BAB II
LANDASAN TEORI

2.1. Kriptografi

Asal – usul kata kriptografi merupakan dari bahasa Yunani yang berasal dari dua kata, yaitu *crypto* dan *graphia*. *Crypto* dapat diartikan rahasia, dan arti kata *graphia* ialah tulisan, sehingga kriptografi dapat diartikan suatu tulisan yang bersifat rahasia. Menurut istilah, kriptografi merupakan ilmu yang digunakan untuk menjaga keaslian sebuah pesan agar orang lain tidak mudah menyalahgunakan. Menurut Menezes, kriptografi adalah sebuah ilmu yang membahas teknik matematis yang berkaitan dengan topik keamanan informasi(Munir, 2019). Semakin berkembangnya zaman, kegunaan kriptografi bertambah pula. Kegunaan lain dari kriptografi antara lain digunakan untuk mengidentifikasi sebuah pengiriman pesan, mengenali tanda tangan digital dan menguji keaslian pesan dengan menggunakan sidik jari digital. Pada algoritma kriptografi aman tidak suatu algoritma ditentukan oleh bagaimana algoritma tersebut bekerja. Algoritma yang seperti ini biasa disebut dengan algoritma terbatas(Rsa, 2016). Algoritma terbatas adalah algoritma yang digunakan oleh suatu organisasi atau sekelompok manusia untuk merahasiakan pesan yang mereka kirim. Pesan tersebut hanya akan diketahui oleh sekelompok manusia pada kumpulan tersebut. Jika suatu hari ada salah satu anggota yang keluar dari kumpulan tersebut, maka algoritma yang digunakan untuk mengirim pesan harus diganti. Jika tidak diganti, akan didapatkan masalah dikemudian hari. Keamanan kriptografi modern terletak pada bagaimana cara kita merahasiakan kunci yang kita miliki, tanpa harus merahasiakan algoritma tersebut kepada orang lain. Kegunaan dari kunci ini sama dengan kegunaan *password*. Jika seluruh keamanan

algoritma bergantung pada kunci yang akan digunakan, maka algoritma tersebut dapat diumumkan dan dianalisis oleh orang lain (Muhammad Sholeh, 2014).Jika algoritma yang telah diumumkan bisa dipecahkan oleh orang lain dalam waktu yang singkat, maka algoritma tersebut kurang aman untuk digunakan. Kesulitan dalam mengolah data ataupun mengolah pesan yang akan disampaikan bukanlah syarat dari algoritma kriptografi yang baik. Yang lebih penting, algoritma kriptografi yang baik harus memenuhi empat persyaratan berikut :

1. Kerahasiaan.

   Kerahasiaan yang dimaksud dalam hal ini adalah menjaga informasi dari orang lain, kecuali yang memiliki akses terhadap kunci untuk membuka pesan tersebut.
2. Autentikasi.

   Autentikasi adalah berhubungan dengan pengenalan informasi. Pengirim dan penerima harus dapat dikenali dengan baik. Serta harus memastikan tidak ada penyusup dalam proses pengiriman pesan.
3. Integritas data.

   Integritas data yang dimaksudkan adalah sistem yang digunakan harus dapat mendeteksi bahwa benar-benar tidak ada manipulasi data oleh pihak manapun yang tidak memiliki kepentingan.
4. Non-repudiasi

   Non-repudiasi atau disebut juga nirpenyangkalan merupakan usaha untuk mencegah penyangkalan. Penyangkalan yang dimaksud bisa pada proses pengiriman maupun penerima pesan.

2.1.1. Pesan, Plaintext, dan Chipertext

Pesan merupakan istilah dalam ilmu kriptografi yang dapat diartikan sebagai data atau informasi yang mudah dimengerti maknanya

(Dadan Rosnawan, 2011). Pada ilmu kriptografi pesan lebih sering disebut sebagai *plaintext* (pesan asli). Pada file citra pesan asli biasa disebut *plain-image*, sedangkan citra yang terenkripsi biasa disebut *cipher-image*. Pesan biasanya berupa infomasi yang dikirim menggunakan saluran komunikasi ataupun disimpan dalam bentuk teks, gambar, video, dan lain-lain. Supaya pesan tersebut tidak mudah disalahgunakan oleh pihak yang tidak berwenang, maka pesan tersebut perlu disandikan. Bentuk pesan yang telah disandikan adalah *ciphertext*. Pesan yang telah tersandi (*ciphertext*) harus dapat diubah kembali menjadi pesan asli (*plaintext*).

2.1.2. Enkripsi dan Dekripsi

Pada ilmu kriptografi terdapat istilah enkripsi dan dekripsi. Enkripsi adalah proses mengubah *plaintext* (pesan asli) menjadi *chipertext* (pesan tersandi). Sedangkan dekripsi merupakan tahapan mengembalikan *ciphertext* (pesan tersandi) menjadi plaintext sesuai pesan asli. Pada bidang kriptografi, enkripsi dapat diartikan sebagai sebuah proses mengamankan sebuah informasi dengan cara mengubah informasi tersebut agar tidak mudah dibaca tanpa bantuan pengetahuan/ilmu khusus.

Konsep matematis pada algoritma kriptografi ditunjukkan pada relasi dari dua buah himpunan. Himpunan yang pertama merupakan himpunan yang elemennya *plaintext* dan himpunan kedua merupakan himpunan yang elemennya berisi *chipertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen dari kedua himpunan tersebut.Misalkan A menyatakan *plaintext* dan B menyatakan *chipertext*, maka fungsi enkripsi E memetakan A ke B,

$$E(A) = B \quad (2.1)$$

Fungsi dekripsi D memetakan B ke A,

$$D(B) = A \quad (2.2)$$

Kemudian proses dekripsi mengembalikan pesan ke pesan asal maka persamaannya menjadi :

$$D(C(A)) = A \quad (2.3)$$

2.1.3. Macam - macam Algoritma Kriptografi

Berdasarkan kunci yang digunakan algoritma kriptografi dibagi menjadi 3, algoritma simetris, algoritma asimetris, dan fungsi hash.

a. Algoritma Simetri

Algoritma simetri atau yang sering disebut algoritma klasik merupakan algoritma yang memakai kunci yang sama dalam proses enkripsi maupun dekripsi. Algoritma ini telah ada sejak 4000 tahun yang lalu. Untuk mengirimkan pesan dengan menggunakan algoritma ini, penerima pesan harus mengetahui kunci dari pesan yang akan di terimanya. Keamanan pesan yang menggunakan algoritma asimetri tergantung pada kunci yang ditentukan di awal. Jika kunci yang ditentukan tersebut diketahui oleh orang lain, maka orang itu dapat melakukan enkripsi dan dekripsi pesan. Algoritma yang menggunakan kunci simetri antara lain:

1. RC2, RC4, RC5, RC6
2. *Internatonal Data Encryption Algoritihm* (IDEA)
3. *Advanced Encryption Standard* (AES)
4. *Data Encryption Standard* (DES)
5. *One Time Pad* (OTP)

b. Algoritma Asimetri

Algoritma asimetri sering juga disebut algoritma kunci public dimana kunci yang digunakan untuk proses enkripsinya berbeda dengan kunci yang digunakan untuk proses dekripsinya. Ada dua kunci yang digunakan pada algoritma asimetri, yaitu :

1. Kunci Umum (*public key*) : kunci yang dapat diketahui oleh semua orang.
2. Kunci Privat (*private key*) : kunci yang diketahui oleh pengirim dan penerima pesan.

Kedua kunci tersebut akan saling berhubungan satu dengan yang lain. Dengan menggunakan kunci publik pesan dapat dienkripsi, namun jika tidak mengetahui kunci privatnya pesan tidak dapat didekripsi. Konsep penerimaan pesan pada algoritma asimetri adalah dimisalkan ada dua orang pengirim dan penerima pesan, maka si penerima pesan yang membangkitkan kunci dan menyimpan semua kunci. Ketika ada yang akan mengirim pesan kepada penerima, maka penerima memberikan kunci publik kepada pengirim untuk mengenkripsi pesan. Namun, kunci rahasianya hanya disimpan oleh penerima pesan selaku yang akan membuka pesan dari pengirim. Algoritma asimetris dapat mengirimkan pesan lebih aman lagi daripada algoritma simetris. Contoh algoritma asimetris antara lain:

1. RSA
2. ElGamal

3. *Digital Signature Algorithm* (DSA)
4. *Diffle-Hellman* (DH)
5. *Eliptic Curve Cryptography* (ECC)

c. Fungsi Hash

Fungsi hash juga sering disebut hash satu arah (*One Way Function*), *message digest*, *fingerprint*, fungsi kompresi, dan *message authentication code* (MAC) merupakan salah satu fungsi matematika yang di gunakan dalam mengambil masukan dari panjang variabel dan mengubahnya ke dalam sebuah urutan biner dengan panjang yang sama. Fungsi hash biasanya digunakan untuk membuat sebuah sidik jari dari suatu pesan. Sidik jari pada sebuah pesan merupakan suatu tanda untuk memastikan bahwasanya pesan tersebut benar – benar terjadi.

2.1.4. Tujuan Kriptografi

Adapun tujuan dari kriptografi yang didefenisikan dalam (Munir, 2019) adalah:

1. Kerahasiaan (*confidentiality*), adalah layanan yang ditujukan untuk menjaga pesan agar tidak bisa dibaca oleh pihak yang tidak berwenang.
2. Integritas Data (*data integrity*), adalah layanan yang menjamin bahwa pesan tersebut masih asli atau belum pernah dimanipulasi selama pengirimannya.
3. Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi sebuah kebenaran kepada pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) ataupun mengidentifikasi sebuah kebenaran

sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi dan harus dapat saling mengotentikasikan satu sama lain sehingga mereka dapat memastikan sumber pesan tersebut.

4. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan sebuah penyangkalan, yaitu pengirim pesan menyangkal melakukan sebuah pengiriman ataupun penerima pesan menyangkal telah menerima pesannya.

2.2. RSA (Rivest-Shamir-Adleman)

Ide awal penemuan algoritma RSA yaitu dari *Clifford Cocks* yang ditemukan kembali oleh tiga orang peneliti yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Mereka mengumumkan temuannya pada tahun 1976, sebuah algoritma kriptografi kunci asimetri yang dikenal dengan nama algoritma kriptografi RSA. RSA merupakan singkatan dari nama belakang penemunya (Rivest, Shamir, dan Adleman) (Simargolang, 2017)

Algoritma RSA adalah salah satu algoritma kriptografi asimetri, yaitu jenis kriptografi yang menggunakan dua kunci berbeda untuk setiap proses enkripsi dan dekripsi. Dua kunci tersebut antara lain kunci publik (*public key*) dan kunci pribadi (*private key*). Kunci publik merupakan kunci yang dapat dikirimkan melalui saluran bebas, tanpa perlu adanya keamanan tertentu. Hal tersebut berbeda dengan kriptografi simetri yang hanya memiliki satu jenis kunci dan kunci tersebut harus dijaga keamanannya. Algoritma RSA mempunyai dasar konsep untuk proses enkripsi dan dekripsi yaitu bilangan prima dan aritmatika modulo. RSA menggunakan 2 angka (e dan d) sebagai kunci publik dan kunci privat.

Keamanan pada algoritma ini ditunjukkan dengan sulitnya mencari hasil faktor-faktor prima dari bilangan yang besar, yang dalam hal ini adalah memfaktorkan n menjadi a dan b. Kemudian sekali n berhasil difaktorkan menjadi a dan b, maka $m = (a - 1)(b - 1)$ dapat dihitung. Selanjutnya karena kunci enkripsi diutamakan e bebas (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan $e.d = 1 \ (mod \ m)$. Hal tersebut merupakan proses dekripsi yang dilakukan oleh orang yang tidak berhak.

1. Parameter Algoritma RSA

Pada algoritma RSA terdapat parameter-parameter yang akan digunakan dalam pengerjaan algoritma ini. Pada parameter tersebut terdapat parameter rahasia dan tidak rahasia, parameter tersebut ditunjukkan pada tabel 2.1,

No	Parameter	Sifat
1	p dan q bilangan prima	Rahasia
2	$n = p.q$	Tidak rahasia
3	$\phi(n) = (p-1)(q-1)$	Rahasia
4	e (kunci enkripsi)	Tidak rahasia
5	d (kunci dekripsi)	Rahasia
6	m (plainteks)	Rahasia
7	c (chipertext)	Tidak rahasia

Tabel 2.1 Parameter RSA

2. Algoritma Pembangkit Kunci

Sebagai algoritma kriptografi asimetri, perumusan algoritma RSA membutuhkan dua kunci yang berbeda untuk enkripsi dan dekripsi. Berikut langkah pembangkitan kunci algoritma RSA :

a. Bangkitkan dua bilangan prima untuk nilai p dan q

b. Hitung nilai $n = p \times q$

(2.4)

c. Hitung nilai g(n) = (p−1)(q −1)

(2.5)

d. Pilih nilai bilangan bulat e acak sebagai kunci publik, yang telah memenuhi syarat Greater Common Divisor (GCD) (e, g(n)) =1,1 < e < g(n)

(2.6)

e. Hitung kunci privat d maka $d \times e = 1$ (mod g(n))

(2.7)

3. Enkripsi dan Dekripsi RSA

Berikut langkah-langkah proses enkripsi dan dekripsi pada algoritma RSA :

a. Ambil kunci publik yang telah dibangkitkan pada proses sebelumnya yaitu (e,n).

b. Untuk proses enkripsi menggunakan rumus yang ditunjukkan pada Persamaan 2.8. $ci = mi\ emod n$

(2.8)

c. Ambil kunci privat yang telah dibangkitkan pada proses sebelumnya yaitu (d,n).

d. Untuk proses dekripsi menggunakan rumus yang ditunjukkan pada Persamaan 2.9.

$mi = ci\ dmod\ n$

(2.9)

dimana :

c = *chipertext*

m = *Plaintext*

e,n = kunci publik

d,n = kunci privat

2.3. Tandatangan Digital

Tanda tangan digital atau *Digital Signature* merupakan suatu tanda tangan (penanda) yang dibubuhkan kedalam data digital. Tanda tangan digital bukanlah merupakan hasil scan ataupun input tanda tangan melalui *interface* tertentu. Tanda tangan digital adalah suatu nilai kriptografis yang bergantung pada isi data itu sendiri beserta kunci yang digunakan untuk membangkitkan nilai kriptografisnya. Sehingga nilai di setiap tanda tangan digital dapat selalu berbeda tergantung data yang ditandatangani (Luthfi, n.d.) Dengan tanda tangan digital tersebut maka integritas keamanan data terjamin, dan juga digunakan untuk membuktikan asal - muasal pesan (keabsahan pengirim), dan nir-penyangkalan.

2.3.1. Sifat umum dari tanda tangan digital

Berikut sifat umum tandatangan digital adalah sebagai berikut:

1. Otentik (*authenticity*), tak bisa atau sulit ditulis maupun ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga bisa sebagai bukti, sehingga penandatangan tidak bisa mengelak lagi bahwa dulu dia tidak menandatanganinya.
2. Sah (*integrity*) untuk dokumen (pesan) itu saja atau salinannya yang sama persis. Tanda tangan itu tidak bisa dipindahkan ke dalam sebuah dokumen lainnya, meskipun dokumen itu hanya berbeda sangat sedikit. Ini juga berarti bahwa dokumen itu telah dirubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah/valid.

3. Nirpenyangkalan (*Non Repudiation*), *non repudiation* ini timbul dari keberadaan sebuah tanda tangan digital yang menggunakan enkripsi asimetris (*asymmetric encryption*). Enkripsi asimetris tersebut juga melibatkan keberadaan dari sebuah kunci privat beserta kunci publik. Suatu pesan yang sudah dienkripsi dengan menggunakan kunci privat hanya dapat di dekripsi dengan menggunakan kunci publik dari pengirimnya saja . Dengan kata lain, pengirim tidak bisa menyangkal akan keberadaan pesan tersebut karena terbukti bahwasannya pesan tersebut dapat didekripsi dengan kunci publiknya.
4. Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatangannya.

2.3.2. Penandatanganan Pesan

Berikut merupakan cara untuk menandatangani pesan yang dapat dilakukan dengan salah satu dari dua cara, yaitu:

1. Enkripsi pesan

   Mengenkripsi pesan dengan sendirinya juga menyediakan ukuran untuk sebuah otentikasi. Pesan yang terenkripsi juga sudah bisa menyatakan bahwasannya pesan tersebut telah ditandatangani.
2. Tanda tangan digital dengan fungsi hash *(hash function).*

   Pengirim pesan mulanya menghitung *message digest* dari pesan. Kemudian *message digest* didapatkan dengan cara mentransformasikan pesan dengan menggunakan fungsi hash 1 arah. Selanjutnya *message digest* akan dienkripsi menggunakan algoritma kriptografi kunci publik dan kunci privat pengirim. Hasil dari enkripsi inilah yang disebut dengan tanda tangan digital.

Selanjutnya tandatangan digital dikaitkan ke pesan dengan cara menyambungkannya (*append*) kemudian dikirim melalui saluran komunikasi.

Kemudian di tempat penerimanya, tanda tangan digital dibuktikan dengan keotentikannya menggunakan cara memverifikasi pesan, yaitu sebagai berikut:

a. Tandatangan digital didekripsikan dengan menggunakan kunci publik pengirim pesan yang menghasilkan *message digest* (MD) semula.
b. Penerima pesan mengubah pesan menjadi *message digest* (MD) menggunakan fungsi hash satu arah yang sama dengan fungsi hash yang digunakan oleh pengirim.
c. Jika MD' = MD, maka pesan dan tandatangan yang diterima memang benar berasal dari pengirim pesan.

3. Layanan Keamanan

Tanda tangan digital bisa digunakan untuk mewujudkan 3 layanan keamanan yaitu berupa otentikasi pesan, keutuhan pesan dan nirpenyangkalan.

a. Otentikasi Pesan

Contoh sistem tanda tangan digital dapat mewujudkan layanan otentikasi pesan dengan ilustrasi berikut ini :

A mengirim pesan M, beserta tanda tangan yang dibuat dengan kunci privat A. B dapat mengotentikasi pesan dengan cara memverifikasi tanda tangan dengan kunci publik A. Pesan terotentikasi bila algoritma *verify* mengembalikan nilai *True.*

b. Keutuhan Data

Selain sebagai otentikasi pesan, pada sistem tanda tangan digital yang ditambahkan fungsi hash dapat mewujudkan layanan keutuhan data beserta dengan proses *sign/verify*. Misalnya A ingin menandatangani pesan M dan mengirimnya ke B dengan menjaga keutuhan pesan. A dapat menggunakan fungsi *hash* h dan mendapatkan tanda tangan dengan cara memanggil algoritma *sign* dengan masukan *digest* M. A mengirim M, ke B. Setelah menerima M B memverifikasi *digest* M.

c. *Non-repudiation*

Layanan keamanan yang juga disediakan oleh sistem tanda tangan digital adalah *non repudiation*. Layanan *non-repudiation* membuat penolakan terhadap pesan yang telah ditandatangani menjadi tidak mungkin terjadi. Misalnya A menolak kalau dia telah menandatangi sebuah dokumen yang sebenarnya ditandatangani oleh A. B dapat membuktikan bahwa A pernah menandatangani dokumennya tersebut. Untuk mewujudkan layanan *non-repudiation* maka diperlukan pihak ketiga yang terpercaya. Pihak ketiga ini berperan sebagai penyalur antara A dan B. Pada awalnya A menandatangani dokumen M dengan menggunakan kunci privat A dan mendapatkan tanda tangan . Kemudian A mengirim pasangan M ke pihak ketiga. Pihak ketiga memverifikasi M dengan kunci publik A dan menyimpan salinan M. Pihak ketiga menandatangani M dengan kunci privat pihak ketiga dan mendapatkan . Pihak ketiga mengirimkan M,ke B. B

memverifikasi M dengan kunci publik pihak ketiga. Jika pada waktu yang akan datang A menolak telah menandatangani M, pihak ketiga memiliki salinan M tersebut.

2.4. Gambar

Gambar adalah segala sesuatu yang diwujudkan secara visual dalam bentuk dua dimensi sebagai curahan perasaan atau pikiran (Hamalik, 1986). Menurut KBBI, Gambar merupakan tiruan barang, binatang, tumbuhan dan sebagainya.

2.4.1. Jenis – Jenis gambar

Pengertian gambar adalah hasil dari penggabungan titik, garis, bidang serta warna yang menjadi suatu bentuk. Dengan pengertian gambar tersebut, maka gambar dibagi atas dua jenis. Jenis gambar tersebut adalah gambar Kreatif dan gambar konstruktif. Gambar kreatif merupakan sebuah gambar yang memerlukan imajinasi dan keahlian dalam proses pembuatannya. Yang termasuk dalam jenis gambar kreatif ini adalah jenis gambar bentuk dan jenis gambar ekspresif.

Selain gambar kreatif masih terdapat satu jenis gambar. Jenis gambar tersebut adalah jenis gambar konstruktif. Pengertian gambar konstruktif adalah sebuah gambar yang dibuat berdasarkan objek pada suatu benda. Jenis gambar konstrukftif ini dibuat sama persis objeknya, yang membedakannya hanya ukuran. Adapun yang termasuk dalam jenis gambar konstruktif adalah jenis gambar tampak, gambar perspektif dan gambar isometri.

2.4.2. Format Gambar

Berikut adalah penjelasan dari berbagai format gambar tersebut, di antaranya :

1. **PSD (*Photoshop Document*)**

   Format file ini merupakan format asli dokumen yang dimiliki oleh *Adobe Photoshop*. Format file ini juga bisa digunakan untuk menyimpan informasi *layer* dan *alpha channel* yang terdapat pada sebuah gambar, sehingga apabila suatu saat bisa dibuka maupun diedit lagi oleh para penggunanya. Format ini juga mampu menyimpan gambar dalam beberapa mode warna yang telah disediakan *Photoshop*. Pengguna dapat menyimpan dengan format file ini jika ingin mengeditnya kembali.

2. **BMP (Bitmap Image)**

   Format file ini adalah format grafis yang fleksibel untuk digunakan dalam *platform Windows* sehingga dapat dibaca oleh program grafis apapun. Format ini bisa menyimpan informasi dengan kualitas dari tingkat 1 bit hingga sampai 24 bit. Kelemahan format file ini ialah tidak mampu untuk menyimpan *alpha channel* serta ada kendala dalam pertukaran platform. Untuk membuat sebuah objek sebagai desktop *wallpaper*, simpanlah dokumen anda dengan format file ini dulu. Anda juga dapat mengkompresikan format file ini dengan kompresi RLE. Format file ini mampu menyimpan gambar dalam beberapa mode warna yaitu RGB, *Grayscale, Indexed Color*, dan *Bitmap*.

3. **EPS (Encapsuled Postcript)**

   Format file ini adalah format yang sering digunakan dalam keperluan pertukaran dokumen antar program grafis. Selain itu, format file ini sering pula digunakan ketika ingin mencetak sebuah gambar. Keunggulan format file ini ialah bisa menggunakan bahasa

postscript sehingga format file ini bisa dikenali oleh hampir semua program persiapan cetak.

Kelemahan format file ini ialah tidak dapat menyimpan *alpha channel*, sehingga banyak pengguna *Adobe Photoshop* yang menggunakan format file ini ketika gambar yang dikerjakan sudah selesai/final. Format file ini mampu menyimpan gambar dengan beberapa mode warna yaitu RGB, CMYK, *Lab, Duotone, Grayscale, Indexed Color,* serta *Bitmap*. Selain itu format file ini juga dapat menyimpan jenis *clipping path.*

4. JPG/JPEG (*Joint Photographic Expert Group*)

Format file ini dapat mengkompresikan objek dengan tingkat kualitas yang sesuai dengan pilihan yang telah disediakan. Format file ini juga sering dimanfaatkan untuk menyimpan gambar yang akan digunakan dalam berbagai macam kebutuhan halaman web, multimedia, dan publikasi elektronik lainnya. Format file ini dapat menyimpan gambar dengan beberapa mode warna RGB, CMYK, dan *Grayscale*. Format file ini juga dapat menyimpan *alpha channel*, namun dikarenakan format file ini orientasinya yang ke publikasi elektronik maka dari itu format ini berukuran relatif lebih kecil dibandingkan dengan format file lainnya.

5. GIF (*Graphic Interchange Format*)

Format file ini hanya dapat menyimpan dalam 8 bit (hanya mendukung beberapa mode warna *Grayscale*, *Bitmap* dan *Indexed Color*). Jenis format file ini ialah format standar untuk publikasi elektronik dan internet.

Format file dapat menyimpan animasi dua dimensi yang akan dipublikasikan pada internet, desain halaman web dan publikasi elektronik. Format file ini mampu mengkompresi dengan ukuran kecil menggunakan kompresi LZW.

2.5. Penelitian Sebelumnya

Penelitian tentang metode RSA dan Tanda Tangan Digital telah banyak dilakukan oleh peneliti terdahulu. Penelitian yang dilakukan menghasilkan berbagai hasil yang berbeda. Penelitian terdahulu yang menjadi acuan peneliti yang sesuai dengan penelitian saat ini antara lain:

1. Yusuf Anshori,A. Y. Erwin Dodu ,Dewa Made P. Wedananta (2019)

   Penelitian ini bertujuan untuk menerapkan algoritma kriptografi Rivest Shamir Adleman (RSA) pada tanda tangan digital. Proses pembuatan tanda tangan digital diawali dengan pembuatan message digest dari sebuah dokumen kemudian proses pembangkitan kunci publik dan kunci privat untuk mengamankan data dan untuk membuat tanda tangan digital. Kunci privat akan dikirimkan kepada penerima pesan untuk memverifikasi tanda tangan digital. Tanda tangan digital dan dokumen dikirmkan kepada penerima. Selanjutnya, pada proses verifikasi, penerima akan mengecek apakah tanda tangan tersebut cocok atau tidak dengan menggunakan kunci privat dan menghitung nilai hash (*message digest*) dari dokumen yang diterima.

   Persamaan dengan Penelitian Terdahulu :

   a. Menggunakan Algoritma RSA dan *Digital Signature*

   Perbedaan dengan Penelitian Terdahulu :

   a. Penelitian saat ini mengunakan objek file berupa gambar.

2. Nofa Riahana Fajriysh (2018)

   Keamanan data merupakan hal yang sangat penting bagi instansi maupun perusahaan. Salah satu data penting yang perlu

diamankan adalah data citra. Citra merupakan pesan multimedia yang sering disalahgunakan. Sehingga diperlukan aplikasi untuk pengamanan data citra. Salah satu ilmu yang berkaitan dengan pengamanan suatu data adalah kriptografi dan algoritma Rivest Shamir Adlemant (RSA) merupakan salah satu dari algoritma kriptografi yang dapat digunakan untuk enkripsi dan dekripsi sebuah data. Keunggulan dari algoritma RSA adalah belum ditemukannya algoritma yang tepat untuk melakukan dekripsi algoritma RSA dengan memfaktorkan bilangan yang besar menjadi faktor prima. Oleh karena itu pada penelitian ini akan diimplementasikan algoritma RSA pada sebuah file citra. Proses pengamanan file data citra pada penelitian ini dimulai dari pembangkitan kunci, enkripsi, dekripsi, dan pengujian. Hasil dari penelitian ini akan dapat digunakan untuk mengenkripsi dan mendekripsi citra dengan baik.

Persamaan dengan Penelitian Terdahulu :

a. Menggunakan Algoritma RSA
b. Data objek yang digunakan menggunakan Data berupa file citra/gambar

Perbedaan dengan Penelitian Terdahulu :

a. Penelitian saat ini mengunakan metode tambahan yaitu *Digital Signature* dan MD5