PROPOSAL PENELITIAN

SISTEM PERLINDUNGAN DOKUMEN BERHARGA DENGAN MENGGUNAKAN METODE *PUBLIC KEY CRYPTOGRAPHY*

Muhammad Alim Bahri

D03219009

DOSEN PEMBIMBING:

Dr. Eng. Ady Wahyudi Paundu S.T., M.T.

PROGRAM PASCASARJANA UNIVERSITAS

HASANUDDIN MAKASSAR

2020

KATA PENGANTAR

Segala puji hanya milik Allah Subhanahu Wa Ta'ala yang telah memberikan rahmat, hidayah, taufik dan pertolongan-Nya dalam menyelesaikan proposal tesis yang berjudul "**Sistem Perlindungan Dokumen Berharga Dengan Menggunakan Metode *Public Key Cryptography***" sebagai salah satu syarat dalam menyelesaikan jenjang Pascasarjana pada Departemen Teknik Elektro Fakultas Teknik Universitas Hasanuddin. Sholawat serta salam semoga tetap tercurahkan kepada Nabi Muhammad Shallallahu 'alaihi Wa Sallam, beserta keluarga dan para sahabatnya yang telah membimbing kita dari jalan kegelapan menuju jalan yang terang benderang.

Penulis menyadari bahwa tanpa bantuan dari berbagai pihak, sangatlah sulit untuk menyelesaikan proposal tesis ini. Oleh karenanya, penulis berterima kasih kepada seluruh dosen dan staf pegawai Departemen Teknik Elektro, Universitas Hasanuddin, dan seluruh pihak yang telah membantu dalam pembuatan proposal tesis ini.

Penulis menyadari bahwa proposal ini masih belum sempurna. Dengan demikian, penulis tetap mengharapkan saran dan kritik dengan harapan semoga tulisan ini bisa memberikan manfaat kepada seluruh pihak.

Makassar, 30 Agustus 2020

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Kemajuan di bidang teknologi informasi telah memungkinkan institusi-institusi melakukan interaksi dengan konsumen melalui jaringan komputer atau secara *online*. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut hilang atau diakses oleh orang-orang yang tidak berhak. Aspek keamanan data sebenarnya meliputi banyak hal yang saling berkaitan, tetapi khusus dalam proposal ini penulis akan membahas tentang enkripsi dan keamanan proteksi data dengan metode *public key cryptography*.

Berdasarkan data dari yang dihimpun dari TribunNews.com pada tahun 2017, Penyidik Direktorat Tindak Pidana Siber Bareskrim Polri menemukan tindak pidana pencurian puluhan data identitas sejumlah orang, dimana data yang dicuri berupa KTP, Ijazah, SIM, paspor, hingga BPJS. Berdasarkan Kasubdit I Direktorat Tindak Pidana Siber data tersebut digunakan untuk melakukan beberapa hal salah satunya untuk melakukan penyamaran dengan melakukan verifikasi di sosial media dan menggunakan data diri dari orang lain [1]**.**

Berbagai cara tetap dilakukan aparat terkait mengenai pencurian dokumen penting di Indonesia, tetapi tetap saja hal ini tidak dapat membuat jerah para pelaku kriminal. Berdasarkan data yang dihimpun dari CNN

Indonesia pada tahun 2019, Direktorat Tindak Pidana Siber Bareskrim Polri mencatat 3.429 kasus tindak pidana siber dari Januari hingga Agustus 2019 [2].

Selain pencurian dokumen, masalah yang kerap terjadi adalah kehilangan dokumen, berdasarkan data dari yang dihimpun dari Kompas.com pada tahun 2018, sebanyak 109 rumah dari 400 pintu terbakar sehingga menyebabkan banyaknya dokumen-dokumen berupa akte kelahiran, ijazah, surat tanah hingga buku nikah yang hangus terbakar [3].

Berdasarkan data-data di atas, dapat kita simpulkan bahwa Perlindungan terhadap Dokumen Berharga merupakan salah satu masalah serius yang wajib diselesaikan. saat ini telah banyak beredar program khusus proteksi data baik *freeware*, *shareware*, maupun komersial yang sangat baik. Pada umumnya program tersebut tidak hanya menyediakan satu metode saja, tetapi beberapa jenis sehingga kita dapat memilih yang menurut kita paling aman. Salah satu metode enkripsi adalah *public key cryptography*. Metode *Public key cryptography* memiliki sifat-sifat asimetrik untuk membuat fungsi satu arah, sebuah fungsi dimana semua orang dapat melakukan satu operasi (enkripsi atau verifikasi sign) akan tetapi sangat sulit untuk menginvers operasi (dekripsi atau membuat sign) tanpa informasi yang selengkap-lengkapnya. *Public key cryptography* dilakukan dengan menggabungkan secara kriptografi dua buah kunci yang berhubungan yang kita sebut sebagai pasangan kunci publik dan kunci privat. Kedua kunci tersebut dibuat pada waktu yang bersamaan dan

berhubungan secara matematis. Secara matematis, kunci privat dibutuhkan untuk melakukan operasi invers terhadap kunci public dan kunci publik dibutuhkan untuk melakukan operasi invers terhadap operasi yang dilakukan oleh kunci privat.

Jika kunci publik didistribusikan secara luas, dan kunci privat disimpan di tempat yang tersembunyi maka akan diperoleh fungsi dari banyak ke satu. Semua orang dapat menggunakan kunci publik untuk melakukan operasi kriptografi akan tetapi hanya orang yang memegang kunci privat yang dapat melakukan invers terhadap data yang telah terenkripsi tersebut. Selain itu dapat juga diperoleh fungsi dari satu ke banyak, yaitu pada saat orang yang memegang kunci privat melakukan operasi enkripsi maka semua orang yang memiliki kunci publik dapat melakukan invers terhadap data hasil enkripsi tersebut.

Salah satu titik fokus dalam membangun sebuah sistem perlindungan dokumen dengan *Public key cryptography* yaitu bagaimana meningkatkan perlindungan terhadap dokumen penting sehingga tidak mudah dicuri atau hilang. Sejauh ini, penelitian yang terkait dengan kemanan data, masih menggunakan metode kriptografi data *encryption* standar (DES). Tentunya metode ini belum efektif untuk keamanan terhadap dokumen penting. Sistem ini masih dapat dikembangkan lebih lanjut dengan menggunakan metode *Public key cryptography*. Kelebihan dari metode ini adalah hanya orang tertentu yang memiliki kunci untuk dapat membuka dokumen, sehingga dokumen lebih aman dan tidak mudah hilang. Berdasarkan latar belakang tersebut, maka penulis mengusulkan

penelitian yang berjudul **"Sistem Perlindungan Dokumen Berharga Dengan Menggunakan Metode *Public Key Cryptography*"**.

B. RUMUSAN MASALAH

Rendahnya metode perlindungan terhadap dokumen berharga membuat dokumen-dokumen tersebut mudah disalahgunakan serta mudah rusak. Untuk itu dibutuhkan sebuah inovasi untuk meningkatkan perlindungan terhadap dokumen-dokumen berharga tersebut.

C. TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah:

1. Untuk menghasilkan sistem perlindungan dokumen berharga dengan menggunakan metode *public key cryptography*.
2. Untuk menganalisis tingkat keamanan dengan menggunakan metode *public key cryptography*.

D. MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah:

1. Manfaat terhadap penulis

   Menambah pengalaman penulis dalam membuat penelitian terkhusus pada bidang *cryptography*.

2. Manfaat terhadap masyarakat

   Sebagai bahan referensi bagi pembaca dalam menambah wawasan ilmu.

3. Manfaat terhadap terhadap industri

Sebagai bahan referensi dalam mengembangkan system perlindungan dokumen berharga dengan menggunakan metode *public key cryptography*.

E. BATASAN MASALAH

Mengingat luasnya ruang lingkup penelitian ini, maka penelitian ini dibatasi pada :

1. Sistem yang dibuat hanya untuk dokumen Ijazah, KTP, dan Kartu Keluarga.
2. Metode yang diusulkan untuk membangun sistem perlindungan dokumen berharga dengan menggunakan metode *public key cryptography*.

F. SISTEMATIKA PENULISAN

Sistematika penulisan pada penelitian ini adalah :

BAB I PENDAHULUAN

Bab I berisi penjelasan tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian serta sistematika penulisan.

BAB II KAJIAN PUSTAKA

Bab II berisi penjelasan tentang landasan teori yang digunakan dalam penelitian dan kerangka pemikiran. Diuraikan pula tentang tinjauan pustaka yang merupakan penjelasan tentang hasil-hasil penelitian lainnya yang berkaitan dengan penelitian yang dilakukan. Landasan teori merupakan suatu penjelasan tentang sumber acuan terbaru dari pustaka *primer* seperti buku, artikel, jurnal, prosiding dan tulisan asli lainnya untuk mengetahui perkembangan penelitian yang relevan dengan judul atau tema penelitian yang dilakukan dan juga sebagai arahan dalam memecahkan masalah yang diteliti. Dalam bab ini juga diurakan tentang kerangka pemikiran yang merupakan penjelasan tentang kerangka berpikir untuk memecahkan masalah yang sedang diteliti, termasuk menguraikan objek penelitian serta *state of the art* dari beberapa penelitian terkait. *Road map* / tahapan – tahapan yang akan dilakukan untuk menyelesaikan penelitian juga akan di bahas pada bab ini.

BAB III METODE PENELITIAN

Bab III ini merupakan penjelasan tentang tahapan penelitian, waktu dan lokasi penelitian, jenis penelitian, bagaimana pengembangan dan penerapan sistem perlindungan dokumen berharga dengan menggunakan metode *public key cryptography*, rancangan sistem dan uraian proses dari metode yang diusulkan, dan sumber data yang digunakan.

BAB II

TINJAUAN PUSTAKA

A. LANDASAN TEORI

1. *Cryptography*

Menurut Lutfi Pratama, dkk. [8]. Kriptografi merupakan sebuah teknik yang bersifat rahasia dengan cara mengubah suatu data yang telah disimpan menjadi sebuah teks, symbol atau pun tulisan-tulisan yang sulit diartikan, sehingga data yang tersimpan tadi tidak mudah disalahgunakan oleh pihak yang tidak berkepentingan. Kriptografi klasik adalah teknik enkripsi yang digunakan dalam enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar [4].

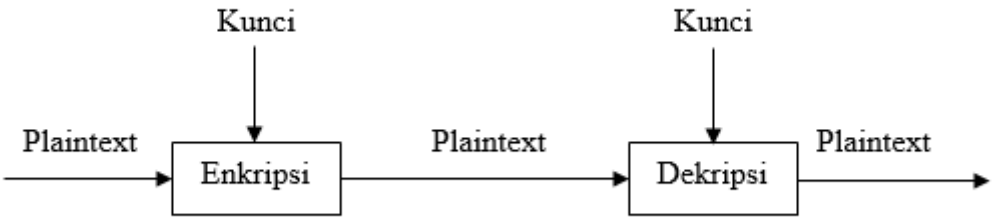
Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses

mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*).

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data [5].

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut *encryption* atau *encipherment*. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut *decryption* atau *decipherment*. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :



Gambar 1. Proses Enkripsi/Dekripsi Sederhana [5].

2. *Public Key Cryptography*

Public key cryptography (lawan dari *symmetric key cryptography*) bekerja berdasarkan fungsi satu arah. Fungsi yang dapat dengan mudah dikalkulasi akan tetapi sangat sulit untuk dibalik/*invers* atau *reverse* tanpa informasi yang mendetail. Salah satu contoh adalah faktorisasi; biasanya akan sulit untuk memfaktorkan bilangan yang besar, akan tetapi mudah untuk melakukan faktorisasi. Contohnya, akan sangat sulit untuk memfaktorkan 4399 daripada memverifikasi bahwa 53 x 83 = 4399. *Public*

key cryptography menggunakan sifat-sifat asimetrik ini untuk membuat fungsi satu arah, sebuah fungsi dimana semua orang dapat melakukan satu operasi (enkripsi atau verifikasi sign) akan tetapi sangat sulit untuk menginvers operasi (dekripsi atau membuat sign) tanpa informasi yang selengkap-lengkapnya [5].

Menurut Antonio Faonio, dkk. [8]. Secara khusus skema public key menggabungkan universal hash-proof (HPS) bersama dengan one-time lossy filter (OTLF) yang terlebih dahulu mengotentikasi ciphertext yang dimana keluarannya dalam keadaan acak untuk melindungi pesan aslinya [6].

3. Algoritma Kriptografi

Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua golongan, yaitu :

a. Symmetric Algorithms

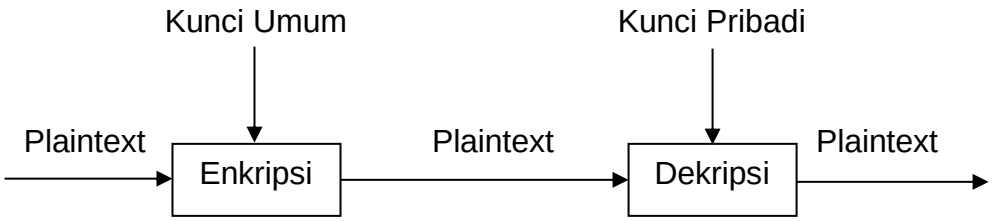
Algoritma kriptografi simeteris atau disebut juga algoritma kriptografi konvensioanl adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.

Algoritma kriptografi simeteris dibagi menajdi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok). Contoh algoritma kunci simetris yang terkenal adalah DES (*Data Encryption Standard*) [5].

b. Asymmetric Algorithms

Algoritma kriptografi nirsimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini

disebut juga algoritma kunci umum (*public key algorithm*) karena kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA dan ECC [5].



Gambar 2. Proses Enkripsi/Dekripsi *Public Key Cryptography* [5]

4. Penggunaan Algoritma *Public Key* dan *Private Key*

a. Algoritma *Public Key*

Algoritma *Public Key* digunakan untuk melakukan enkripsi, dimana cara kerja dari *Public Key* sebagai berikut, *plaintext* M dipecah menjadi blok-blok m1, m2, m3, dan seterusnya, setelah itu Setiap blok mi di enkripsikan menjadi blok ci, dengan rumus ci = mi mod n [4].

b. Algoritma *Private Key*

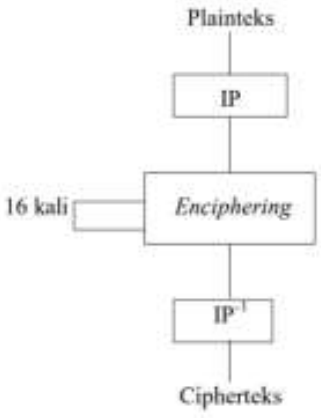
Algoritma *Private Key* digunakan untuk melakukan dekripsi, dimana cara kerja dari *Private Key* sebagai berikut, pilih ciphertext dari C, setelah itu Setiap blok ci didekripsikan menjadi blok mi, dengan rumus mi = ci mod n [4].

5. Algoritma *Encryption* dan *Decryption*

Algoritma *Encryption* dan *decryption* bisa kita asumsikan contohnya, A dan B adalah entitas yang ingin berkomunikasi mengirim dan menerima pesan secara aman melalui publik jaringan. Kemudian kedua entitas harus menghasilkan private dan kunci publik. Kunci publik harus didistribusikan dan bersifat pribadi kunci harus disimpan secara rahasia dengan mereka. Asumsikan bahwa, A mengirim pesan ke B dengan mengenkripsi pesan dengan kunci publik B. PUB. B mendekripsi pesan ini dengan kunci pribadinya PRB hanya diketahui olehnya. [13]

6. Data *Encryption Standard* (DES)

Data *Encryption Standard* (DES) merupakan algoritma kunci-simetris, yang dimana kunci yang sama digunakan untuk enkripsi dan dekripsi. Algoritma Data *Encryption Standard* termasuk ke dalam blok cipher, dimana data tergabung dalam blok berukuran masing-masing 64 bit. DES mengenkripsikan 64bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau sub-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit. [7]



Gambar 2. Skema global algoritma Data *Encryption Standard* [7]

Terdapat tiga Skema Global Dari Algoritma DES, yaitu:

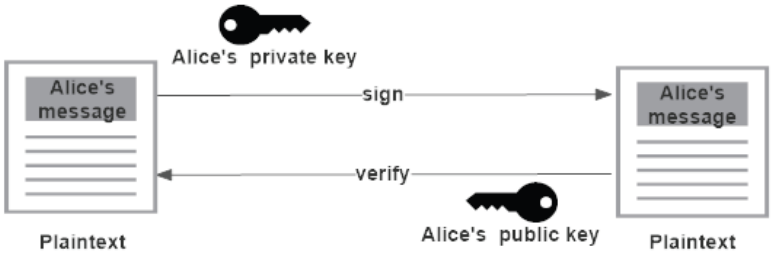
1. Blok *plaintext* dipermutasi dengan matriks permutasi awal (*Initial Permutation* atau IP).
2. Hasil permutasi awal kemudian di*enchipering* sebanyak 16 kali putaran. Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil *enchipering* kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP-1) menjadi blok *ciphertext*.

7. *Cryptosystem*

Setiap pengguna sistem kriptografi dapat menyimpan keduanya, yaitu kunci publik dan kunci privat yang dirahasiakan, sedangkan kunci publik di publikasikan ke seluruh jaringan. Pengirim pesan dapat menggunakan kunci publik dari penerima untuk mengenkripsi pesan, di samping itu, penerima dapat menggunakan kunci pribadinya untuk mendekripsi teks tersandi untuk mendapatkan pesan asli. Tidak mungkin dapatkan pesan asli tanpa mengetahui kunci privatnya. Karenanya, keamanan di sini hanya bergantung pada kerahasiaan kunci pribadi, bukan kerahasiaan algoritma. Enkripsi bisa dilakukan sebelum dekripsi dan penandatanganan sebelum memverifikasi [9]**.**

8. *Digital Signatures*

Digital Signatures terhadap suatu dokumen adalah sidik jari dari dokumen tersebut beserta *timestamp*-nya dienkripsi dengan menggunakan kunci privat pihak yang menandatangani. Tanda tangan digital memanfaatkan fungsi *hash* satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Keabsahan tanda tangan digital itu dapat diperiksa oleh pihak yang menerima pesan [9].



Gambar 5. Skema penandatanganan dan *veryfing* [9]

B. PENELITIAN TERKAIT

Beberapa penelitian terkait mengenai deteksi rambu dan marka jalan adalah sebagai berikut:

1. (Jaewon Noh, dkk, 2016) pada penelitian ini mngusulkan otentikasi dan pertukaran kunci untuk berkomunikasi antar pengguna dengan aman dalam skala jaringan Wi-Fi dengan menerapkan *public key cryptography*. Penelitian ini bertujuan untuk dapat melindungi pengguna dari beberapa serangan di jaringan Wi-Fi yang sama. Hasil dari penelitian ini berdasarkan *Traffic analysis* dapat melindungi informasi dengan otentikasi yang dikirim dengan di engkripsi menggunakan *public key* AP sehingga meskipun penyerang menangkap paket selama akses prosedurnya, penyerang harus memecahkan kunci pribadi AP. [8]
2. (Reem Alfaifi, 2017) pada penelitian ini menerapkan *cryptosystem* dengan menggunakan dua pasang kunci yaitu public/private, yang dimana untung menghasilkan kunci public/private menggunakan teorema Euler dan Fermat *little*. Penelitian ini menghasilkan algoritma dan perhitungan dari ciphertext yang lebih efisien sehingga akan menjadi lebih cepat. [9]
3. (Leihong Zhang, dkk, 2019) pada penelitian ini mengusulkan skema enkripsi beberapa gambar yang menggabungkan kriptografi kunci publik dan pola basis Hadamard. Dalam Penelitian ini kelayakan serta

keamanan metode yang diusulkan diverifikasi dengan simulasi numerik, dimana hasil dari penelitian ini koefisien korelasi rata-rata dari gambar asli berbeda dalam arah horizontal, vertikal dan diagonal yaitu sekitar 0,8, dan korelasinya sangat kuat. Namun, koefisien korelasi gambar setelah enkripsi dalam tiga arah mendekati 0 di sekitar 0,02, dan korelasinya sangat lemah, yang menunjukkan bahwa enkripsi memiliki kinerja yang baik dalam hal keamanan. [10]

4. (Kaibin Huang, dkk, 2017) dalam penelitian ini mengusulkan skema engkripsi komutatif satu kali dengan menggunakan dua algoritma yaitu engkripsi komutatif dan dekripsi komutatif. Pesan diengkripsi secara komutatif atau satu kali, dan pesan yang diengkripsi secara komutatif harus didekripsi dengan menggunakan dekripsi komutatif, dengan menggunakan engkripsi komutatif terbukti aman berdasarkan IND-CPA. [11]
5. (Mazhar Islam, dkk, 2015) dalam penelitian menggunakan kunci dalam skema engkripsi kunci simetris dengan menggunakan gambar sebagai kunci rahasia, dimana pesan akan diubah menjadi kode biner 8-bit, lalu kode 8-bit dipindai untuk mencari nilai piksel gambar yang diwakili oleh kode 8-bit yang sama, dengan menggunakan skema ini maka kemananan lebih tinggi karena ukuran kuncinya sangat besar sehingga dari hasil yang telah dilakukan dapat disimpulkan bahwa skema yang digunakan lebih baik dari pada AES, 3DES, dan DES. [12]

C. STATE OF THE ART

Dalam penelitian ini tidaklah terlepas dari penelitian-penelitian sebelumnya yang dirangkum dalam *state of the art*. Adapun penelitian yang

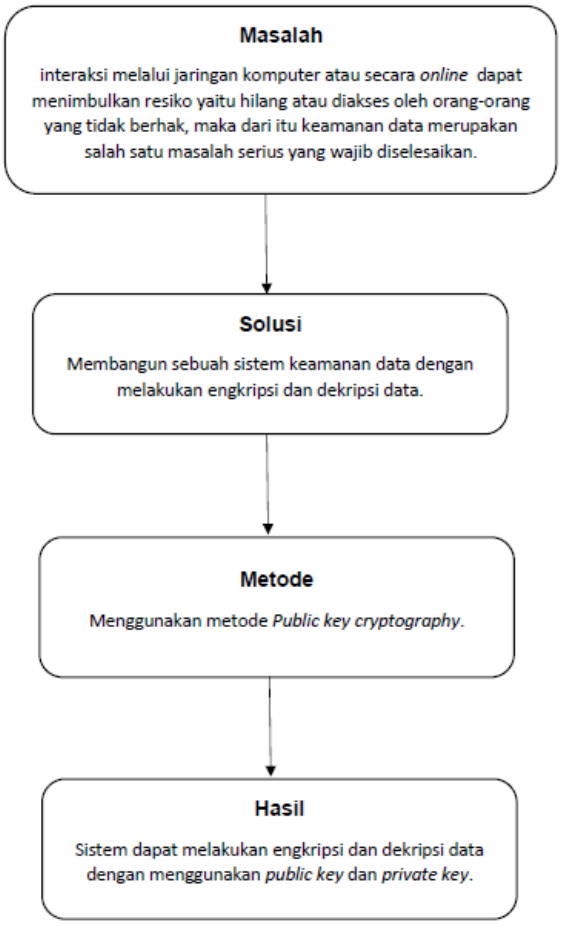
terkait mengenai keamanan data dengan menggunakan metode *public key cryptography* dan *face recognition* telah kami rangkum dalam Tabel 1.

Tabel 1. State of The Art

No.	Judul	Penulis	Penerbit	Tahun	Metode	Hasil
1	Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography	Jaewon Noh, et al	International Conference on Consumer Electronics-Asia (ICCE-Asia)	2016	Algoritma public key cryptography	Hasil dari penelitian ini berdasarkan *Traffic analysis* dapat melindungi informasi dengan otentikasi yang dikirim dengan di engkripsi menggunakan *public key* AP sehingga meskipun penyerang menangkap paket selama akses prosedurnya, penyerang harus memecahkan kunci pribadi AP.
2	*Probabilistic Cryptosystem with Two Pairs of Private/Public Keys*	Reem Alfaifi	*IEEE International Conference on Electrical and Computing Technologies and Applications* (ICECTA)	2017	Teorema Euler dan Fermat *little*	Penelitian ini menghasilkan algoritma dan perhitungan dari ciphertext yang lebih efisien sehingga akan menjadi lebih cepat.
3	Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography	Leihong Zhang, et al.	IEEE Photonics Journal	2019	*Public key cryptography* dan pola Hadamard	Hasil dari penelitian ini koefisien korelasi rata-rata dari gambar asli berbeda dalam arah horizontal, vertikal dan diagonal yaitu sekitar 0,8, dan korelasinya sangat kuat. Namun, koefisien korelasi gambar setelah enkripsi dalam tiga arah mendekati 0 di sekitar 0,02, dan korelasinya sangat lemah, yang menunjukkan bahwa enkripsi memiliki kinerja yang baik dalam hal keamanan.
4	*One-Time-Commutative Public Key Encryption*	Kaibin Huang, et. al.	*IEEE Computing Conference*	2017	*Normalisasi RGB and SVM Classifier*	Dalam penelitian ini Pesan diengkripsi secara komutatif atau satu kali, dan pesan yang diengkripsi secara komutatif harus didekripsi dengan menggunakan dekripsi komutatif, dengan menggunakan engkripsi komutatif terbukti aman berdasarkan IND-CPA
5	*A New Symmetric Key Encryption Algorithm using Images as Secret Keys*	Mazhar Islam, et. al.	*IEEE International Conference on Frontiers of Information Technology (FIT)*	2015	Engkripsi kunci simetris dengan menggunakan gambar	Dengan menggunakan skema ini maka kemananan lebih tinggi karena ukuran kuncinya sangat besar sehingga dari hasil yang telah dilakukan dapat disimpulkan bahwa skema yang digunakan lebih baik dari pada AES, 3DES, dan DES

D. KERANGKA PIKIR

Kerangka pikir akan ditampilkan pada Gambar 6, yang menjelaskan alur penelitian yang akan dilakukan. Pada tahap pertama menjelaskan permasalahan yang ada yaitu interaksi melalui jaringan komputer atau secara *online* dapat menimbulkan resiko yaitu hilang atau diakses oleh orang-orang yang tidak berhak, maka dari itu keamanan data merupakan salah satu masalah serius yang wajib diselesaikan. Solusi yang akan ditawarkan adalah Membangun sebuah sistem keamanan data dengan melakukan engkripsi dan dekripsi data. Metode yang diusulkan yaitu Menggunakan metode *Public key cryptography*. Dan tahap akhir yang diharapkan yaitu Sistem dapat melakukan engkripsi dan dekripsi data dengan menggunakan *public key* dan *private key*.



Gambar 6. Kerangka Pikir Penelitian

BAB III

METODE PENELITIAN

A. TAHAPAN PENELITIAN

Pada penelitian ini, tahapan yang akan di lakukan adalah sebagai berikut:

1. Studi literatur mengenai penelitian yang terkait dengan deteksi rambu dan marka jalan yang akan digunakan untuk tahap *pre-processing* dan tahap identifikasi objek.
2. Perancangan sistem sebagai proses yang dilakukan dengan membuat sistem yang dimulai dari tahap *design system* sampai pada tahap system dapat melakukan engkripsi dan dekripsi dengan menggunakan *public key*, *private key*.
3. Melakukan pengujian dan analisa sistem yang dibuat sesuai dengan metode yang digunakan untuk mengetahui tingkat keberhasilan sistem.
4. Pembuatan laporan untuk publikasi dan laporan akhir tesis.

B. WAKTU DAN LOKASI PENELITIAN

1. Waktu

   Waktu penelitian akan dilaksanakan selama 10 bulan.

2. Lokasi Penelitian

   Penelitian ini dilaksanakan di lingkup Prodi Teknik Informatika Universitas Hasanuddin, Gowa, Sulawesi Selatan.

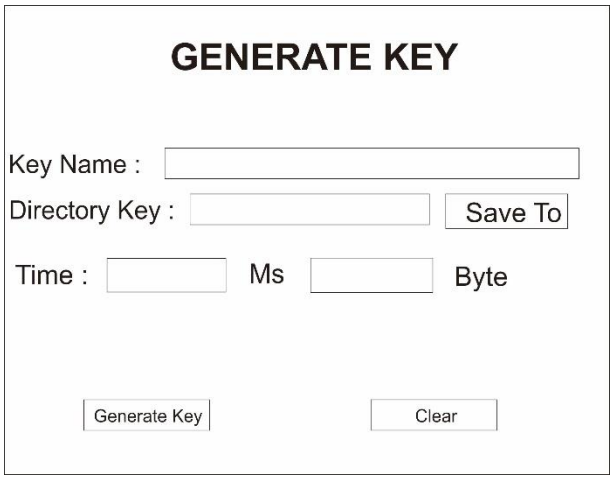
C. JENIS PENELITIAN

Jenis penelitian ini merupakan penelitian eksperimental yang bersifat analisis dengan penelusuran sumber-sumber tertulis (*library*

research), dipadukan dengan pengumpulan data-data *factual* dari sistem perlindungan dokumen berharga dengan menggunakan metode *public key cryptography*.

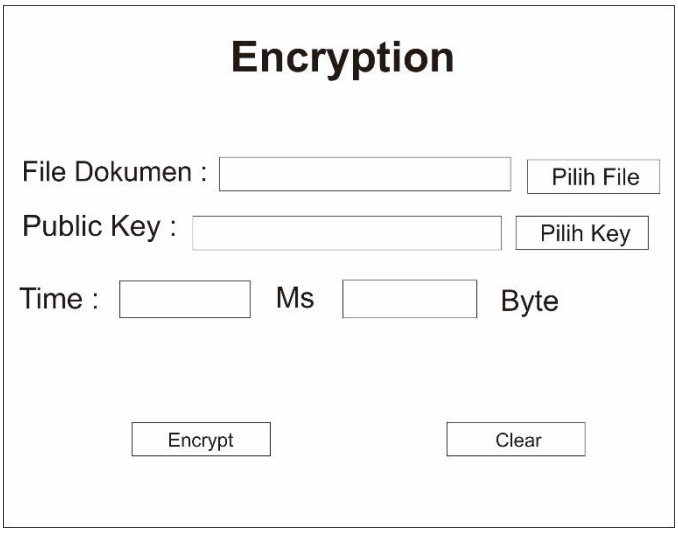
D. DESAIN SISTEM

Rancangan sistem yang diusulkan dapat dilihat pada gambar 7 sampai dengan gambar 12 berikut.



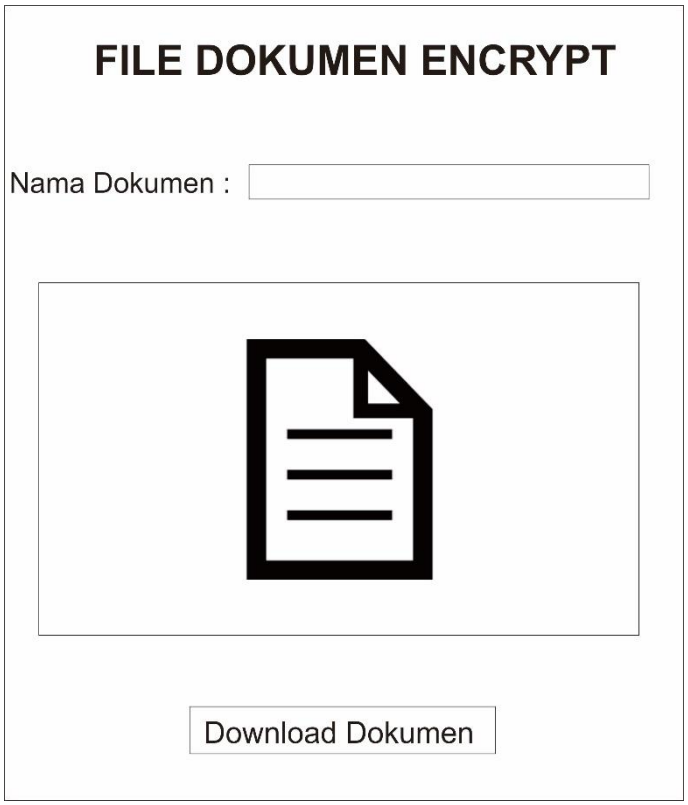
Gambar 7. *Form Generate Key*

Form Generate Key yang berfungsi untuk membuat dua buah kunci yaitu *public key* dan *private key*. Dua buah kunci ini nantinya akan digunakan pada saat melakukan enkripsi dan dekripsi. Pengguna harus membuat nama kunci dan dilanjutkan dengan menentukan lokasi untuk menyimpan kunci tersebut lalu pengguna menekan tombol *generate key, dimana key di generate* menggunakan algoritma Asymmetric untuk menghasilkan *public key* dan *private key*.



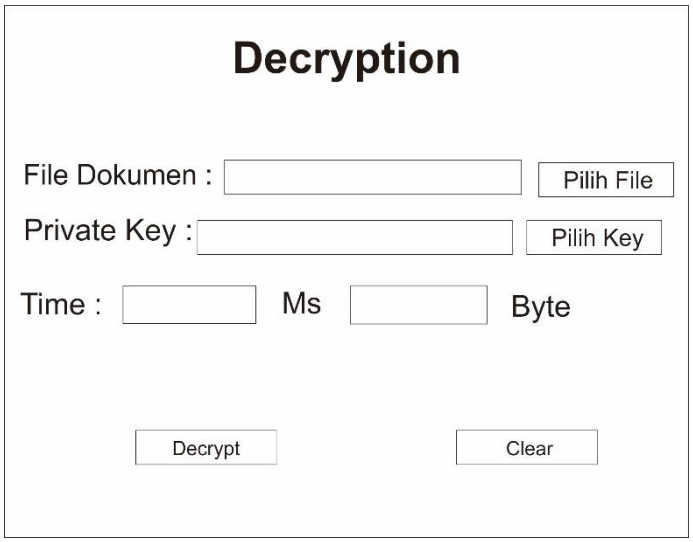
Gambar 8. *Form Encryption*

Pada rancangan layar *form encryption*, *form* ini berfungsi untuk melakukan enkripsi pada dokumen berharga. Pertama pengguna harus memilih dokumen terlebih dahulu, selanjutnya pengguna memilih *public key* yang sebelumnya sudah dibuat di *form generate key*, selanjutnya pengguna menekan tombol *encrypt*.



Gambar 9. *Form File Dokumen Encrypt*

Pada rancangan layar *form* file dokumen *encrypt*, *form* ini berfungsi untuk melakukan *download* dokumen yang telah berhasil di *encrypt,* jika *public key* seusai dan berhasil digunakan maka dokumen yang telah di *encrypt* dapat didownload.

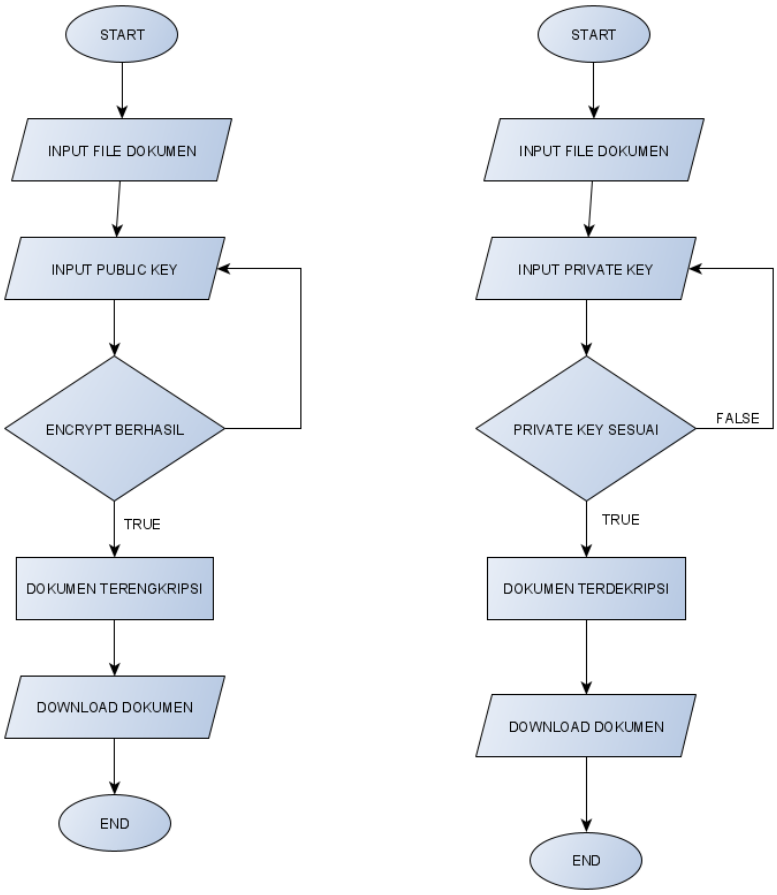


Gambar 10. *Form Decryption*

Pada rancangan layar *form decryption*, *form* ini berfungsi untuk melakukan dekripsi pada dokumen. Sama seperti proses di *form encryption*, pertama pengguna harus memilih dokumen terlebih dahulu, selanjutnya pengguna memilih *private key* yang sebelumnya sudah dibuat di *form generate key*, selanjutnya pengguna menekan tombol *decrypt*.

Gambar 11. *Form* Dokumen Decrypt

Pada rancangan layar *form* file dokumen *decrypt*, *form* ini berfungsi untuk melakukan *download* dokumen penting yang telah berhasil di *decrypt,* jika *private key* yang dimasukkan benar maka dokumen yang telah di *decrypt* dapat didownload.



Gambar 12. Flowchart *Encryption* dan *Decryption*

Pada Gambar 12 dijelaskan mengenai *flowchart* dari proses *encryption* dan *decryption*. Dimana pada proses *encryption* dokumen yang akan di *encrypt* dimasukkan lalu *public key* yang telah di buat di masukkan, setelah itu dokumen akan di *encryption*, jika *encryption* berhasil maka dokumen akan di *encrypt* dan dokumen yang telah di *encrypt* dapat di *download*, namun jika *encryption* gagal maka akan kembali memasukkan *public key*.

Untuk proses *decryption,* pertama pengguna akan memasukkan dokumen yang akan di *decrypt*, selanjutnya *private key* yang telah di buat di

masukkan, jika *private key* yang dimasukkan tidak sesuai maka kembali memasukkan *private key* hingga *private key* sesuai, jika *private key* sesuai maka dokumen akan di *decrypt* dan dokumen yang telah di *decrypt* dapat di *download*.

E. SUMBER DATA

Pengambilan data untuk *data testing* berupa dokumen Ijazah, KTP, dan Kartu Keluarga akan diambil dari data pribadi peneluis. Selain itu, berbagai literatur-literatur yang berkaitan dengan penelitian ini juga menjadi sumber data pendukung yang tentu sangat bermanfaat bagi penelitian ini.

F. INSTRUMEN PENELITIAN

1. Software
   a). Sistem Operasi Windows 10-64 bit
   b). Xampp
   c). Sublime
   d). Chrome Browser
   f). Microsoft Office 2016 64 bit
2. Hardware
   1) AMD ® 2nd Generation Ryzen 7 2700X CPU @ 3.7 GHz Processor
   2) MSI GTX 1060 6GB OC 1759 MHz Video Graphic Card
   3) RAM 16 GB
   4) HDD 1TB

DAFTAR PUSTAKA

[1] TribunNews, Ternyata Pimpinan Saracen Curi Puluhan Data KTP dan Ijazah untuk Buat Akun Facebook Palsu (Online), https://www.tribunnews.com/nasional/2017/11/14/ternyata-pimpinan-saracen-curi-puluhan-data-ktp-dan-ijazah-untuk-buat-akun-facebook-palsu. Diakses 28 Agustus 2020.

[2] CNN Indonesia, Polri Catat 3.000 Kasus Kejahatan Siber Hingga Agustus 2019 (Online), https://www.cnnindonesia.com/teknologi/20191029183819-185-443890/polri-catat-3000-kasus-kejahatan-siber-hingga-agustus-2019, Diakses 28 Agustus 2020.

[3] Kompas, Korban Kebakaran Minta Anies Bantu Urus Dokumen yang Hangus (Online), https://megapolitan.kompas.com/read/2018/03/30/13103741/korban-kebakaran-minta-anies-bantu-urus-dokumen-yang-hangus Diakses 28 Agustus 2020.

[4] L. Pratama *et al.*, “Pengamanan Table Database Menggunakan,” vol. 1, no. 3, pp. 925–930, 2018.

[5] I. SUPRAPTI, “Studi Sistem Keamanan Data Dengan Metode Public Key Cryptography.” 2003.

[6] A. Faonio and D. Venturi, “Efficient public-key cryptography with bounded leakage and tamper resilience,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10031 LNCS, pp. 877–907, 2016.

[7] A. A. Permana, "Application of cryptography with data encryption standard (des) algorithm in picture 1,2," pp. 82-87, 2020.

[8] J. Noh, "Secure key exchange scheme for WPA / WPA2-PSK using public key cryptography," pp. 2-5, 2016.

[9] M. R. Alfaifi, “Probabilistic Cryptosystem with Two Pairs of Private / Public,” 2017.

[10] K. Wang, "Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography Multiple-Image Encryption Mechanism," vol. 11, no. 4, pp. 1-14, 2019.

[11] Y. Chen, “One-Time-Commutative Public Key Encryption,” no. July, 2017.

[12] M. Islam, M. Shah, Z. Khan, T. Mahmood, and M. J. Khan, “A New Symmetric Key Encryption Algorithm using Images as Secret Keys,” pp. 17–21, 2015.

[13] M. Srinivas, "for Public key Cryptosystems," pp. 1300-1303, 2017.