BAB II

KAJIAN LITERATUR

2.1 Pengantar

Proses pengamanan data atau yang sering disebut dengan teknik kriptografi sangat beragam dengan berbagai macam metode enkripsi data yang tidak hanya mempunyai kelebihan namun juga memiliki kekurangan pada setiap implementasi algoritma. Kriptografi masa kini berfokus kepada algoritma transformasi matematika dengan memperlakukan pesan sebagai bilangan atau elemen aljabar (Rabah, 2005) Algoritma kriptografi dibedakan menjadi dua berdasarkan jumlah kunci yang dipakai dalam proses enkripsi dan dekripsi data yaitu simetris kriptografi dan asimetris kriptografi seperti algoritma *Data Encryption Standard* (DES), *Advanced Encryption Standard* (AES), *Message Digest Algorithm 5* (MD5), *Blowfish*, etc. Penggunaan jaringan saraf tiruan juga dikelompokkan menjadi dua yaitu jaringan saraf *single-layer* dan *multi-layer* berdasarkan jumlah lapisan tersembunyi yang digunakan.

Pada pembahasan ini akan dijelaskan mengenai kriptografi termasuk teknik enkripsi dan dekripsi serta kaitannya terhadap jaringan saraf tiruan *backpropagation* dan bagaimana cara menggabungkan dua metode tersebut untuk memproses data gambar sebagai domain penelitian.

2.2 Data

Data merupakan manifestasi dari beberapa konsep intelektual, kontruksi, atau peristiwa sesungguhnya yang telah dilakukan oleh manusia dengan tujuan interaksi, komunikasi, atau tujuan penafsiran lainnya (Checkland & Holwell, 1998)

Dalam kehidupan sehari-hari umat manusia, keterkaitan interaksi dengan data tidak hanya terbatas pada batasan tempat yang sempit namun penggunaan data untuk tujuan komunikasi memiliki cakupan wilayah yang sangat luas yang melibatkan banyak orang bahkan telah mencakup proses pengiriman data antarnegara. Jenis data yang dikirimkan juga sangat beragam contohnya teks, gambar, jaringan, dan suara yang didasari oleh kebutuhan pengirim dan penerima data tersebut.

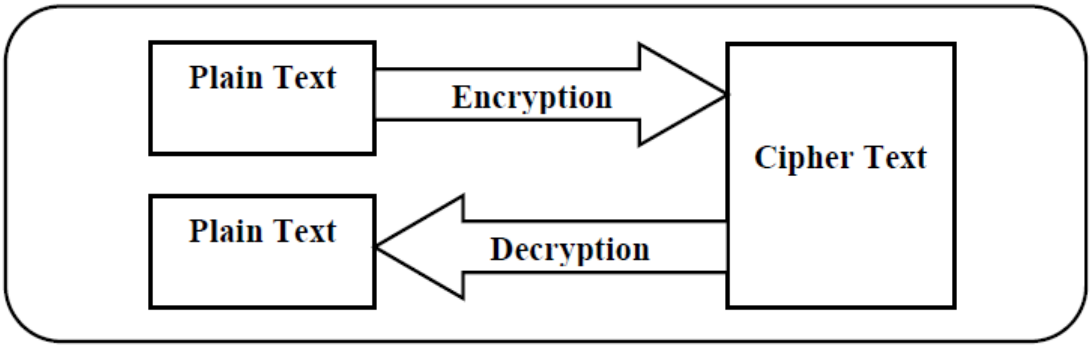
2.2.1 Data Teks

Teks merupakan tipe data umum yang sering digunakan untuk merepresentasikan informasi atau bahkan pengetahuan. Teks pada kriptografi mempunyai berbagai macam metode untuk mengkonversi teks tersebut menjadi teks sandi. Cara pemrosesan ini juga dapat menjadi salah satu cara untuk menciptakan sistem kriptografi karena penyerang data memerlukan pengetahuan bagaimana caranya data diolah sebelum algoritma kriptografi tertentu diterapkan. Dalam kebnayakan kasus enkripsi data, teks data akan dijadikan segmen atau potongan sub-data. Proses enkripsi dimulai dengan bagian dari data tersebut satu per satu atau sekaligus.

2.3 Kriptografi

Menurut Tripathi dan Agrawal (2014), yang dimaksud sebagai kriptografi adalah kemampuan untuk mengamankan data dalam rangka untuk mempertahankan informasi yang berharga dari individu yang tidak berwenang dan mengubahnya menjadi pola yang tidak dapat diidentifikasi oleh penyerang data. Kriptografi merupakan teknik yang memungkinkan penyebaran atau pengiriman data secara aman untuk megnhidari pihak tanpa izin (Mahesha, 2016). Secara prakteknya, proses kriptografi mengubah data awal yang dapat dikenali dan dimengerti menjadi bentuk yang bersifat acak yang sulit untuk dimengeri tanpa mengetahui metode untuk membuka atau menembus algoritma kriptografi tersebut. Dalam kriptografi, terdapat kunci yang digunakan sebagai bagian penting yang menentukan tingkat keamanan suatu algoritma yang berbanding lurus dengan jumlah penyerangan yang dapat terjadi (Gupta & Mittal, 2014)

Bentuk asli dari data yang dapat dipahami biasanya disebut dengan teks asli atau *plain text* contohnya "Halo ! Apa kabar?" yang akan seterusnya diproses dengan menggunakan satu atau lebih metode untuk memanipulasi kalimat tersebut dan mengubahnya menjadi *cipher text* atau teks sandi. Teks sandi terlihat seperti data yang rusak atau sembarang secara sekilas untuk memastikan bahwa tidak ada yang dapat memahami maksud dari teks sandi tersebut kecuali orang-orang yang mengetahui cara membacanya dengan menggunakan algoritma yang sesuai. Contohnya "KHOOR" adalah teks sandi untuk teks asli dari "HELLO".



Gambar II-1. Alur dari kriptografi (Tripathi dan Agrawal, 2014).

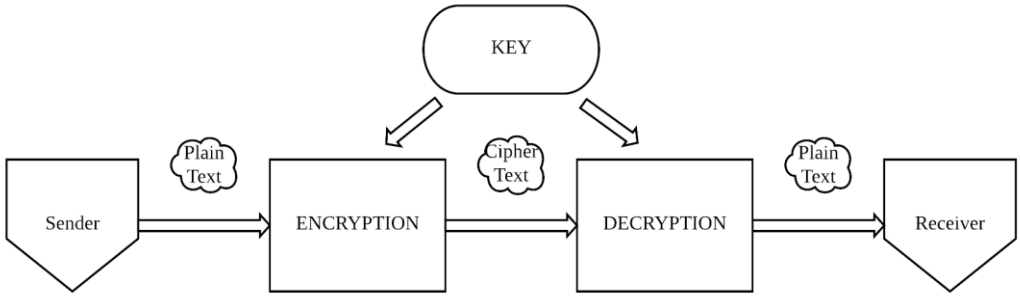
Seperti yang tampak pada gambar 2.1, process mengubah teks asli menjadi teks sandi disebut dengan proses enkripsi sementara proses sebaliknya yaitu mengubah teks sandi kembali menjadi teks asli disebut dengan dekripsi. Proses perubahan ini baik enkripsi dan juga dekripsi menggunakan kunci yang berbentuk angka numerik atau berbagai macam karakter tertentu. Keberadaan kunci ini sangat krusial untuk menetukan keamanan algoritma yang dikarenakan proses enkripsi didasarkan oleh kunci secara langsung. Kesempatan untuk melakukan intervensi secara ilegal terhadap data sejalan dengan kemampuan dari kunci yang digunakan pada sistem kriptografi (Gupta & Mittal, 2014).

Berdasarkan teknik pengimplementasian kunci yang digunakan pada tahap enkripsi dan dekripsi, kriptografi sendiri dibedakan menjadi dua tipe yaitu simetris dan asimetris kriptografi.

2.3.1 Kriptografi Simetris

Menurut pendapat Komal et al (2015) kriptografi simetris atau yang biasanya disebut dengan kriptografi kunci pribadi merupakan suatu proses pembagian kunci yang sama untuk kedua proses yang berbeda yaitu enkripsi dan

dekripsi. Penggunaan kunci secara bersama berarti pengirim data yang berupa teks asli dan penerima data yang berupa teks sandi akan menggunakan satu kunci atau berbagi kunci yang sama pada suatu regulasi sistem enkripsi dan dekripsi seperti ilustrasi yang ditunjukkan oleh gambar 2.1.

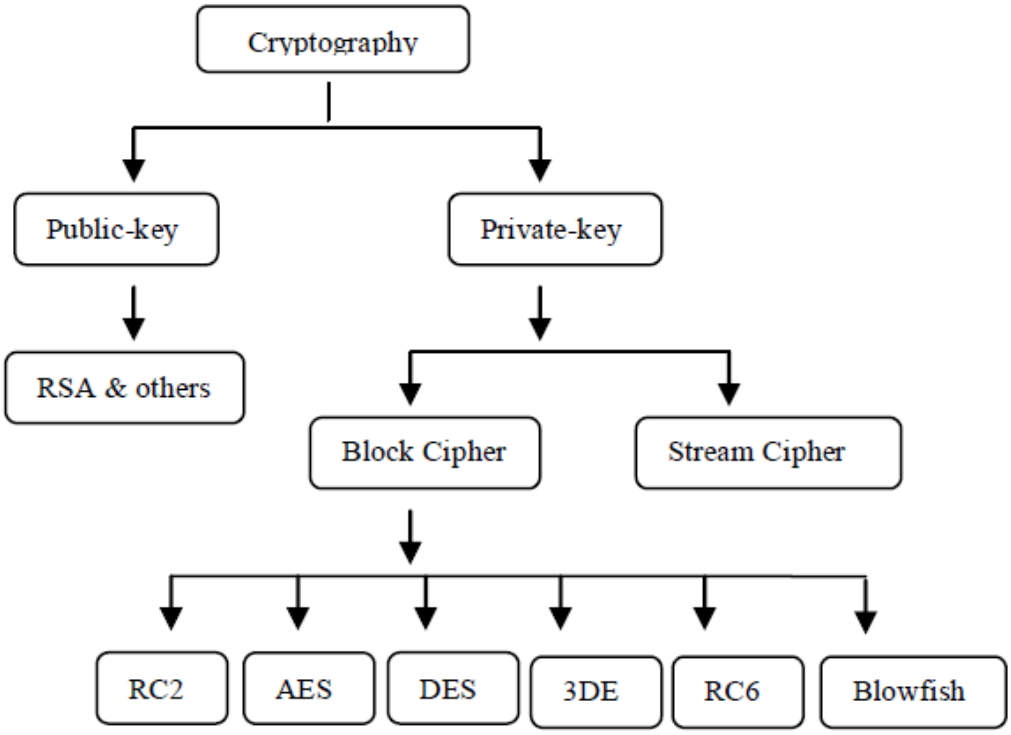


Gambar II-2. Kriptografi Simetris

Jumlah waktu yang dihabiskan untuk proses enkripsi pada kriptografi kunci simetris lebih cepat dibandingkan dengan enkripsi pada kriptografi tidak simetris karena proses yang terdapat pada kriptografi kunci simetris mengkonsumsi waktu yang lebih sedikit dalam hal pesebaran kunci dan proses kalkulasi (Gupta & Mittal, 2014). Walaupun kriptografi simetris terlihat lebih konservatif dalam hal kriptografi karena menggunakan kunci bersama pada setiap prosesnya, namun pengembangan dari jenis kriptografi ini masih tetap banyak digunakan karena memiliki keunggulan dalam hal kompleksitas yang lebih rendah dibandingkan algortima kriptografi kunci tidak simetris. Chandra et. al (2014) menyimpulkan bahwa kriptografi simetris memiliki performa tingkat tinggi dalam hal keamanan terutama keamanan dengan tingkat yang sama karena penerimaan kunci otomatis yang digunakan pada kriptografi simetris berguna untuk mengamankan data walaupun membutuhkan jumlah *cache* yang banyak.

2.3.2 Jenis-jenis Kriptografi Simetris

Menurut Tripathi dan Agrawal (2014) kriptografi kunci simetris dibagi menjadi dua bagian yaitu *block cipher* dan *stream cipher* yang didasari oleh metode untuk membagi data menjadi partisi dalam proses pengolahan data. Pada *block cipher* atau sandi balok, seluruh data dipisahkan menjadi beberapa blok dengan jumlah karakter atau ukuran yang sama pada setiap blok yang dihasilkan. Sedangkan *stream cipher* atau yang disebut dengan sandi alir pembagian data dibagi menjadi sebuah bit dan kemudian disusun sedemikian rupa untuk proses enkripsi.



Gambar II-3. Tipe-tipe kriptografi (Gupta and Mittal, 2014)

Gambar 2.3 menunjukkan klasifikasi dari kriptografi berdasarkan metode pengenkripsian data. Berdasarkan jumlah kunci yang digunakan, kriptografi tidak

simetris mempunyai kunci publik dan kunci pribadi atau *private*. *Private key* dibagi lagi menjadi dua cara enkripsi data yaitu sandi blok dan sandi alir.

1. Advance Encryption Standard (AES)

AES merupakan salah satu teknik enkripsi yang mengenkripsi data pada setiap blok atau salah satu teknik yang menggunakan penerapan dari sandi blok atau *cipher block*. Data yang dienkripsi dengan menggunakan metode ini harus memiliki Panjang kunci dalam ukuran 128 bits blok dengan 128, 192, atau 256 bits variable.

Proses enkripsi untuk metode AES seperti yang diterangkan oleh Abdullah (2017) yaitu keamanan AES berdasarkan jumlah putaran yang ada pada tiap proses. Contohnya, kunci 128-bit akan memiliki 10 putaran, kunci 192-bit akan memiliki 12 putaran, dan kunci 256-bit akan memiliki 14 putaran yang di setiap putaran tersebut akan berisi 4 proses lanjutan. Singkatnya, proses enkripsi dengan menggunakan metode ES akan dimulai dengan menggantikan *bytes*, menggeser baris, menggabung kolom, dan yang terakhir adalah menambah putaran kunci di akhir.

2. Data Encryption Standard (DES)

DES merupakan blok sandi yang juga menerapkan pembagian data menjadi beberapa blok untuk proses enkripsi dan dekripsi data. DES bekerja pada 64 bit blok yang menggunakan kunci dengan ukuran panjang 56 bit. Menurut Rabah (2008) DES merupakan algoritma yang popular untuk melakukan enkripsi dalam rentan 25 tahun terakhir terutama pada sector

perbankan dan pemerintahan, namun kemudian DES dipandang sebagai metode yang lemah karena penyerangan dengan menggunakan kunci sembarang atau yang lebih dikenal dengan metode *brute force* mungkin sekali terjadi karena Panjang kunci yang digunakan pada DES tergolong pendek pada sistem yang banyak digunakan saat ini.

Proses enkripsi bercabang menjadi 16 fase yang terbagi menjadi 8 *S-Boxes.* Proses awal dimulai dengan memindahkan bit yang kemudian dilanjutkan menjadi proses pergantian tidak linier dan diakhiri dengan operasi XOR untuk menghasilkan teks sandi. Membalikkan prosedur sub-kunci akan menghasilkan teks asli kembali atau proses dekripsi dari DES (Chandra et. al 2014)

3. Triple Data Encryption Standard (3DES)

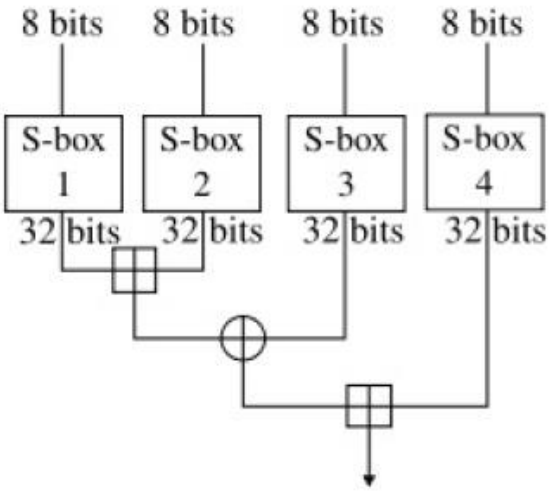
3DES merupakan pengembangan dari versi DES yang dilaporkan memiliki banyak cacat dan dianggap sebagai metode sandi blok yang tidak menjamin keamanan tingkat tinggi yang dikarenakan Panjang kunci yang digunakan. Blok 3DES berukuran 64 bits dengan Panjang kunci yang lebih Panjang dari DES yaitu 192 bit. Algoritma ini disebut dengan 3DES karena algorritma 3DES menyajikan tiga kali level enkripsi dalam hal kunci dari 64-bit menjadi 192-bit dibandingkan dengan algoritma DES.

Ratnadewi et. al (2018) menjelaskan bahwa ada tiga probabilitas cara yang dapat dilakukan untuk menerapkan algoritma 3DES yang akan mengkonversi kunci menjadi tiga bagian dengan ukuran yang sama untuk

setiap bagian yaitu 64 bits.cara yang pertama yaitu seluruh kunci menggunakan urutan beragam pada setiap bagian yang ada pada proses kriptografi algoritma 3DES. Solusi yang kedua yaitu mempunyai kombinasi kunci yang sama untuk kunci pertama dan terakhir namun berbeda pada kunci yang kedua (2K3DES). Cara yang terakhir yaitu menerapkan penggunaan kunci bersama untuk setiap kunci di setiap proses enkripsi.

4. Algoritma blowfish

Algoritma blowfish juga merupakan blok sandi pada kelompok kriptografi tidak simetris. Blowfish memiliki blok dengan ukuran 64 bits dengan rentang Panjang kunci dari 32 bits hingga 448 bits.



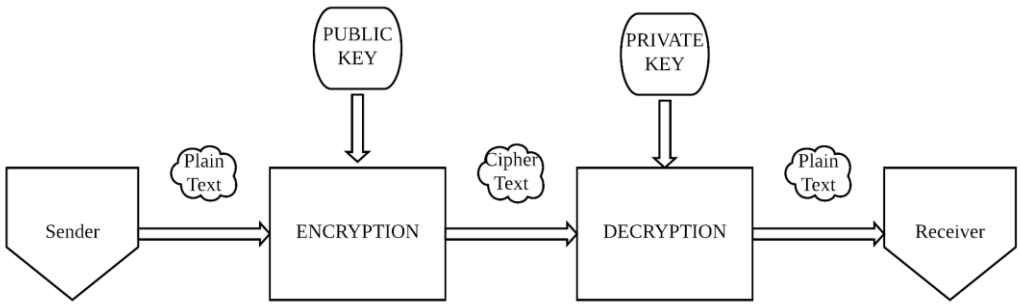
Gambar II-4. Arsitektur algoritma *blowfish* (Kumar 2014)

Seperti yang tampak pada gambar 2.4, algoritma blowfish memiliki 32-bit *s-boxes* yang terdiri dari 256 masukan untuk setiap *s-box.* Untuk data yang akan dienkripsi dengan menggunakan algoritma *blowfish,* operasi yang

digunakan yaitu XOR. Blok sandi *blowfish* dianggap baik dalam hal mengatasi jumlah blok data dengan ukuran yang sangat besar (Kumar, 2014)

2.3.3 Kriptografi Asimetris

Perbedaan kunci asimetris atau tidak simetris dibandingkan dengan algoritma simetris yaitu penggunaan tambahan kunci pada salah satu proses baik enkripsi ataupun dekripsi. Kriptografi tidak simetrismempunyai dua kunci yang berbeda yang disebut dengan kunci publik yang tidak perlu memiliki kerahasiaan atau boleh dipublikasikan dan kunci pribadi yang penggunaannya sama seperti kunci pada simetri simetris yaitu harus dijaga kerahasiaannya. Kriptografi tidak simetris dikembangkan karena adanya upaya untuk mengatasi permasalahan pada kriptografi simetris dalam hal pesebaran kunci yang digunakan.



Gambar II-5. Kriptografi Asimetris

Gambar 2.5 menunjukkan bahwa kunci publik boleh diketahui oleh setiap orang dan akan digunakan dalam hal enkripsi sedangkan kunci probadi lebih berperan dalam proses dekripsi dan hanya dapat diketahui oleh pengguna yang diizinkan untuk mengetahui teks asli. Proses membangkitkan kunci dilakukan di

akhir proses dari algoritma ini yang akan menghasilkan dua kunci yang berbeda secara acara dalam skala besar dibandingkan dengan algoritma simetris (Neidhart)

2.3.4 Jenis-jenis Kriptografi Asimetris

Kriptografi asimetris juga dikenal dengan kriptografi modern yang dikarenakan penggunaan secara berbeda terhadap metode yang telah berkembang di bidang kriptografi yang menyebabkan penelitian serta pengembangan di bidang kriptografi asimetris sangat marak dilakukan oleh berbagai pihak. Kriptografi tidak simetris merupakan pengembangan lanjutan dari kriptografi simetris yang dianggap kurang kuat dalam hal kuantitas kunci yang digunakan dalam bidang kriptografi.

1. Algoritma Rivest-Shamir-Adleman (RSA)

   Menurut Tripathi dan Agrawal (2014) menyatakan bahwa algoritma RSA menjadi salah satu algortima kriptografi yang cukup dimmintai karena dapat menghasilkan kunci publik untuk setiap orang namun tetap memiliki keamanan pada kunci pribadi. Tripathi dan Agrawal menambahkan bahwa perhitungan pada algoritma ini diawali dengan melakukan modulo terhadap bilangan bulatuntuk mengambil dua nilai variable yang berbeda pada variabel “p” dan “q” secara acak sehingga *(n=p*q)*. Pesan dalam bentuk “m” akan dienkripsi dengan menggunakan eksponen “e” dan menghasilkan teks sandi “c” dengan (c=me (mod n)).

   Seperti metode kriptografi asimetris lainnya, proses enkripsi data dan menghasilkan dua kunci akan berakibat pada performa yaitu proses

menghasilkan teks sandi atau dengan kata lain metode RSA kurang cepat dibandingkan dengan penggunaan satu kunci (Neha Garg et al, 2014)

2. Algoritma Diffle-Hellman

Proses yang terdapat pada algoritma *diffle-Hellman* menuntut pengirim dan penerima data untuk memiliki kunci yang sama pada akhir proses untuk mengetahui pesan secara bersama. Pengirim akan menentukan nilai dari a" dan penerima akan menentukan nilai dari "b" dalam bentuk bilangan bulat serta menjaga agar nilainya tetap rahasia. Setelah itu, g^a mod p dari pengirim akan ditukarkan dengan g^b mod p dari penerima. Pada tahapan akhir pada algoritma ini pengirim akan mengakumulasikan nilai dari B^a mod p sementara penerima akan mengakumulasikan nilai dari A^b mod p yang dimana "p" merupakan bilangan prima (Khaldi 2018).

Bagaimanapun juga, algoritma *diffle-hellman* tidak menyediakan identifikasi pemilik antara pengirim dan penerima serta kurang dalam hal autentikasi dalam proses pertemuan yang yang menyebabkan proses komunikasi antar kedua pihak tersebut sangat rentan diinterupsi oleh pihak lain karena interupsi di tengah jalan sangat mungkin untuk terjadi (Devi dan Makani 2015).

2.3.5 Proses Enkripsi pada Kriptografi data Teks

Pada enkripsi teks, pemrosesan data dibagi menjadi dua kategori, yaitu sandi alir atau *stream cipher* dan sandi blok atau *block cipher* dalam penanganan sebelum data diolah sebagai masukan dalam sistem kriptografi yang dikembangkan (Sharif dan Mansoor, 2010)

a. Stream Cipher

Pada sandi alir, setiap angka pada teks asli akan dienkripsi tepat satu dengan angka yang bersesuaian dari kunci alir dalam rangka untuk mendapatkan jumlah angka pada teks sandi. Dalam metode pemrosesan data ini, kunci dan algoritma yang digunakan pada enkripsi data akan diimplementasikan pada setiap jumlah angka dalam bentuk biner atau bentuk yang dapat diterima sebagai masukan dalam sistem yang dikembangkan.

b. Block Cipher

Pada sandi blok, teks secara keseluruhan akan dibagi menjadi bentuk blok atau dengan kata lain teks asli akan diubah menjadi beberapa bagian dalam blok teks yang apabila digabung kembali akan membentuk teks data secara keseluruhan. Jumlah blok atau angka dalam bit pada setiap blok akan didasarkan oleh kunci dan algoritma yang digunakan oleh pengguna sistem kriptografi. Teks asli yang dihasilkan kembali dalam proses dekripsi akan disusun kembali dari setiap blok untuk menghasilkan teks asli seperti sedia kala.

2.4 Perbandingan antara Kriptografi Simetris dan Asimetris

Tabel 2.1 menunjukkan bahwa seluruh kriptografi simetris mampu bekerja dalam jumlah waktu yang singkat atau hanya mengkonsumsi lebih sedikit waktu operasi untuk melakukan proses enkripsi dibandingkan dengan algoritma tidak simetris. Kecepatan dalam kriptografi merupakan jumlah waktu yang dibutuhkan untuk menghasilkan taks sandi dari sejumlah teks yang diberikan dalam rentang waktu tertentu (Srikantaswamy et. al 2011). Hal ini membuktikan bahwa jumlah kunci yang digunakan dalam proses enkripsi mempengaruhi performa metode dalam hal waktu walaupun tidak berlaku untuk

semua kriptografi tidak simetris karena algorima RSA juga dapat bekerja dalam tingkat yang sama dari segi waktu konsumsi dibandingkan dengan metode kunci simetris. Srikantaswamy et al (2011) juga menambahkan bahwa semakin banyak jumlah kunci yang digunakan maka semakin sedikit kecepatan yang dapat dihasilkan untuk melakukan proses enkripsi dan dekripsi.

Sumber daya yang dipergunakan dalam proses didasarkan oleh seberapa banyak teks asli yang dapat diubah menjadi teks acak oleh suatu algoritma dalam rentang waktu yang diberikan (Tripathi and Agrawal, 2014). Jumlah data yang dienkripsi pada setiap algoritma mempunyai cara yang beragam untuk mengolah data berdasarkan ukuran data dan kunci yang digunakan. Kompleksitas metode sebanding lurus dengan waktu konsumsi, semakin kompkes proses pengolahan data akan menyebabkan semakin banyaknya konsumsi waktu yang dibutuhkan (Srikantaswamy et. al 2011)

Tabel. II-1. Perbandingan spesifikasi pada kriptografi kunci Simetris dan Asimetris (Tripathi & Agrawal, 2014)

Parameter	Enkripsi Simetris				Enkripsi Asimetris	
	AES	DES	3DES	Blowfish	RSA	Diffie-Hellman
Konsumsi daya	Lebih tinggi dibandingkan dengan blowfish	Lebih tinggi dibandingkan dengan AES	Lebih tinggi dibandingkan dengan DES	Sangat rendah	tinggi	Lebih rendah dibandingkan dengan RSA
Throughput	Lebih rendah dibandingkan dengan *Blowfish*	Lebih rendah dibandingkan dengan AES	Lebih rendah dibandingkan dengan DES	Sangat tinggi	rendah	Lebih rendah dibandingkan dengan RSA
Rasio enkripsi	tinggi	tinggi	Menegah atau cukup	tinggi	tinggi	tinggi

Panjang kunci	128 atau 192 atau 256 bit	56 bit	112 hingga 168 bit	32 bits hingga 448 bit	Lebih dari 1024 bit	Manajemen pertukaran kunci
Kecepatan	Akselerasi tinggi	Akselerasi tinggi	Akselerasi tinggi	Akselerasi tinggi	Akselerasi tinggi	Akselerasi rendah
Keamanan	Bagian atau potongan Teks asli yang diketahui akan menimbulkan kerentanan	Lemah terhadap serangan acak atau serangan paksa (*brute force)*	Rentan terhadap serangan yang memiliki bagian atau potongan dari teks asli	Serangan dengan metode berdasarkan data pada kamu (*Dictionary attacks)*	Rentan terhadap serangan yang memperhatikan situasi waktu (*Timing attacks*)	Lemah terhadap tindakan penyadapan illegal *(Eavesdropping)*

2.5 Kelemahan Kriptografi saat ini

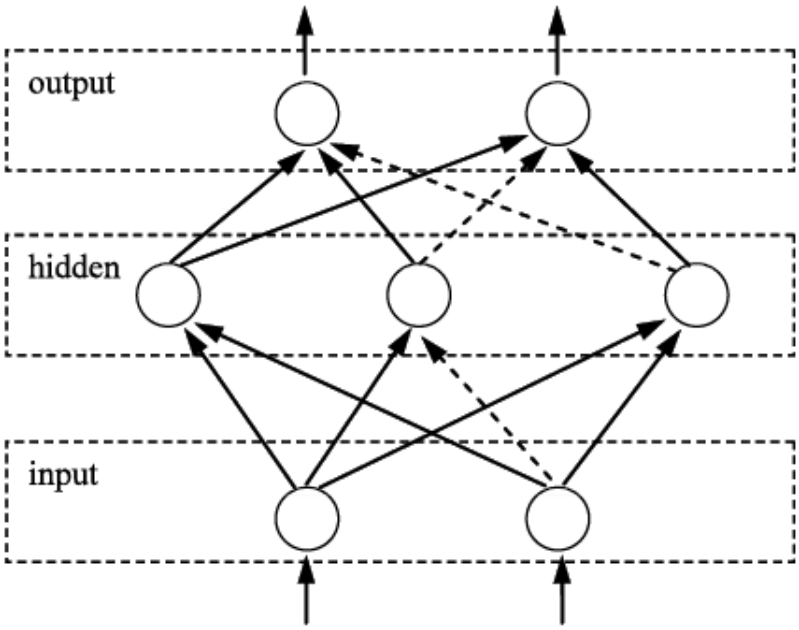
Pemakaian kunci yang tidak selalu dapat digunakan serta penggunaan metode aritmatik atau perhitungan matematika standar sebagai landasan membangkitkan kunci sehingga menimbulkan proses statis (Marta, 2013). Penelitian yang sering dilakukan terhadap kriptografi sebelumnya fokus terhadap distribusi kunci serta menjaga kerahasiaan kunci tersebut. Sekarang pengembangan difokuskan terhadap cara efektif kemungkinan adanya proses yang dinamik dalam menghasilkan teks sandi namun tetap memperhatikan *throughput* yang dihasilkan.

2.6 Jaringan Saraf Tiruan

Tingkat efisiensi jaringan saraf pada manusia terutama otak yaitu 10^{10} jika dibandingkan dengan perhitungan komputer standar pada tiap operasi (Shafi, 2007). Jaringan saraf tiruan merupakan salah satu kecerdasan buatan yang menyediakan perhitungan sebagai releksi dari impuls manusia untuk menentukan aksi yang akan disimpulkan berdasarkan masukan yang ada. Secara sederhana, jaringan saraf tiruan akan menitu reaksi manusia terhadap beberapa aksi yang diberikan (Endarko & Wardana, 2015). Berdasarkan jumlah lapisan, jaringan saraf tiruan dibagi menjadi lapisan tunggal dan lapisan majemuk atau banyak. Jaringan saraf tiruan dapat mengolah masukan yang dapat dipergunakan untuk menghasilkan pengetahuan terutama dalam hal mengenali pola (Tarigan et al. 2017)

2.6.1 Jaringan Saraf Tiruan *Single-layer* dan *Multi-layer*

Perbedaan yang sesungguhnya dapat terlihat pada kedua jenis jaringan ini yaitu jumlah lapisan tambahan yang digunakan dalam pemrosesan data untuk menghasilkan keluaran. Tidak seperti jaringa lapisan tunggal, jaringan lapisan banyak memiliki setidaknya satu lapisan tersembunyi yang berada diantara lapisan keluaran dan lapisan masukan. Contoh dari jaringan saraf tiruan adalah jaringan *McCulloch-Pitts*, jaringan *Hebb*, and jaringan *Perceptron*.



Gambar II-6. Jaringan dengan lapisan tersembunyi (*hidden layer*)

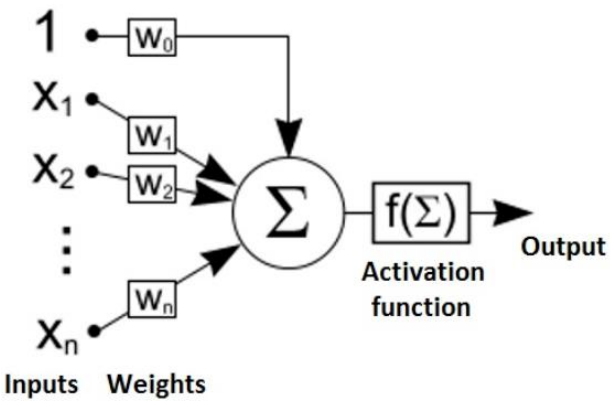
Gambar 2.6 menunjukkan struktur yang terdapat pada jaringan saraf tiruan yang mempunyai jaringan tambahan diantara lapisan masukan dan keluaran. Pada jaringan tersebut, sebelum diteruskan menuju jaringan keluaran, data akan dikirim menuju *neuron* yang terdapat pada jaringan tersembunyi yang kemudian hasilnya akan diteruskan menuju jaringan keluaran. Jumlah jaringan tersembunyi yang digunakan tidak berpengaruh besar terhadap maksimalisasi jaringan dan sebaliknya

dapat menurunkan nilai akurasi dari data yang diinginkan (Shafi, 2007). Semakin banyak jumlah jaringan tambahan yang digunakan akan menambah kesulitan dalam proses pengujian serta akan mengkonsumsi lebih banyak waktu namun memiliki kapabilitas yang hamper sama dengan jaringan yang mempunyai lapisan tersembunyi yang lebih sedikit (Villiers & Barnard, 1992)

2.6.2 Jaringan Saraf Propagasi Balik pada Kriptografi

Pada *backpropagation,* nilai keluaran akan dibandingkan dengan lapisan sebelumnya untuk mengurangi jumlah perbedaan hingga mencapai nilai maksimum sebagai batas toleransi (Alsmadi et. al, 2009). Pada gambar II-7. neuron selain pada lapisan masukan merupakan nilai gabungan dari setiap neuron sebelumnya sebanyak n (Xn) dikalikan dengan bobot yang terdapat antara kedua neuron (Wn) yang kemudian akan dihitung dengan persamaan fungsi aktivasi (f(∑)) yang dipakai pada neuron.

Nilai yang dihasilkan pada setiap *neuron* tergantung pada nilai masukan, bobot, serta fungsi aktivasi yang digunakan dalam membangun jaringan saraf tiruan seperti yang ditunjukkan pada gambar II-7. Proses yang terjadi pada jaringan saraf *backpropagation* mencakup proses pemeriksaan ulang terhadap bobot dengan membandingkan hasil yang diinginkan dengan hasil yang didapat ketika kedua nilai tersebut tidak sama atau memiliki perbedaan *error* yang jauh.



Gambar II-7. Struktur yang terdapat pada suatu *neuron* (Volna et al. 2012)

Pada kriptografi, alur pemeriksaan ulang yang terdapat pada *backpropagation* digunakan untuk memastikan sistem yang dibangun dapat mengenali kembali teks asli dari teks sandi yang dihasilkan. Al-nima et al (2009) menjelaskan bahwa proses dari kriptografi menggunakan jaringan saraf tiruan diawali dengan melakukan pengujian terhadap jaringan *backpropagation* untuk mendapatkan bobot yang diinginkan sehingga proses enkripsi dan dekripsi akan berdasarkan jaringan yang sudah diuji tersebut.

2.7 Penelitian Terkait

Tabel II-2. Penelitian terkait penerapan jaringan saraf tiruan pada kriptografi

No	Tahun	Penulis	Judul	Metode	Penjelasan
1	2016	Mahesha NB	Authentication Based Two Level Encryption & Decryption of An Image Using Artificial Neural Network	Enkripsi & dekripsi dua tingkat (*two level*)	Proses yang diterapkan berupa penambahan proses lain yang bertujuan untuk memastikan keamanan tambahan terhadap proses enkripsi data. Data yang dienkripsi secara dua tingkatan atau *two level* menyebabkan proses dekripsi data juga naik menjadi dua tingkatan yang meningkatkan waktu pengolahan serta sumber daya yang digunakan.

2	2015	Tope Komal, Rane Ashutosh, Rahate Roshan, Asst. Prof. S. M. Nalawade	Encryption and Decryption Using Artificial Neural Network	Chaotic neural network	Sistem kalut (chaos) akan menghasilkan nilai yang berbeda secara acak yang akan menyebabkan pengguna yang mengakses data tidak dapat menebak nilai yang akan muncul berikutnya yang baik untuk mencegah penyerangan secara acak (*brute force*) dikarenakan perubahan data dari waktu ke waktu. Namun sayangnya, metode ini mengkonsumsi sumber daya yang cukup besar untuk menyimpan data secara acak.
3	2012	A. Ismail, Galal H. Galal-Edeen, Sherif	Satelite Image Encryption Using Neural Network Backpropagation	Pemrosesan gambar dalam kriptografi dengan bantuan	Proses pada penelitian ini akan membagi proses menjadi dua bagian, enkripsi akan menggunakan proses yang ada di lapisan masukan menuju lapisan tersembunyi

		Khattab, Mohamed Abd Elhamid M. El Bahtity.		jaringa saraf tiruan	sementara proses dekripsi akan menggunakan proses dari lapisan tersembunyi menuju lapisan keluaran. Kelemahan dari proses ini adalah data yang telah dienkripsi tidak sepenuhnya tertutupi atau tidak sepenuhnya berubah dari gambar yang sebenarnya yang menyebabkan kemungkinan untuk menebak gambar yang dienkripsi dapat mungkin terjadi.
4	2012	Eva Volna, Michal Janosel, Martin Kotyrba	Cryptography Based On Neural Network	Neural cryptography	Metode jaringan saraf di implementasikan dengan kriptografi kunci tidak simetris terhadap blok data yang bersesuaian terhadap teks sandi dengan mendapatkan bobot pada jaringan yang telah diuji. Bobor yang

					didapatkan akan dijadikan kunci publik sedangkan bias akan dijadikan kunci pribadi.
5	2009	Raid R. Al-nima, Muhanad L, Saba Q. Hassan	Data Encryption Using Backpropagation Neural Network	Multi-layer backpropagation neural network	Penelitian ini menjelaskan enkripsi dengan menggunakan bobot yang dilatih dengan menggunakan jaringan saraf tiruan dengan menggunakan jumlah lapisan masukan, lapisan tersembunyi, serta lapisan keluaran yang berjumlah sama.

Tabel II-2 menunjukkan bahwa jaringan saraf tiruan dapat digunakan untuk melakukan proses enkripsi dan dekripsi data karena memiliki kemampuan untuk melatih data masukan terhadap bobot yang digunakan untuk mengenali target. Selain itu, enkkripsi dan dekripsi dengan jaringan saraf dipengaruhi oleh jumlah lapisan, jumlah node, penggunaan kunci, penggunaan bobot, dll. Beberapa penelitian juga menunjukkan bahwa kriptografi menggunakan jaringan saraf dapat menghasilkan *cipher text* yang berbeda .

2.8 Kesimpulan

Pembahasan ini menyediakan penjelasan mengenai kajian literatur mengenai kriptografi, jaringan saraf tiruan, metode-metode yang berlaku, serta penerapan kombinasi antara metode pada jaringan saraf tiruan dengan metode kriptografi. Selain itu, bab ini menerangkan kemungkinan untuk melakukan kombinasi dari jaringan saraf *backpropagation* dengan metode kriptografi yang mungkin dalam upaya meningkatkan performa yang dihasilkan dari kombinasi algoritma tersebut. Teori-teori yang dipergunakan dalam bab ini akan dipergunakan untuk menentukan performa dari kriptografi yang dikombinasikan dengan jaringan saraf tiruan untuk melakukan enkripsi serta dekripsi pada data teks di pembahasan selanjutnya.