3. Enkripsi nilai *hash*, tujuannya adalah menyandikan tanda tangan digital.
Untuk proses enkripsi, maka plainteks terlebih dahulu harus didefeniskan nilai ke dalam biner berdasarkan tabel *ascii*. Berikut uraiannya.

Tabel 1. Nilai Hash

Pi	Pi$_{(10)}$	Pi$_{(2)}$
9	57	00111001
6	54	00110110
f	102	01100110
c	99	01100011
1	49	00110001
d	100	01100100
f	102	01100110
d	100	01100100
5	53	00110111
a	97	01100001

Kelompokkan pesan menjadi subblok bit Hitung nilai b sedemikian sehingga 2^b <= n, n = 629 ; nilai b yang dipilih = 9.
M(1)= 001110010 = 114
M(2)= 011011001 = 217
M(3)= 100110011 = 307
M(4)= 000110011 = 51
M(5)= 000101100 = 44
M(6)= 100011001 = 281
M(7)= 100110010 = 306
M(8)= 000110111 = 55
M(9)= 001100001 = 97

4. Pilih bilangan prima *r* secara acak, *r* =19
5. Menghitung nilai Temp2
Temp2=(r^n) mod (n^2).
Temp2= 19^{629} mod 629^2
Nilai Temp2 bergantung sepenuhnya pada nilai *n*,sehingga untuk memperoleh nilai dari Temp2 dapat dilakukan dengan cara berikut ini.
629=512+64+32+16+4+1
Pangkat 1=19 mod 629^2 = 19
Pangkat 2=19^2 mod 629^2=361
Pangkat 4=361^2 mod 629^2= 130321
Pangkat 8= 130321^2 mod 629^2= 277475
Pangkat 16= 277475^2 mod 629^2= 241384
Pangkat 32= 241384^2 mod 629^2= 185386
Pangkat 64= 185386^2 mod 629^2= 217890
Pangkat 128= 217890^2 mod 629^2= 319023
Pangkat 256= 319023^2 mod 629^2= 192407
Pangkat 512= 192407^2 mod 629^2= 325279
Jadi, Temp2=(325279*217890*185386*241384*130321*19) mod 629^2
Temp2= 27980
Mencari nilai C(1):

$$C(1) = g^{M(1)} * r^n \ mod \ n^2$$
$$C(1) = \left(\left(g^{M(1)} mod \ n^2\right) * \left(r^n \ mod \ n^2\right)\right) \ mod \ n^2$$
$$C(1) = (Temp1 * Temp2) \ mod \ n^2$$
$$Temp1 = \left(g^{M(1)} \ mod \ n^2\right)$$
$$Temp1 = (23^{114} \ mod \ 629^2)$$

ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

Cara memperoleh Temp1 adalah mirip dengan metode sebelumnya dengan menggunakan nilai biner kelipatan.
114=64+32+16+2
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910, sehingga
$Temp1 = ((99910 * 56747 * 23172 * 529)\ mod\ 629^2)$
$Temp1 = 75516$,maka
$C(1) = (75516 * 27980)\ mod\ 629^2$
$C(1) = 214740$
$C(2) = g^{M(2)} * r^n\ mod\ n^2$
$C(2) = \left(\left(g^{M(2)} mod\ n^2\right) * (r^n\ mod\ n^2)\right)\ mod\ n^2$
$C(2) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(2) berdasarkan nilai pada M(2)
$Temp1 = \left(g^{M(2)}\ mod\ n^2\right)$
$Temp1 = (23^{217}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(1), yaitu faktor biner dari M.
$217 = 128 + 16 + 8 + 1$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga
$Temp1 = (381311$ *23172*179587*23)mod 629^2
$Temp1 = 247059$, maka
$C(2) = (Temp1 * Temp2)\ mod\ n^2$
$C(2) = (247059 * 27980)\ mod\ 629^2$
$C(2) =71268$
$C(3) = g^{M(3)} * r^n\ mod\ n^2$
$C(3) = \left(\left(g^{M(3)} mod\ n^2\right) * (r^n\ mod\ n^2)\right)\ mod\ n^2$
$C(3) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(3) berdasarkan nilai pada M(3)
$Temp1 = \left(g^{M(3)}\ mod\ n^2\right)$
$Temp1 = (23^{307}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(2), yaitu faktor biner dari M.
$307 = 256 + 32 + 16 + 2 + 1$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga
$Temp1 = (11221$ *56747*23172*529*23)mod 629^2
$Temp1 = 383885$, maka
$C(3) = (Temp1 * Temp2)\ mod\ n^2$
$C(3) = (14031 * 27980)\ mod\ 629^2$
$C(3) =111508$
$C(4) = g^{M(4)} * r^n\ mod\ n^2$
$C(4) = \left(\left(g^{M(4)} mod\ n^2\right) * (r^n\ mod\ n^2)\right)\ mod\ n^2$

ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

$C(4) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(4) berdasarkan nilai pada M(4)
$Temp1 = \left(g^{M(4)}\ mod\ n^2\right)$
$Temp1 = (23^{51}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(4), yaitu faktor biner dari M.
$51 = 32 + 16 + 2 + 1$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga
$Temp1 = (11221 * 99910 * 23172 * 529 * 23) mod\ 629^2$
$Temp1 = 159974$, maka
$C(4) = (Temp1 * Temp2)\ mod\ n^2$
$C(4) = (159974 * 27980)\ mod\ 629^2$
$C(4)$ =185887
$C(5) = g^{M(5)} * r^n\ mod\ n^2$
$C(5) = \left(\left(g^{M(5)} mod\ n^2\right) * (r^n\ mod\ n^2)\right)\ mod\ n^2$
$C(5) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(5) berdasarkan nilai pada M(5)
$Temp1 = \left(g^{M(5)}\ mod\ n^2\right)$
$Temp1 = (23^{44}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(4), yaitu faktor biner dari M.
$44 = 32 + 8 + 4$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga
$Temp1 = (56747 * 179587 * 279841) mod\ 629^2$
$Temp1 = 327994$, maka
$C(5) = (Temp1 * Temp2)\ mod\ n^2$
$C(5) = (327994 * 27980)\ mod\ 629^2$
$C(5)$ =379125
$C(6) = g^{M(6)} * r^n\ mod\ n^2$
$C(6) = \left(\left(g^{M(6)} mod\ n^2\right) * (r^n\ mod\ n^2)\right)\ mod\ n^2$
$C(6) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(6) berdasarkan nilai pada M(6)
$Temp1 = \left(g^{M(6)}\ mod\ n^2\right)$
$Temp1 = (23^{281}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(4), yaitu faktor biner dari M.
$281 = 256 + 16 + 8 + 1$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga

ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

$Temp1 = (11221*23172*179587*23) mod\ 629^2$
$Temp1 = 293159$, maka
$C(6) = (Temp1 * Temp2)\ mod\ n^2$
$C(6) = (293159 * 27980)\ mod\ 629^2$
$C(6) =159608$
$C(7) = g^{M(7)} * r^n\ mod\ n^2$
$C(7) = \left(\left(g^{M(7)} mod\ n^2\right) * \left(r^n\ mod\ n^2\right)\right)\ mod\ n^2$
$C(7) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(7) berdasarkan nilai pada M(7)
$Temp1 = \left(g^{M(7)}\ mod\ n^2\right)$
$Temp1 = (23^{306}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(4), yaitu faktor biner dari M.
$306 = 256 + 32 + 16 + 2$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga
$Temp1 = (11221 *56747*23172*529) mod\ 629^2$
$Temp1 = 240314$, maka
$C(7) = (Temp1 * Temp2)\ mod\ n^2$
$C(7) = (240314 * 27980)\ mod\ 629^2$
$C(7) =66925$
$C(8) = g^{M(8)} * r^n\ mod\ n^2$
$C(8) = \left(\left(g^{M(8)} mod\ n^2\right) * \left(r^n\ mod\ n^2\right)\right)\ mod\ n^2$
$C(8) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(8) berdasarkan nilai pada M(4)
$Temp1 = \left(g^{M(8)}\ mod\ n^2\right)$
$Temp1 = (23^{55}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(4), yaitu faktor biner dari M.
$55 = 32 + 16 + 4 + 2 + 1$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841
g^8=279841^2 mod 629^2=179587
g^{16}=179587^2 mod 629^2=23172
g^{32}=23172^2 mod 629^2=56747
g^{64}=56747^2 mod 629^2=99910
g^{128}=99910^2 mod 629^2=381311
g^{256}=381311^2 mod 629^2= 11221
g^{512}=11221^2 mod 629^2= 97003, sehingga
$Temp1 = (56747 *23172*279841*279841*529*23) mod\ 629^2$
$Temp1 = 161078$, maka
$C(8) = (Temp1 * Temp2)\ mod\ n^2$
$C(8) = (161078 * 27980)\ mod\ 629^2$
$C(8) = 215809$
$C(9) = g^{M(8)} * r^n\ mod\ n^2$
$C(9) = \left(\left(g^{M(9)} mod\ n^2\right) * \left(r^n\ mod\ n^2\right)\right)\ mod\ n^2$
$C(9) = (Temp1 * Temp2)\ mod\ n^2$
Mencari Temp1 untuk C(9) berdasarkan nilai pada M(9)
$Temp1 = \left(g^{M(9)}\ mod\ n^2\right)$
$Temp1 = (23^{97}\ mod\ 629^2)$, cara kerja hampir sama dengan pada proses C(4), yaitu faktor biner dari M.
$97 = 64 + 32 + 1$
g^1=23 mod 629^2 = 23
g^2= 23^2 mod 629^2= 529
g^4= 529^2 mod 629^2= 279841

ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

$g^8=279841^2 \bmod 629^2=179587$
$g^{16}=179587^2 \bmod 629^2=23172$
$g^{32}=23172^2 \bmod 629^2=56747$
$g^{64}=56747^2 \bmod 629^2=99910$
$g^{128}=99910^2 \bmod 629^2=381311$
$g^{256}=381311^2 \bmod 629^2= 11221$
$g^{512}=11221^2 \bmod 629^2= 97003$, sehingga
$Temp1 = (99910 * 56747 * 23) mod\ 629^2$
$Temp1 = 129597$ maka
$C(9) = (Temp1 * Temp2)\ mod\ n^2$
$C(9) = (129597 * 27980)\ mod\ 629^2$
$C(9)$ =74295, sehingga diperoleh seluruh cipherteks adalah sebagai berikut:
$C(1) = 214740$
$C(2)$ =71268
$C(3)$ =111508
$C(4)$ =185887
$C(5)$ =379125
$C(6)$ =159608
$C(7)$ =66925
$C(8) = 215809$
$C(9)$ =74295

6. Selanjutnya mengkoversi seluruh cipherteks dari format desimal ke format biner dan menggabungkannya.
   $C(1) = 214740$ =110100011011010100
   $C(2)$ =71268 =10001011001100100
   $C(3)$ =111508=11011001110010100
   $C(4)$ =185887=101101011000011111
   $C(5)$ =379125=1011100100011110101
   $C(6)$ =159608=100110111101111000
   $C(7)$ =66925=10000010101101101
   $C(8) = 215809$=110100101100000001
   $C(9)$ =74295=10010001000110111
7. Gabungkan Seluruh biner cipherteks, berikut hasil penggabungannya,
   Cipherteks="1101000110110101001000101100110010011011001110010100101101011000011111101110010001111010110011011111011110001000001010110110111010010110000000110010001000110111"

   Kelompokkan kembali data biner pada langkah ke-7 menjadi sub blok bit, dengan ukuran 8-bit agar dapat dikonversi ke desimal untuk mengembalikan ke karakter *ascii.*
   Bit-1=11010001=209=Ñ
   Bit-2=10110101=181=µ
   Bit-3=00100010=34= “
   Bit-4=11001100=204=Ì
   Bit-5=10011011=155= >
   Bit-6=00111001=57= 9
   Bit-7=01001011=75=K
   Bit-8=01011000=88=X
   Bit-9=01111110=126= ~
   Bit-10=11100100=228= ä
   Bit-11=11001101=205=Í
   Bit-12=11101111=239=ï
   Bit-13=00010000=16=(karakter tidak dapat ditampilkan)
   Bit-14=01010110=86=V
   Bit-15=11011101=221=Y
   Bit-16=00101100=44= ,
   Bit-17=00000110=6= (karakter tidak dapat ditampilkan)
   Bit-18=01000100=68=D
   Bit-19=00110111=55=7
   Bit-19=01111010=122=z

ISSN 2745-7966 (Media Online)
Vol 2, No 5, Mei2022
Hal 187-194
https://djournals.com/resolusi

4. KESIMPULAN

Berdasarkan Penelitian ini dapat diambil kesimpulan *Paillier cryptosystem* efektif dalam menyembunyikan pesan karena perubahan karakter *plaintext* dengan *ciphertext* sangat kontras perbedaannya. Hal ini akan mempersulit pihak penyerang untuk melakukan serangan otentikasi data. Dengan menerapkan *paillier cryptosystem* untuk mengenkripsi nilai *hash* diyakini mampu mengelabuhi pihak penyerang, hal terlihat dari adanya penambahan karakter pada *chipertext*, karena *chipertex* lebih panjang dari *plaintext. Paillier cryptosystem* tidak efesien digunakan untuk enkripsi data dalam ukuran besar, karena akan membebani memori. *Paillier cryptosystem* cukup efektif untuk tanda tangan digital bila dikombinasi dengan fungsi *hash.*

REFERENCES

[1] Rinaldi Munir.Kriptografi Edisi Kedua. Bandung. Penerbit Informatika. 2019.
[2] Rohi Abdullah. 7 in 1 Pemograman Web Untuk Pemula. Jakarta. Penerbit Elex Media Komputindo. 2018.
[3] Kadri Yusuf." Penerapan Algoritma Md5 Sebagai Pengaman Akun Pada Aplikasi Web Emusrenbang Kota Binjai". Jurnal Teknik Informatika Kaputama (Jtik) Vol. 4 , No1.
[4] Juni Ade Nawer Purba, Taronisokhi Zebua, Rivalri K Hondro." Implementasi Algoritma Paillier Cryptosystem Pengamanan Citra Digital Pada Aplikasi Chat". Komik (Konferensi Nasional Teknologi Informasi Dan Komputer)Volume 3, Nomor1
[5] T. Zebua And E. Ndruru, "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma Rc4", *J.Teknol. Infomasi Dan Ilmu Komput.*, Vol. 4, No. 4, Pp. 275–282, 2017.
[6] Janner Simarmata Dkk. Kriptografi Teknik Keamanan Data Dan Informasi. Yogyakarta. Penerbit Andi. 2019.
[7] Muhadi M.Ilyas Gultom1, Darjat Saripurna2," Perancangan Sistem Keamanan Aplikasi *E-Voting* Untuk Pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik Uisu Dengan Menggunakan Algoritma Md5", Algoritma: Jurnal Ilmu Komputer Dan Informatika, Volume: 03, Number: 02
[8] Juni Ade Nawer Purba, Debora Sinaga, Saima Ronita Purba." Implementasi Algoritma Paillier Cryptosystem Pengamanan Audio" Seminar Nasional Teknologi Komputer & Sains (Sainteks) 2019.
[9] Menanti Cristian Sianturi, Firman Telaumbanua, Zul Fikri Sofyan." Pengamanan Citra Digital Dengan Algoritma Paillier Criptosystem". Eminar Nasional Teknologi Komputer & Sains (Sainteks).2020
[10] Asep Roy Panggabean." Implementasi Algoritma *Paillier Cryptosystem* Untuk Keamanan Data Video Mpeg Pada Aplikasi Chat". Jurnal Informasi Dan Teknologi Ilmiah (Inti)Volume 8, No 1, 2020
[11] Christine Jost1, Ha Lam2, Alexander Maximov3, And Ben Smeets3." Encryption Performance Improvementsof The Paillier Cryptosystem".
[12] Junaidy B. Sanger." Desain Dan Implementasi Mekanisme Tanda Tangan Dijital Dalam Pertukaran Data Dengan Hash Md5 Dan Enkripsi/Dekripsi Menggunakan Algoritma Rsa". *Jurnal Lasallian Vol. 12 No. 2 September 2015*