Volume 1, Nomor 4, April 2021
p-ISSN ***2774-5147*** ; e-ISSN ***2774-5155***

# IMPLEMENTASI ALGORITMA *CAESAR CIPHER* DAN ALGORITMA RSA UNTUK KEAMANAN DATA SURAT WASIAT PADA KANTOR NOTARIS/PPAT ROBERT TAMPUBOLON, S.H.

**Robertus Silalahi, Iin Parlina, Sumarno, Indra Gunawan dan Widodo Saputra**
STIKOM Tunas Bangsa Pematangsiantar
E-mail: robertussilalahi02@gmail.com, iin@amiktunasbangsa.ac.id, sumarno@amiktunasbangsa.ac.id, indra@amiktunasbangsa.ac.id dan widodo@amiktunasbangsa.ac.id

Diterima:
**13 Februari 2021**
Direvisi:
**11 April 2021**
Disetujui:
**14 April 2021**

**Abstrak**

Keamanan dan kerahasiaan adalah salah satu kebutuhan penting dari suatu data, atau informasi. Terkait betapa pentingnya menjaga isi data file surat wasiat dari pihak yang merugikan dengan cara merusak dan memanipulasi data pada kantor Notaris Robert Tampubolon, SH. Pada penelitian ini penulis membuat Aplikasi pengamanan berupa data surat wasiat pada isi file document dengan mengkombinasikan algoritma *caesar cipher* dan RSA. Metode yang digunakan adalah kombinasi algoritma *caesar cipher* dan algoritma RSA yang menggunakan dua kunci berbeda dalam melakukan enkripsi dan dekripsi yaitu kunci publik untuk enkripsi dan kunci *private* untuk dekripsi. dalam proses mengenkripsi pesan dengan menggunakan kunci yang berupa angka-angka yang telah ditentukan pengirim, dan mendekripsi pesan yang dikirim menjadi pesan asli, sehingga pesan tersebut cukup aman dan tidak akan terbaca pihak-pihak yang tidak mempunyai hak atas pesan tersebut. Tujuan penelitian ini adalah memberikan solusi terhadap masalah yang dihadapi untuk memastikan keadaan akta surat wasiat benar-benar aman pada kantor Notaris Robert Tampubolon SH. Metode ini menggunakan kombinasi algoritma *caesar chiper* dan RSA (*Rivest Shamir Adleman*) untuk menghasilkan aplikasi yang digunakan pada proses enkripsi dan dekripsi pada akta surat wasiat. Pengamanan data pada kantor notaris memiliki beberapa kesimpulan yaitu aplikasi yang dibangun dapat membantu dalam mengamankan data *file* surat wasiat pada kantor notaris menggunakan kombinasi metode *caesar cipher* dan *RSA*, surat wasiat yang di enkripsi dan didekripsi hanya dapat dibaca oleh orang yang memiliki akses kedalam aplikasi dan sistem yang dibangun mampu memberikan keamanan yang baik sehingga data isi dari surat wasiat tidak dapat dibaca oleh orang yang tidak berkepentingan.

**Kata kunci**: *Caesar cipher; Keamanan Data; Enkripsi; Dekripsi; Kombinasi, RSA.*

***Abstract***

*Security and confidentiality are one of the essential needs of a data, or information. Related to how important it is to maintain the contents of the will file data from adverse parties by damaging and manipulating the data in the office of Notary*

*Robert Tampubolon, SH. In this study the authors made a security application in the form of will data on the contents of document files by combining caesar cipher and RSA algorithms. The method used is a combination of caesar cipher algorithm and RSA algorithm that uses two different keys in performing encryption and decryption i.e. public key for encryption and private key for decryption. in the process of encrypting a message by using a key that is a predetermined number of the sender, and decrypting the message sent to the original message,so that the message is quite secure and will not be read by those who do not have rights to the message. The purpose of this research is to provide solutions to the problems faced to ensure the state of the deed of will is completely safe in the office of Notary Robert Tampubolon SH. This method uses a combinationof caesar chiper and RSA (Rivest Shamir Adleman) algorithmsto generate applications used in the encryption and decryption process on will deed. Data security in the notary office has several conclusions that the application that is built can help in securing the data of will files in the notary office using a combination of caesar cipher and RSA methods, wills that are encrypted and decrypted can only be read by people who have access to applications and systems built capable of providing good security so that the data of the contents of the will can not be read by unauthorized persons.*

**Keywords***:* Caesar cipher; Data security; Encryption; Decryption; Combination, RSA.

## PENDAHULUAN

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data, pesan dan informasi (Nugroho, Azmi, & Arif, 2016). Data menjadi hal vital dimasa ini, terkait betapa pentingnya pihak atau orang berkepentingan mengakses data tersebut (Pramusinto, Wizaksono, & Saputro, 2020). Apabila ada pihak yang tidak berkepentingan mengakses data tersebut (Murdani, 2017).

Akta surat wasiat ini dilakukan untuk memuat keinginan-keinginan terakhir seseorang yang akan apabila yang bersangkutan meninggal dunia (Siregar, 2018). Di wasiat ini lebih sering memuat keinginan yang terakhir berkaitan dengan harta yang dimilikinya (Megajati & Mutimatun, 2021) yang hendak dia berikan atau wariskan kepada orang-orang yang disayanginya. Meskipun surat wasiat dalam bentuk akta (Sanjaya, 2018), namun hukum perdata tidak mensyaratkan apakah surat wasiat itu harus dibuat dalam bentuk akta dibawah tangan (Simanjuntak, 2016) atau akta otentik (dibuat dihadapan Notaris) Hal ini penting mengingat dalam segi pembuktian akta otentik memiliki pembuktian yang sempurna (Setiadewi & Wijaya, 2020).

Dalam penelitian ini akan dilakukan pengamanan berupa data surat wasiat pada pesan teks yang berupa isi *file document* dengan mengimplementasikan metode kriptografi yaitu algoritma *caesar chiper* dan RSA (*Rivest Shamir Adleman*). Hasil penelitian yaitu membuat sistem keamanan akta surat wasiat pada kantor Notaris/PPAT Robert Tampubolon, SH. Semua dilakukan untuk menjaga keamanan dan pemalsuan pada akta surat wasiat. Tujuan penelitian ini adalah memberikan solusi terhadap masalah yang dihadapi untuk memastikan keadaan akta surat wasiat benar-benar aman pada kantor

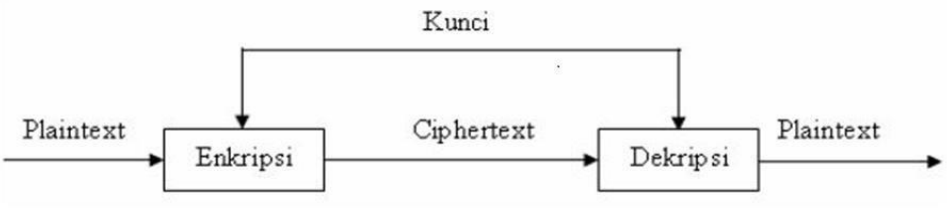
Notaris Robert Tampubolon SH. Metode ini menggunakan kombinasi algoritma *caesar chiper* dan RSA (*Rivest Shamir Adleman*) untuk menghasilkan aplikasi yang digunakan pada proses enkripsi dan dekripsi pada akta surat wasiat. Manfaat dari hasil penelitian adalah menambah wawasan dan kemampuan dalam pengimplementasian ilmu kriptografi, khususnya pada algoritma *Caesar Cipher* dan RSA (*Rivest Shamir Adleman*) dalam mengenkripsi dan dekripsi suatu isi *file document*.

Surat wasiat ini lebih sering memuat keinginan yang terakhir (Yenni, 2017) berkaitan dengan harga yang dimilikinya yang hendak ia berikan atau wariskan kepada orang-orang yang disayanginya. Hal ini penting mengingat dalam segi pembuktian akta otentik memiliki pembuktian yang sempurna.

Menurut (Siburian & Harianja, 2017) "Kriptografi berasal dari bahasa yunani, yaitu *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan, jadi kriptografi adalah tulisan rahasia. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya, Atau dalam defenisi lain kriptografi adalah seni dan ilmu dalam mengamankan pesan".

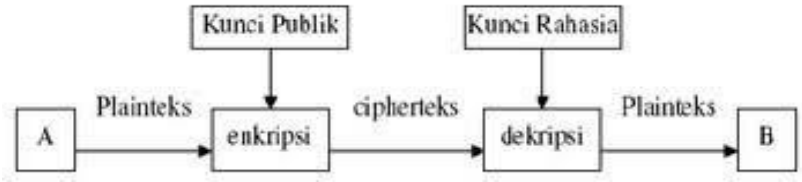
Kriptografi bertujuan untuk memberi layanan keamanan, yang dinamakan aspek-aspek keamanan yaitu kerahasiaan adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak, integritas data adalahlayanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman, otentikasi adalah layanan yang berhubungan dengan identifikasi, baik yang mengidentifikasi kebenaran pihak-pihak yang berkomunikasi, dan *non-repudiation* adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

Proses enkripsi/dekripsi kriptografi simetrik dapat dilihat pada gambar 1. dibawah ini.




Gambar 1. Proses *enkripsi/dekripsi* kriptografi simetris

*Plain text* adalah data asli yang bisa memberikan informasi bila dibaca (Ridho, 2017). *Ciphertext* adalah data yang sudah mengalami proses kriptografi, sehingga informasi didalamnya bisa disembunyikan. *Ciphertext* inilah yang kemudian akan dikirimkan melalui jaringan (Haji & Mulyono, 2012). Enkripsi adalah proses untuk mengubah *plaintext* menjadi *ciphertext* (Cahyadi, 2012). Sebaliknya dekripsi adalah proses untuk mengubah *ciphertext* menjadi *plaintext* kembali (Hasugian, 2013). Proses enkripsi/dekripsi kriptografi asimetrik dapat dilihat pada gambar 2 dibawah ini.




Gambar 2. Proses *enkripsi/dekripsi* kriptografi asimetris

A adalah pihak yang mengirimkan data, sedangkan B adalah pihak yang menerima data. *Plaintext* adalah data asli yang bias memberikan informasi bila dibaca. *Ciphertext* adalah data yang sudah mengalami proses kriptografi, sehingga informasi didalamnya bisa disembunyikan. *Ciphertext* inilah yang kemudian akan dikirimkan melalui jaringan. Enkripsi adalah proses untuk mengubah *plaintext* menjadi *ciphertext.* Sebaliknya dekripsi adalah proses untuk mengubah *ciphertext* menjadi *plaintext* kembali.

Kriptografi, sandi *Caesar*, atau sandi pindah, kode *Caesar* yaitu metode enkripsi sangat sederhana dan sangat populer. Kode ini terdiri dari semua huruf semua huruf pada teks asli *(Plaintext)* disubstitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alphabet. Dalam *Caesar cipher*, huruf-huruf diubah dengan huruf selanjutnya dari posisi alphabet yang sama. Proses *Caesar cipher* adalah:

1. Tentukan berupa besar pemindahaan karakter yang dipakai untuk membuat *cipherteks* ke *plainteks.*
2. Tukar posisi karakter *plainteks* menjadi *cipherteks* berdasarkan pemindahan yang telah ditentukan sebelumnya. Contoh pemindahan huruf D, huruf B menjadi huruf E dan berikutnya".

Rumus untuk enkripsi:
C = E (P) = (P+K) Module (26)
Maka dari contoh diatas, maka enkripsi dapat dilakukan rumus:
C = E (P) = (P+3) Module (26)
Rumus untuk Dekripsi:
P = D (C) = (C-K) Module (26)
Maka dari contoh diatas, maka dekripsi dapat dilakukan rumus:
P = D (C) = (C-3) Module (26)

RSA *(Rivest Shamir adleman*) merupakan salah satu dari *Public key cryptosystem* yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data. algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus *n* yang sangat besar.

Menurut (Agustina, 2017) "Keamanan dari sistem kriptografi RSA adalah didasari oleh dua problem matematika yaitu masalah dalam faktorisasi bilangan berjumlah banyak. Sumber masalah dari RSA, yaitu mencari modulo akar e n dari sebuah bilangan komposit yang faktor-faktornya tidak diketahui proses dekripsinya penuh dari sebuah *ciphertext* RSA dianggap sesuatu hal yang tidak mudah karena kedua masalah ini diasumsikan sulit. Permasalahan dari RSA didefenisikan sebagai tugas untuk mencari suatu akar modulo e n (e pangkat ke n) dari bilangan komposit. Mengembalikan suatu nilai m dimana m e=c mod n, (e, n) adalah kunci publik RSA dan c adalah *ciphertext* RSA. Metode pendekatan yang diyakini dapat menyelesaikan masalah RSA saat iniadalah memfaktor dari modulus n. Dengan kemampuan untuk mengembalikan faktor yang merupakan bilangan prima, sebuah serangan dapat menghitung eksponen rahasia dari d dan dari kunci publik (e, n), lalu mendekripsi c menggunakan prosedur standart. Untuk menyelesaikan, penyerang. Memfaktor nilai n menjadi p dan q, lalu menghitung (p-1) (q-1) yang dapat menghasilkan nilai d dan e.

Algoritma pembentukan kunci

1. Tentukan p dan q bernilai dua bilangan prima besar, acak dan rahasiakan, $p \neq q$, p dan q memiliki ukuran yang sama.
2. Hitung $n = p \times q$, dan hitung $\phi(n) = (p-1) \times (q-1)$, bilangan integer *n* disebut (RSA) modulus.
3. Tentukan *e* bilangan prima acak yang memiliki syarat :

$1 < e ,< \mathrm{I}(n)$, *GCD (e, i(n)* = 1, disebut *e* relative prima terhadap i(*n*), bilangan integer *n* disebut (RSA) enciphering component, sehingga menghasilkan D*d(*Ee(m)) = E*e*(D*d*(c)) = $m^d \bmod n$

Tabel ASCII merupakan tabel atau daftar yang bersi semua huruf dalam alfabet romawi ditambah beberapa karakter tambahan. Dalam tabel ini setiap karakter akan selalu diwakili oleh sejumlah kode yang sama. Misal untuk huruf "b" (b kecil) selalu diwakili oleh urutan nomer 98, dan kalo dipresentasi menggunakan 0 dan 1 dalam bilangan biner, 98 adalah bilangan biner 110 0010 (Dosen, 2016)
Tabel ASCII dapat dilihat pada tabel 1. dibawah ini.

Tabel 1. ASCII

| Char | ASCII Code | Binary | Char | ASCII Code | Binary |
|---|---|---|---|---|---|
| A | 097 | 01100001 | A | 065 | 01000001 |
| B | 098 | 01100010 | B | 066 | 01000010 |
| C | 099 | 01100011 | C | 067 | 01000011 |
| D | 100 | 01100100 | D | 068 | 01000100 |
| E | 101 | 01100101 | E | 069 | 01000101 |
| F | 102 | 01100110 | F | 070 | 01000110 |
| G | 103 | 01100111 | G | 071 | 01000111 |
| H | 104 | 01101000 | H | 072 | 01001000 |
| I | 105 | 01101001 | I | 073 | 01001001 |
| J | 106 | 01101010 | J | 074 | 01001010 |
| K | 107 | 01101011 | K | 075 | 01001011 |
| L | 108 | 01101100 | L | 076 | 01001100 |
| M | 109 | 01101101 | M | 077 | 01001101 |
| N | 110 | 01101110 | N | 078 | 01001110 |
| O | 111 | 01101111 | O | 079 | 01001111 |
| P | 112 | 01110000 | P | 080 | 01010000 |
| Q | 113 | 01110001 | Q | 081 | 01010001 |
| R | 114 | 01110010 | R | 082 | 01010010 |
| S | 115 | 01110010 | S | 083 | 01010011 |
| T | 116 | 01110100 | T | 084 | 01010100 |
| U | 117 | 01110101 | U | 085 | 01010101 |
| V | 118 | 01110110 | V | 086 | 01010110 |
| W | 119 | 01110111 | W | 087 | 01010111 |
| X | 120 | 01111000 | X | 088 | 01011000 |
| Y | 121 | 01111001 | Y | 089 | 01011001 |
| Z | 122 | 01111010 | Z | 090 | 01011010 |

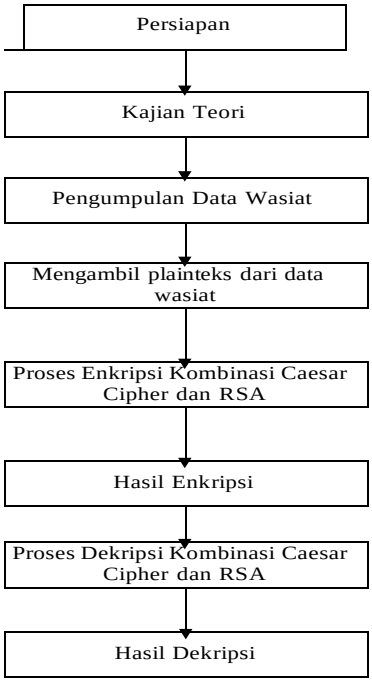
Sumber: *https://www.google.com/search?q=tabel+ascii&safe*

Menurut (Deval Gusrion, 2018) ”Basis data (*database*) adalah kumpulan suatu informasi yang disimpan di dalam komputer secara sistematik dimana suatu informasi tersebut dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi. Ada beberapa perangkat lunak atau *software open source* yang disediakan untuk membuat suatu basis data. Perangkat lunak tersebut merupakan suatu pemrogramanyang dikategorikan sebagai bahasa pemrograman tingkat tinggi *(high level language)* salah satunya adalah *MySQL*. Database *MySQL* dapat dibuat menggunakan tampilan *phpmy admin* atau menggunakan sebuah scrip dalam PHP. *MySQL* merupakan sebuah perangkat lunak/software system manajemen basis data *SQL* atau DBMS *Multitheread* dan *multi user*. *MySQL* sebenarnya merupakan turunan dari salah satu konsep utama

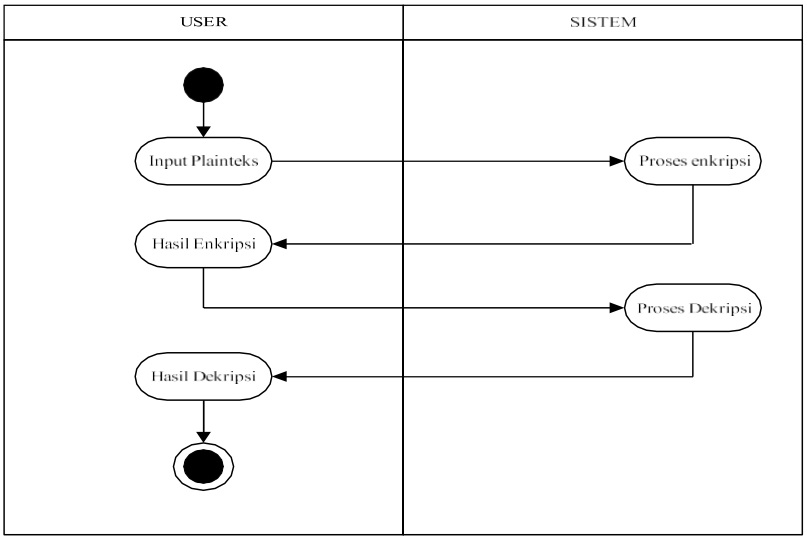
dalam *database* untuk pemilihan atau seleksi dan pemasukan data yang memungkinkan pengoperasian data dikerjakan secara mudah dan otomatis".

## METODE PENELITIAN

Metode penelitian merupakan prosedur dan langkah-langkah yang dilakukan oleh peneliti dalam rangka untuk mengumpulkan data. Adapun prosedur dan langkah-langkah yang harus ditempuh adalah waktu penelitian, sumber data, dan dengan langkah apa data tersebut diperoleh dan selanjutnya diolah dan dianalisis.

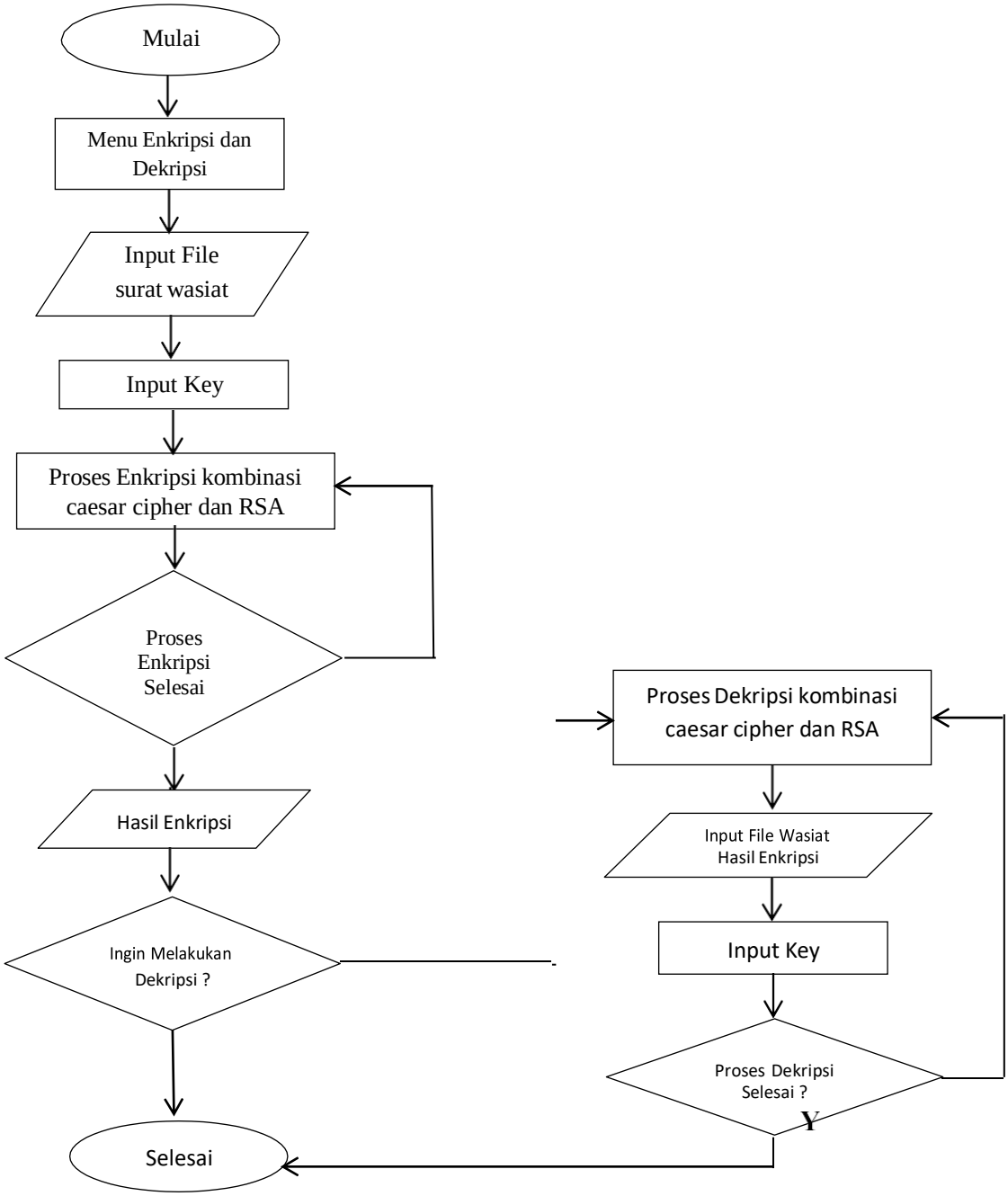



Gambar 3. Rancangan Alur Penelitian

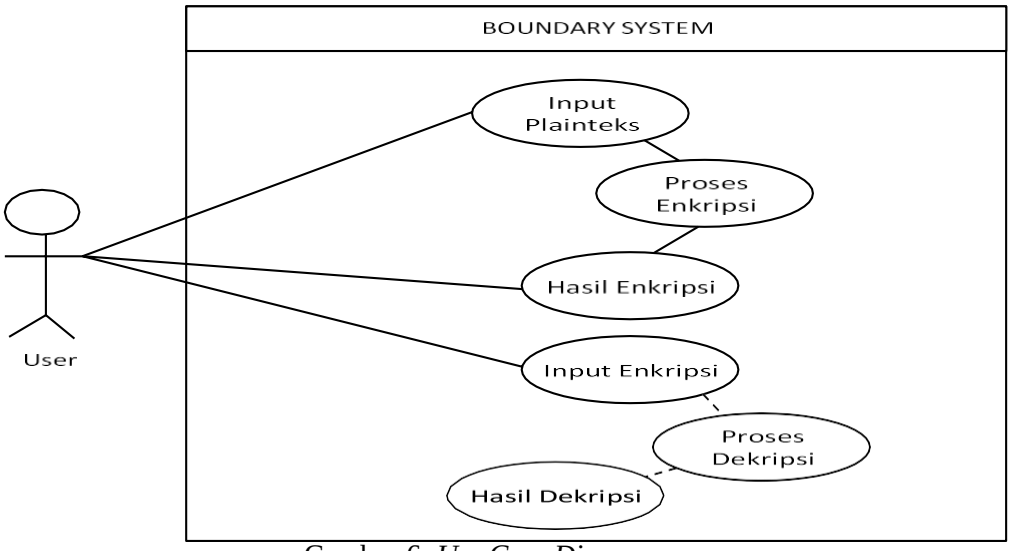



Gambar 4. *Activity Diagram*

Instrumen Penelitian *flowchart* sistem dapat dilihat pada gambar 5 dibawah ini.




Gambar 5. Instrumen penelitian *flowchart* sistem




Gambar 6. *Use Case Diagram*

Metode yang digunakan dalam pengamanan data surat wasiat saat ini adalah menggunakan *caesar cipher* dikombinasikan dengan algoritma RSA. Berikut ini akan dijelaskan secara singkat masing-masing metode yang digunakan;

Algoritma *Caesar Cipher*

Dalam kasus yang dibahas ini penulis menggunakan pergeseran sebanyak 4 posisi dengan plainteks : ROBERT. Substitusi dapat dilihat pada Tabel 3.1. dibawah ini.

Tabel 2. Substitusi

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |

Berdasarkan tabel substitusi di atas maka dapat diambil hasil enkripsi caesar cipher yaitu menjadi:

Plainteks : ROBERT
Enkripsi : VSFIVX

Algoritma RSA

Dalam melakukan enkripsi data menggunakan RSA ada beberapa tahapan yang harus dilakukan yaitu menentukan 2 buah bilangan prima acak sampai kepada pembangkitan kunci (Listiyono, 2012). Keamanan dari algoritma RSA masih tergolong cukup aman selagi masih belum ditemukannya faktorisasi prima dari kunci pribadi maka selama itu keamanan menggunakan algoritma RSA masih terjaga (Yulian, 2018). Berikut ini akan dijelaskan bagaimana proses pembangkitan kunci RSA:

Tahap 1
Pilih 2 buah bilangan prima yang acak, dalam kasus ini penulis memilih p=23 dan q=43
Tahap 2
Hitung nilai n dimana n = p*q = 989
Tahap 3
Hitung nilai totient(n) = (p-1)*(q-1)=22*42=924
Tahap 4
Pilih nilai e sedemikian sehingga relatif prima terhadap totient(n) =924 dan kurang dari totient(n); maka harus didapatkan nilai e*d mod 924=1

Tahap 5
Karena hasil totient(n) berakhiran 4 maka kita mengambil angka 5 karena hasil dari 5 mod 4 =1, maka kita harus mencari 925 karena nilai 925 mod 924=1, maka didapatkan e*d mod 924 = 1 dimana nilai e = 25 dan nilai d = 37
Berdasarkan uraian diatas maka didapatkan kunci *private* (d) = 37 dan kunci publik (e) = 25 dengan n = 989

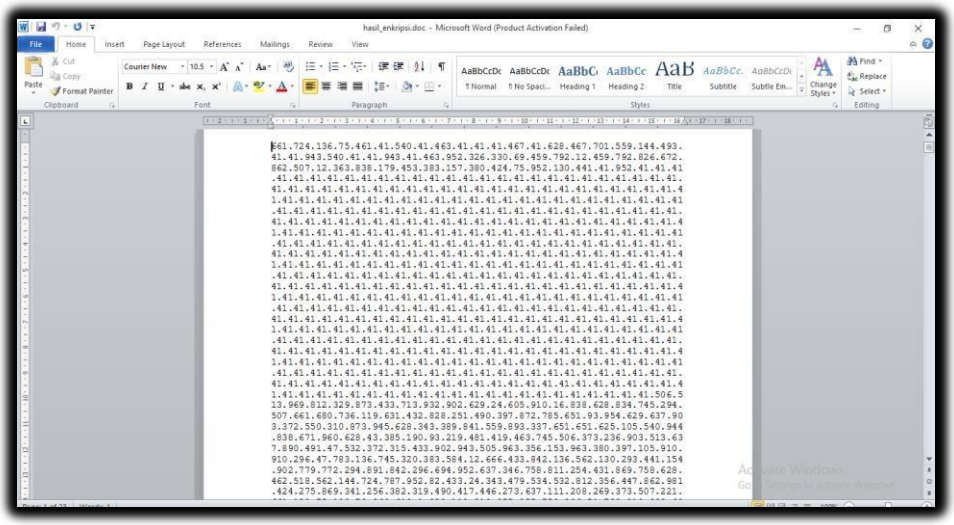
Kemudian akan kita lakukan enkripsi data dengan menggunakan metode RSA, plainteks yang digunakan adalah ROBERT yang di enkripsi menggunakan caesar cipher menjadi VSFIVX
Plainteks : VSFIVX

m1: 86
m2: 83
m3: 70
m4: 73
m5: 86
m6: 88
$c = m^e mod(n)$
c = *cipherteks*
m = *message*/*plainteks*
e = kunci *private*
n = modulo Pembagi

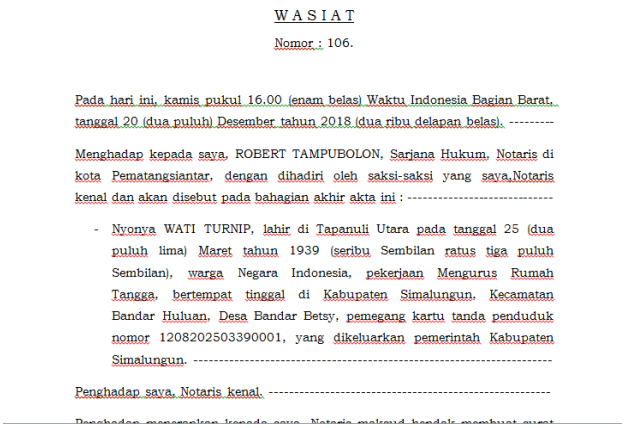
Enkripsi: 129 812 254 593 129 672
$c = m^e mod(n)$
$c1 = 86^{25} mod(989) = 129$
$c2 = 83^{25} mod(989) = 812$
$c3 = 70^{25} mod(989) = 254$
$c4 = 73^{25} mod(989) = 593$
$c5 = 86^{25} mod(989) = 129$
$c6 = 88^{25} mod(989) = 672$
Deskripsi : 86 83 70 73 86 88
$m = c^e mod(n)$
$m1 = 129^{37} mod(989) = 86$
$m2 = 812^{37} mod(989) = 83$
$m3 = 254^{37} mod(989) = 70$
$m4 = 593^{37} mod(989) = 73$
$m5 = 129^{37} mod(989) = 86$
$m6 = 672^{37} mod(989) = 88$

## HASIL DAN PEMBAHASAN


Gambar 7. Tampilan *Form Login*



Gambar 8. Tampilan Hasil Enkripsi surat Wasiat



W A S I A T

Nomor : 106.

Pada hari ini, kamis pukul 16.00 (enam belas) Waktu Indonesia Bagian Barat, tanggal 20 (dua puluh) Desember tahun 2018 (dua ribu delapan belas). ---------

Menghadap kepada saya, ROBERT TAMPUBOLON, Sarjana Hukum, Notaris di kota Pematangsiantar, dengan dihadiri oleh saksi-saksi yang saya,Notaris kenal dan akan disebut pada bahagian akhir akta ini : ----------

- Nyonya WATI TURNIP, lahir di Tapanuli Utara pada tanggal 25 (dua puluh lima) Maret tahun 1939 (seribu Sembilan ratus tiga puluh Sembilan), warga Negara Indonesia, pekerjaan Mengurus Rumah Tangga, bertempat tinggal di Kabupaten Simalungun, Kecamatan Bandar Huluan, Desa Bandar Betsy, pemegang kartu tanda penduduk nomor 1208202503390001, yang dikeluarkan pemerintah Kabupaten Simalungun. ----------

Penghadap saya, Notaris kenal. ----------

Gambar 9. Tampilan Hasil Dekripsi Surat Wasiat

Dalam pembahasan ini menjelaskan *spesifikasi* kebutuhan sistem, prosedur kerja sistem serta kelemahan dan kelebihan sistem.

Kebutuhan *Software* diantaranya *web* sebagai aplikasi bahasa pemrograman yang digunakan, *xampp* sebagai server, *adobe dreamwaver Cs* 6 sebagai aplikasi desain *from.* Kebutuhan *Hardware* diantaranya untuk menjadikan aplikasi pengamanan data maka komputer yang mengoperasikan aplikasi ini harus memiliki komponen perangkat keras minimal yaitu p*rocessor* minimal setara *Dual-Core*, *memory ram* 2 GB, *hardisk minimal* 500 GB. Tampilan menu utama terdapat menu aplikasi yaitu menu Enkripsi *file*, Dekripsi *file* dan *logout.* Pada menu utama pilih menu Enkripsi *file*, jika sudah selesai maka selanjutnya muncul *form* pencarian *file* yang akan di enkripsi. Jika sudah selesai pilih *file* yang akan di enkripsi. Kemudian pengisian kunci *(n)* 989 dan *(d)* 25 untuk proses selanjutnya dilakukan setelah memilih *file* yang akan di enkripsi.

Jika semua benar maka tampilan berhasil dan disarankan untuk mendownload *file document* yang di enkripsi. Untuk melakukan dekripsi kembali dilakukan ke form utama. klik menu dekripsi lalu input kemudian pilih file untuk didekripsi. Pengisian kunci sebagai langkah selanjutnya dengan kunci (n) 989 dan (d) 37 dalam proses dekripsi tersebut. Jika semua benar maka tampilan berhasil dan disarankan untuk mendownload *file document* yang di enkripsi.

## KESIMPULAN

Pengamanan data pada kantor notaris memiliki beberapa kesimpulan yaitu aplikasi yang dibangun dapat membantu dalam mengamankan data *file* surat wasiat pada kantor notaris menggunakan kombinasi metode *caesar cipher* dan *RSA*, surat wasiat yang di enkripsi dan didekripsi hanya dapat dibaca oleh orang yang memiliki akses kedalam aplikasi dan sistem yang dibangun mampu memberikan keamanan yang baik sehingga data isi dari surat wasiat tidak dapat dibaca oleh orang yang tidak berkepentingan. Adapun saran-saran yang diberikan sebagai pertimbangan kepada pihak-pihak yang berkepentingan untuk mengembangkan lebih lanjut lagi dan menyempurnakan hasil dari penelitian ini sehingga nantinya ini menjadi lebih baik lagi yaitu penelitian ini dapat dikembangkan dengan menggunakan *QR Code* pada metode algoritma *RSA* dan *caesar cipher*, sebaikanya dikembangkan agar tampilan lebih dinamis dan *user friendly*, bagi pembaca yang ingin mengembangkan aplikasi ini, sebaiknya menambah tingkat keamanan dengan melakukan enkripsi lainnya.

## BIBLIOGRAPHY

Agustina, Ardelia Nidya. (2017). Pengamanan Dokumen Menggunakan Metode RSA (Rivest Shamir Adleman) Berbasis Web. *Public Knowledge Project*.

Cahyadi, Tri. (2012). Implementasi steganografi LSB dengan enkripsi vigenere cipher pada citra JPEG. *Transient: Jurnal Ilmiah Teknik Elektro*, *1*(4), 281–288.

Dosen, Materi. (2016). Pengertian dan Fungsi Kode ASCII Lengkap. Retrieved from Online Submission website: http://www.materidosen.com/2016/10/pengertian-dan-fungsi-kode-ascii-lengkap.html#more

Haji, Wachyu Hari, & Mulyono, Slamet. (2012). Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.

Hasugian, Abdul Halim. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. *Pelita Informatika Budi Darma*, *4*(2), 115–122.

Listiyono, Hersatoto. (2012). *Implementasi Algoritma kunci public pada algoritma RSA*.

Megajati, Aditya Putra, & Mutimatun, Ni'ami. (2021). *Perbandingan Hukum Wasiat*

*Harta Peninggalan Berdasarkan Hukum Islam Dan Hukum Perdata Di Indonesia*. Universitas Muhammadiyah Surakarta.

Murdani, Murdani. (2017). Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma Merkle Hellman Knapsack. *Pelita Informatika: Informasi Dan Informatika*, *6*(1), 121–124.

Nugroho, Nurcahyo Budi, Azmi, Zulfian, & Arif, Saiful Nur. (2016). Aplikasi Keamanan Email Menggunakan Algoritma Rc4. *Jurnal Saintikom*.

Pramusinto, Wahyu, Wizaksono, Nugroho, & Saputro, Ari. (2020). Aplikasi Pengamanan File Berbasis Web Dengan Metode Kriptografi Aes 192, Rc4 Dan Metode Kompresi Huffman. *Budi Luhur Information Technology*, *16*(2), 47–53.

Ridho, Muhammad Fahmi. (2017). Perancangan Aplikasi Keamanan Data dengan Algoritma Serpent. *Pelita Informatika: Informasi Dan Informatika*, *6*(1), 116–120.

Sanjaya, Umar Haris. (2018). Kedudukan Surat Wasiat Terhadap Harta Warisan Yang Belum Dibagikan Kepada Ahli Waris. *Jurnal Yuridis*, *5*(1), 67–97.

Setiadewi, Kadek, & Wijaya, I. Made Hendra. (2020). Legalitas Akta Notaris Berbasis Cyber Notary Sebagai Akta Otentik. *Jurnal Komunikasi Hukum (JKH)*, *6*(1), 126–134.

Siburian, Agustin, & Harianja, Andy Paul. (2017). *Perancangan Aplikasi Pengamanan Basis Data Menggunakan Algoritma Caesar Cipher*. *02*(479), 1–6.

Simanjuntak, Arlianti Imaria. (2016). Analisis Yuridis Terhadap Kedudukan Akta Wasiat Yang Tidak Diketahui Oleh Ahli Waris Dan Penerima Wasiat. *Premise Law Journal*, *8*, 161601.

Siregar, Hariati Novrina Dewi. (2018). *Komparasi UU no. 1 tahun 2015 dengan UU no. 14 tahun 2015 tentang pemilihan Kepala Daerah satu pasangan calon ditinjau dari fiqh siyasah*. IAIN Padangsidimpuan.

Yenni, Yenni. (2017). *Tanggung Jawab Hukum Notaris Terhadap Akta Wasiat (Testament Acte) yang Dibuat Dihadapan Notaris di Kabupaten Batang*. Fakultas Hukum UNISSULA.

Yulian, Ahmat Yavi. (2018). *Pengembangan Authentifikasi QR Code Menggunakan Algoritma RSA pada Aplikasi Delivery Order Makanan Berbasis Android*.Universitas Muhammadiyah Jember.