BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam penelitian ini akan digunakan sepuluh tinjauan studi yang nantinya dapat mendukung penelitian, berikut ini merupakan tinjauan studi yang diambil dapat dilihat pada Tabel 2.1 Daftar Literatur.

Tabel 2. 1 Daftar Literatur

No Literatur	Penulis	Informasi Publikasi (Volume, Tahun, ISSN, Penerbit)	Judul
Literatur 01	Gaurav Agarwal, Saurabh Singh, Meeta Chaudhary	Vol 1, No 2,2010, ISSN: 0976-5697 International Journal of Advanced Research in Computer Science	IMAGE ENCRYPTION USING THE STANDARD HILL CIPHER
Literatur 02	Ziad E. Dawahdeh, Shahrul N. Yaakob, Rozmie Razif bin Othman	2017, Journal of King Saud University – Computer and Information Sciences	A NEW IMAGE ENCRYPTION TECHNIQUE COMBINING ELLIPTIC CURVE CRYPTOSYSTEM WITH HILL CIPHER
Literatur 03	Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran	Vol 9,2014, p-ISSN : 2278-2834 *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*	DIGITAL IMAGE ENCRYPTION BASED ON RSA ALGORTHM
Literatur 04	Osama S. Faragallah	Vol 12, 2011, *Sensing and Imaging: An*	DIGITAL IMAGE ENCRYPTION

		International Journal	BASED ON THE RC5 BLOCK CIPHER ALGORITHM
Literatur 05	Andro Alif Rakhman, Achmad Wahid Kurniawan	Vol 14, No 2, 2015 Techno.COM	IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) DAN *VIGENERE CIPHER* PADA GAMBAR BITMAP 8 BIT
Literatur 06	M. Taufiq Tamam, Wakhyu Dwiono, Tri Hartanto	Vol 4, No 1, 2010, Jurnal ECCIS	PENERAPAN ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK PENGAMANAN FILE CITRA
Literatur 07	Taronisokhi Zebua, Eferoni Ndruru	Vol 4,no 4,2017,p-ISSN : 2355-7699, Jurnal Teknologi Informasi dan Illmu Komputer (JTIIK)	PENGAMANAN CITRA DIGITAL BERDASASRKAN MODIFIKASI ALGORITMA RC4
Literatur 08	Emy Setyaningsih	Vol 2, No 2, 2009, Jurnal Teknologi	PENYANDIAN CITRA MENGGUNAKAN METODE PLAYFAIR CIPHER

Literatur 09	Arief Susantom Tutik Khotimah, Muhammad Taufik Sumadi, Joko Warsito,	2018, International Journal of Engineering & Technology	IMAGE ENCRYPTION USING VIGNERE CIPHER WITH BIT CIRCULAR SHIFT
Literatur 10	Aji Supriyanto, Eka Ardhianto	Vol 13,No 2,2008, ISSN : 0854-9524	PENYANDIAN FILE GAMBAR DENGAN METODE SUBSTITUSI DAN TRANSPOSISI

2.1.1 Literatur 1

1. Masalah

   Transmisi gambar yang aman di internet telah menjadi persyaratan penting hari ini. Untuk transmisi yang aman disini menggunakan kriptografi yang memainkan peran penting dalam kemanan untuk komunikasi di antara berbagai saluran. Pada saaat ini kriptografi adalah bagian dari keamanan jaringan yang dapat digunakan untuk enkripsi teks, audio, video, grafik dan file multimedia lainnya.

2. Pembahasan

   Didalam makalah ini metode yang diajukan adalah hill cipher untuk enkripsi gambar. Untuk enkripsi pertama kali kita harus menemukan matriks dari gambar asli. Dan secara acak menghasilkan matriks kunci yang sama dengan dimensi matriks gambar yang akan dienkripsi. Lalu baru terapkan konsep hill cipher standart

C = E_k(P)

Tetapi dalam konsep ini gambar kita mempunyai 256 keabuan (untuk contohnya) tingkat intensitas maka akan berfungsi sebagai :

C = E_k(P)mod 256

Dimana C adalah matriks dari *cipher image*, P adalah matriks dari gambar asli dan k adalah nilai kunci matriks yang dihasilkan secara acak.

3. Hasil Pembahasan

   Dengan metode hill cipher standar yang diterapkan pada citra gambar ini memberikan kemanan terhadap berbagai serangan seperti brute-force. Gambar yang dihasilkan dari enkripsi tidak dapat dikenali sama sekali

4. Tinjauan terhadap Literatur 01

   Dalam literatur penulis mengenkripsi gambar dengan menggunakan standar hill cipher yang menghasilkan gambar tidak dikenal tetapi penulis tidak melakukan analisis hasil pengujian sehingga tidak diketahui hasil analisis besar file sebelum dan seudah enkripsi, perubahan nilai indeks warna mengalami perubahan atau tidak dan waktu proses enkripsi dekripsi tidak diketahui.

2.1.2 Literatur 2

1. Masalah

   Meningkatnya pengguna internet dan komunikasi media, sharing gambar melalui saluran yang tidak aman besar kemungkinan untuk diserang dan dicuri. Enkripsi merupakan teknik yang cocok untuk melindungi gambar dari serangan, algoritma hill cipher salah satunya memiliki struktur yang simple dan komputasi yang cepat, tapi lemah dalam keamanan karena

pengirim dan penerima perlu menggunakan dan membagi private key yang sama dalam saluran yang tidak aman.

2. Pembahasan

Dalam Jurnal 02 ini *Hill Cipher* dikombinasikan dengan teknik enkripsi *Elliptic Curve Cryptography (ECC).* Sehingga menjadi pendekatan baru yang bernama *Elliptic Curve Cryptosystem and Hill Cipher* (ECCHC). Modifikasi ini membuat system lebih efisien dibandingkan teknik *Hill Cipher* yang asli, serta mempercepat waktu komputasi dekripsi mengingat teknik ini tidak membutuhkan kunci matriks yang dibalik. Misalkan sender (User A) ingin mengirimkan pesan gambar ke User B menggunakan ECCHC di saluran yang tidak aman. Pertama mereka harus menyetujui Elliptic Curve fungsi E dan membagi domain parameter {a,b,p,G}, dimana a,b koefisien dari fungsi elliptic, p adalah bilangan prima yang besar, dan G adalah generator point. Kemudian masing-masing memilih acak kunci private dari interval [1,p-1];n_A untuk User A and n_B untuk User B, dan membuat public key dengan :

$P_A = n_A$.G

$P_B = n_B$.G

Setiap pengguna mengalikan kunci private dengan kunci public pengguna lain untuk mendapatkan kunci K_1= (x,y).

3. Hasil Pembahasan

Sebuah pendekatan baru cryptosystem (ECCHC) telah diusulkan di makalah ini menggabungkan ECC dengan algoritma cipher Hill standar untuk meningkatkan keamanan cipher hill asli untuk enkripsi gambar. Ini

menghasilkan kunci enkripsi/ dekripsi baru dengan menggunakan pendekatan ECC yang menhasilkan kunci rahasia yang kuat, tahan terhadap penyusup dan memberikan keamanan yang lebih. Dikarenakan tidak perlu membagikan kunci melalui internet, *Self-invertible key* atau kunci matriks yang dapat dibalik sendiri digunakan untuk enkripsi dan dekripsi. Jadi tidak dibutuhkan untuk mencari *inverse key* matriks dalam proses dekripsi.

4. Tinjauan terhadap Literatur 02

   Dalam literatur ini penulis menganalisa dari segi keamanan, ada beberapa parameter yang digunakan dalam menilai efisiensi enkripsi citra grayscale dan membandingkan citra yang dienkripsi dan citra asli untuk di evaluasi kinerja enkripsinya. Berbagai metode diterapkan dalam penelitian ini untuk evaluasi efisiensi enkripsi, misalnya, *Entropy*, *Peak Signal to Noise Ratio* (PSNR), dan *Unified Average Changing Intensity* (MSE).

2.1.3 Literatur 3

1. Masalah

   Keamanan informasi telah menjadi masalah penting dalam komunikasi data. Kriptografi merupakan sebuah solusi dan memainkan peran yang penting dalam sistem keamanan informasi.

2. Pembahasan

   Didalam makalah ini menjelaskan tentang kriptografi RSA dan menyajikan perbandingan antara *Cryptosystem* RSA dengan DES dan *Blowfish* yang diterapkan pada gambar skala abu-abu atau grayscale. Untuk melakukan enkripsi dengan RSA pertama kita harus menentukan 2

bilangan prima P dan Q dengan nilai yang berbeda. Peneliti menggunakan citra grayscale berukuran 256 x 256 dalam pengujianya.

3. Hasil Pembahasan

   Hasil penelitian menunjukkan bahwa waktu yang digunakan RSA membuat langkah lebih cepat diimplementasikan daripada DES dan Blowfish dan dengan keamanan data yang lebih dari sistem simetris. Tapi pada RSA nilai bilangan prima Q dan P mengontrol waktu dalam pembuatan kunci sehingga meningkatkan waktu yang diambil karena membuatnya lebih aman daripada sebelumnya.

4. Tinjauan terhadap Literatur 03

   Didalam jurnal ini penulis melakukan perbandingan RSA terhadap dua algoritma yaitu DES dan Blowfish dilihat dari Key generation time, Encryption time, dan decryption time. RSA membuat langkah-langkah lebih cepat diimplementasikan dibandingkan dua algoritma tersebut. Tetapi, dalam RSA memilih nilai bilangan prima Q dan P pada proses yang disebut *Key generation* akan menambah sedikit waktu ini yang membuat lebih aman dari sebelumnya.

2.1.4 Literatur 4

1. Masalah

   Perkembangan sekarang dalam pemrosesan gambar digital dan komunikasi jaringan selama decade terakhir telah menciptakan permintaan besar akan citra yang aman dan transmisi realtime yang aman melalui internet dan jaringan nirkabel. Dengan demikian, teknik enkripsi citra

dapat diandalkan untuk perlindungan data dari *counterfeiting, tampering,* dan *unauthorized* access.

2. Pembahasan

   Makalah ini menyajikan implementasi dan analisis cipher blok RC5 algoritma untuk citra dalam berbagai mode operasi dengan mempertimbangkan analisis enkripsi dengan pengujian *visual testing, maximum deviation, irregular deviation, information entropy, correlation coefficients, avalanche effect, histogram uniformity* dan *key space analysis.* Algoritma cipher blok RC5 adalah enkripsi simetris parameter algoritma, dinotasikan dengan RC5-w/r/b, dimana w / r / b adalah parameter yang dapat dikonfigurasi ulang. “w” adalah bits dan nilai standarnya adalah 32bits, nilai yang diijinkan 16,32, dan 64 bit . “r” merupakan jumlah putaran, angkanya bisa dalam range 0 sampai 255. “b” menandakan jumlah byte dalam kunci rahasia K. ukuran kunci mulai dari 0 bit hingga 2040 bit. Block cipher dapat dijalankan dalam berbagai mode operasi, seperti ECB (*The Electronic Codebook)* mode, CFB (*The Cipher Feedback)* mode, OFB *(The Output Feed Back)* mode. Menggunakan mode ECB dalam enkripsi dengan algoritma cipher blok RC5 tidak efisien karena tidak menyembunyikan semua informasi dari gambar asli. Sedangkan untuk metode CBC, OFB, dan CFB dengan algoritma RC5 semua informasi sama sekali tidak terlihat.

3. Hasil Pembahasan

   Efisiensi enkripsi dari algoritma cipher blok RC5 sudah diuji menggunakan berbagai citra digital dalam berbagai mode operasi dengan

berbagai metrik dan di bawah berbagai jenis serangan. Hasil percobaan menunjukkan bahwa RC5 algoritma cipher blok dapat diandalkan, memiliki struktur enkripsi yang efisien, kebal terhadap serangan dan memiliki mekanisme difusi yang efisien.

4. Tinjauan terhadap Literatur 04

   Dalam literatur 04 peneliti menggunakan algoritma RC5 dan dilakukan pengujian visual testing dengan 4 mode operasi berbeda yaitu ECB, CBC, OFB, CFB. Hasilnya enkripsi dengan mode ECB dengan algoritma RC5 block cipher tidak efisien mengingat ECB tidak menyembunyikan semua informasi dari original image lain dengan CBC, CFB, atau OFB mode informasi original image tidak terlihat total.

2.1.5 Literatur 5

1. Masalah

   Penggunaan informasi melalui media gambar atau citra memiliki beberapa kelemahan, salah satunya adalah kemudahan manipulasi citra oleh beberapa pihak dengan bantuan teknologi yang berkembang saat ini.

2. Pembahasan

   Metode yang digunakan dalam Jurnal ini yaitu mengkombinasikan algoritma *Rivest Shamir Adleman* (RSA) dan *Vignere Cipher* terhadap nilai indeks warna dari masing-masing piksel. Enkripsi gambar dilakukan melalui perhitungan kriptografi RSA terlebih dahulu kemudian dilanjutkan dengan *Vignere Cipher*.

3. Hasil Pembahasan

   Hasil dari pengujian dari Jurnal ini menunjukan secara visual, citra yang dikodekan sulit dibaca atau dilihat. Hal ini disebabkan keacakan pola warna yang dihasilkan setelah melalui proses encoding. Keteracakan pola warna hasil enkripsi dipengaruhi pola warna citra asli. Semakin banyak variasi pola warna pada citra asli, semakin sulit dan acak pola warna enkripsi yang dihasilkan.

4. Tinjauan terhadap Literatur 05

   Hasil pengujian dalam literatur 05 dilihat dari perbandingan citra sebelum dan sesudah dilakukan proses enkripsi dan dekripsi, analisis ruang kunci, analisis perubahan nilai indeks warna. Hal ini dilakukan untuk memastikan bahwa gambar yang dikodekan dan didekodekan bebas cacat sedikitpun dan kembali ke bentuk aslinya, dan juga menganalisis waktu proses encoding dan decoding. Rata-rata waktu yang dibutuhkan untuk proses dekripsi lebih lama dari enkripsi. Kekurangan penelitian dalam literatur 05 adalah format citra yang digunakan dalam penelitian ini hanya citra berformat bitmap 8 bit dan pengkodean citra yang dihasilkan lebih besar dari citra aslinya.

2.1.6 Literatur 6

1. Masalah

   Ilmu kriptografi sebenarnya sudah sangat lama digunakan, sejak dahulu kala sebelum ada metode pengiriman data melalui komputer. Seiring dengan perkembangan teknologi telekomunikasi, ilmu kriptografi juga semakin berkembang, baik dari segi bentuk maupun fungsinya.

2. Pembahasan

   ElGamal *algorithm* memerlukan sepasang kunci yang dibangkitkan dengan cara bilangan prima *p* dan dua buah bilangan acak (*random*) *g* dan *x,* dengan syarat bahwa nilai *g* dan *x* lebih kecil dari *p* yang memenuhi persamaan.

   y= g^x mod p

   Dari persamaan tersebut nilai y, g dan p merupakan pasangan kunci public sedangkan x, p merupakan pasangan kunci pribadi.

3. Hasil Pembahasan

   Hasil enkripsi dilihat secara visual citra tidak dapat dikenali, file bitmap citra diubah ekstensinya menjadi “este” melalui proses enkripsi dan dapat dikembalikan menjadi file berektensi bitmap lagi melalui proses dekripsi.

4. Tinjauan terhadap Literatur 06

   Aplikasi yang dihasilkan dalam penelitian literatur 06 hanya dapat digunakan untuk file bitmap dengan format piksel 24bit.

2.1.7 Literatur 7

1. Masalah

   Gambar digital yang bersifat pribadi dan rahasia sangat mungkin disadap oleh orang lain, terutama ketika gambar didistribusikan melalui Internet. Tentu saja, penyadapan dan penyalahgunaan gambar rahasia dapat merugikan pihak pemilik gambar.

2. Pembahasan

   Berdasarkan tata cara menggunakan algoritma enkripsi dan dekripsi algoritma RC4, kita menemukan bahwa rumus melakukan proses enkripsi dan dekripsi sangat sederhana. Ini adalah operasi XOR. Namun, ini menjadi salah satu kelemahan algoritma RC4. Perubahan pada algoritma ini adalah dengan menambahkan nilai inisialisasi. Itu di-XOR dengan setiap *plain* atau *cipher* secara berurutan untuk mengoptimalkan ketahanannya terhadap teknik serangan. Ada 3 proses utama algorritma RC4 yaitu proses *key scheduling algoritm (KSA), Pseudo Random Generation Algorithm (PRGA)* proses PRGA proses ini dilakukan untuk menghasilkan *keystream* yang akan digunakan saat enkripsi atau dekripsi, dan proses enkripsi dekripsi untuk proses enkripsi diawali dengan mengubah nilai yang terdapat pada warna elemen pixel citra ke bilangan biner.

3. Hasil Pembahasan

   Kekuatan data terenkripsi berdasarkan perubahan algoritma RC4 untuk serangan biasa *know plain* dan *know cipher*, kompleksitas menemukan aliran kunci yang digunakan oleh proses enkripsi maupun dekripsi. Keuntungan dari RC4 yang dimodifikasi tidak hanya terletak pada kunci, tetapi juga pada blok biner inisialisas dan operasi XOR yang dilakukan dalam proses pemindahan bit tertentu dari posisi kiri ke kanan untuk mengacak posisi. Proses dilakukan secara berurutan pada setiap blok asli maupun terenkripsi.

4. Tinjauan terhadap Literatur 07

   Ketahanan data yang dienkripsi dengan algoritma RC4 terhadap serangan jenis *know plain* dan *know cipher* terletak pada sulitnya menemukan aliran kunci yang digunakan dalam proses enkripsi dan dekripsi. menambahan blok vector inisialisasi dan pergeseran bit ke proses enkripsi dan dekripsi algoritma RC4 yang dimodifikasi bisa sangat efektif.

2.1.8 Literatur 8

1. Masalah

   Dipercaya secara luas bahwa internet sebagai sarana informasi telah menguybah banyak aspek kehidupan manusia. Salah satunya adalah fungsi email. Ini banyak digunakan oleh banyak orang untuk mengirim dokumen yang dilampirkan ke email melalui internet. Proses pengiriman melalui fasilitas ini sangat efisien, cepat dan murah. Namunm internet juga merupakan jaringan publik yang tidak aman. Kegiatan ini tentu akan menimbulkan risiko jika orang yang tidak berhak mengakses informasi sensitif dan berharga, seperti informasi tentang dokumen sensitive berupa teks atau data gambar digital.

2. Pembahasan

   Didalam makalah ini proses enkripsi citra dilakukan dengan sandi *playfair* dengan cara melakukan proses perubahan warna yang memisahkan nilai RGB setiap piksel menjadi komponen Red, Green dan Blue (untuk citra warna). Namun, untuk citra skala keabuan tidak perlu dilakukan proses perubahan warna.

3. Hasil Pembahasan

   Berdasarkan hasil penelitian, eksperimen, analisis dan pembahasan dapat disimpulkan bahwa penggunaan metode enkripsi playfair dalam pengkodean gambar sangat baik karena kunci matriks yang digunakan cukup besar. Kemungkinan matrik kunci yang akan ditebak juga cukup besar yaitu 256! kemungkinan. Namun, metode ini juga memiliki kelemahan. Dengan kata lain, frekuensi kemunculan bigram pada ciphertext sesuai dengan frekuensi kemunculannya pada plaintext.

4. Tinjauan terhadap Literatur 08

   Kelemahan dari penelitian literatur 08 ini pola sebelum dan sesudah enkripsi sangat terlihat jelas jika citra yang digunakan citra berwarna. Sebaiknya metode playcipher digabungkan dengan algoritma kriptografi lainnya.

2.1.9 Literatur 9

1. Masalah

   Data dan informasi adalah komoditas penting baik untuk individu maupun organisasi. Informasi dapat disajikan dalam bentuk teks, gambar, audio, video atau campurannya. Beberapa informasi tersedia dan dapat diakses oleh publik di mana beberapa diantaranya bersifat rahasia yang rentan untuk dicuri dan diserang.

2. Pembahasan

   Dalam penelitian ini diajukan pengembangan metode *Vignere Cipher* menggunakan *bit circular shift* pada enkripsi citra. Di dalam penelitian ini menggunakan citra RGB dan grayscale sebagai sampel dan menunjukan

bahwa *Vignere cipher* dengan *bit circular shift* memiliki kinerja yang baik ketika mengenkripsi gambar baik secara visual maupun keacakannya. Rumus dari vignere untuk enkripsi adalah :

C = (P+K)mod 26 Enkripsi

P = (C-K)mod 26 Dekripsi

Nilai 26 merupakan nomor dari huruf A-Z, kemudian angka 0-25 menunjukan posisi huruf dalam urutan abjad. Karena intensitas piksel adalah nilai angka 0-255 maka metode vignere yang asli dimodifikasi menjadi :

C = (P+K)mod 256 Enkripsi

P = (C-K)mod 256 Dekripsi

Proses enkripsi dan dekripsi ini diterapkan untuk semua intensitas nilai dalam setiap piksel. Selanjutnya *bit circular shift* diterapkan untuk meningkatkan hasil enkripsi *Vignere cipher*.

3. Hasil Pembahasan

   Enkripsi gambar menggunakan *Vignere cipher* dengan *bit circular shift* memberikan hasil yang baik yang menghasilkan gambar yang sulit dikenali.

4. Tinjauan terhadap Literatur 09

   Didalam literatur ini peneliti menggunakan *Mean Absolute Error* (MAE) dan *correlation coefficient* untuk membandingkan hasil enkripsi dan gambar original. Peneliti juga membandingkan enkripsi menggunakan Vignere saja dan enkripsi menggunakan Vignere with Bit Circular Shift untuk mengetahui hasil enkripsi mana yang lebih baik.

2.1.10 Literatur 10

1. Masalah

   Siapa pun yang ingin merahasiakan sesuatu akan melakukan segala kemungkinan untuk menyembunyikan dari orang lain. Contoh sederhana, ketika anda akan mengirim surat kepada seseorang, bungkus surat itu sehingga tidak ada orang lain yang bisa membacanya. Mengupayakan sebuah mekanisme yang membuat isi surat sulit dipahami untuk meningkatkan kerahasiaan surat agar tidak terbaca oleh orang lain saat amplop dibuka.

2. Pembahasan

   Dalam makalah ini penulis menggunakan teknik enkripsi tradisonal untuk menggabungkan metode Substitusi dan Transposisi. Objek yang diganti dalam penelitian ini adalah piksel. Nilai piksel dari gambar dimasukkan dalam matriks dengan ordo sama dengan ukuran gambar. Matriks dibaca dengan spiral yang dimulai di sudut kiri atas dan berakhir di tengah matriks.

3. Hasil Pembahasan

   Teknik penyandian dengan metode substitusi dan transposisi yang dilakukan oleh peneliti pada gambar berformat BMP dapat menghasilkan suatu gambar yang tidak dapat dikenali lagi. Dan ketika pengujian dilakukan dalam membandingkan gambar asli sebelum disandikan (plainteks) dengan gambar setelah disandikan (chiperteks) tidak terdapat perbedaan dalam ukuran gambar.

4. Tinjauan terhadap Literatur 10

   Dalam literatur 10 ini dilakukan dua pengujian, pengujian pertama resolusi dan besar file sebelum dan sesudah di enkripsi, dari hasil pengujian yang didapat antara gambar plaintext image dan cipher image tidak memiliki perbedaan di besar file maupun ukuran resolusi dan hasil cipher image tidak dapat dikenali. Pengujian kedua dilakukan proses enkripsi dengan gambar bersifat homogen dan heterogen lalu dibandingkan. Hasilnya citra yang bersifat homogen (warna sedikit) akan lebih mudah diidentifikasi dibandingkan gambar yang memiliki jumlah warna lebih banyak (heterogen).

Dari beberapa literatur yang penulis amati, dalam setiap literatur hanya melakukan proses enkripsi pada citra. disini penulis akan melakukan proses enkripsi terhadap citra dan enkripsi terhadap kunci Hill cipher yang digunakan untuk enkripsi dekripsi citra untuk meningkatkan keamanan jika citra dikirim ke penerima.

2.2 Pengertian Citra Digital

Istilah lain dari gambar adalah citra digital, yang merupakan bagian dari komponen multimedia yang berperan sangat penting dalam penciptaan informasi visual (Munir, 2004). Gambar atau citra digital sangat informatif sehingga membedakanya dari teks dengan karakteristik ini. Citra atau gambar dibagi menjadi dua jenis yaitu gambar kontiun dan gambar diskrit. Gambar digital (*digital image*), atau gambar diskrit, dibuat dari proses digitalisasi terhadap gambar kontinu. Menurut (Zebua dan Nduru, 2017), citra monokrom (hitam putih/ biner), gambar keabuan (grayscale), dan citra *true color* (berwarna) merupakan

salah satu jenis citra digital. Piksel gambar berwarna memiliki tiga elemen warna yang biasa disebut dengan RGB, yaitu *Red*(Merah), *Green*(Hijau), dan *Blue*(biru).

2.3 Algoritma Kriptografi

Kata “Kriptografi” berasal dari dua kata bahasa Yunani yaitu crypto dan graphia. Crypto artinya rahasia dan graphia artinya tulisan. Kriptografi adalah ilmu dan seni menjaga kerahasiaan pesan ketika pesan dikirim dari satu lokasi ke lokasi lain. Definisi dari istilah algoritma adalah urutan sistematis langkah-langkah logis untuk memecahkan masalah. Algoritma kriptografi adalah cara logis untuk menyamarkan pesan dari orang yang tidak memiliki izin untuk pesan tersebut. Algoritma kriptografi memiliki tiga fungsi dasar yaitu (Ariyus, 2008) :

1. *Enkripsi:* merupakan proses penting yang terdapat dalam kriptografi, berupa pengamanan data atau informasi yang akan dikirimkan agar tetap rahasia. Plaintext atau pesan asli akan diubah menjadi kode-kode yang tidak dimengerti. Hasil dari enkripsi dinamakan cipher atau kode. Ketika kita tidak mengerti sebuah kata maka yang kita lakukan melihatnya didalam kamus atau melihatnya didaftar istilah. Bedanya pada proses enkripsi, proses mengubah teks-asli ke teks-kode kita menggunakan algoritma yang dapat merubah teks menjadi kode yang kita inginkan.
2. *Dekripsi:* merupakan kebalikan dari proses enkripsi. Pesan yang sudah melalui proses enkripsi dikembalikan ke bentuk pesan yang bisa terbaca, proses ini dinamakan proses dekripsi pesan. Algortima yang digunakan untuk mendekripsi pesan tentu berbeda dengan algoritma yang digunakan untuk mengenkripsi pesan.

3. *Kunci:* Di sini, kunci digunakan untuk melakukan proses enkripsi dan dekripsi. Kunci atau *key* dapat dibagi menjadi dua jenis, kunci pribadi *(private key)* dan kunci publik *(public key).*

Keamanan pada kriptografi modern dicapai dengan cara merahasiakan kunci yang dimiliki dari orang lain, tanpa perlu merahasiakan algoritma yang dipakai. Kunci atau *key* memiliki fungsi yang sama dengan kata sandi. Jika integritas dan keamanan sautu algoritma tergantung pada kunci yang digunakan, maka algortima tersebut dapat dipublikasikan dan dianalisis oleh orang lain. Jika suatu algoritma telah dipublikasikan dan dianalisa oleh orang lain dan dapat diselesaikan dalam waktu yang singkat oleh orang lain itu berarti algoritma tersebut tidak aman untuk digunakan. Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya:

1. Algoritma Simetri

   Algoritma Simetri disebut juga algoritma klasik karena pada algoritma simetri kunci yang digunakan untuk melakukan proses enkripsi maupun dekripsi sama. Saat mengirim pesan menggunakan algortima ini, penerima pesan harus mengetahui kunci pesan untuk mendekripsi pesan yang dikirim. Untuk kemanan pesan yang menggunakan algoritma ini tergantung pada kuncinya. Jika orang lain yang tidak memiliki wewenang atas pesan tersebut mengetahui kuncinya, dia dapat mengenkripsi dan mendekripsi pesan. Algortima yang menggunakan kunci simetris antara lain Data Encryption Standard (DES), RC2, RC4, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), One Time Pad (OTP) dan algoritma lainnya.

2. Algoritma Asimetri

   Untuk algoritma asimetri sendiri kuncinya terbagi menjadi dua, kunci umum (public key) yang boleh diketahui orang lain dan kunci rahasia (private key) kunci yang hanya boleh diketahui satu orang saja. Algoritma yang memakai kunci publik diantaranya Digital Signature Algorithm (DSA), Rivest Shamir Adleman(RSA), Elliptic Curve Cryptography (ECC) dan algortima lainnya.

3. Hash function

   Fungsi hash, umumnya dikenal sebagai hash satu arah (*one-way function*), *message digest, fingerprint,* fungsi kompresi dan *message authentication code* (MAC), adalah fungsi matematika yang mengambil input panjang variable dan mengubahnya menjadi urutan biner dengan panjang yang sama. Hash sering diperukan ketika ingin membuat sidik jari dari suatu pesan.

Kriptografi klasik merupakan suatu algoritma kriptografi yang sudah lama digunakan sejak beberapa abad lalu. Teknik ini menggunakan kunci yang sama untuk mengamankan data. Ada dua cara yang bisa digunakan pada algortima jenis ini :

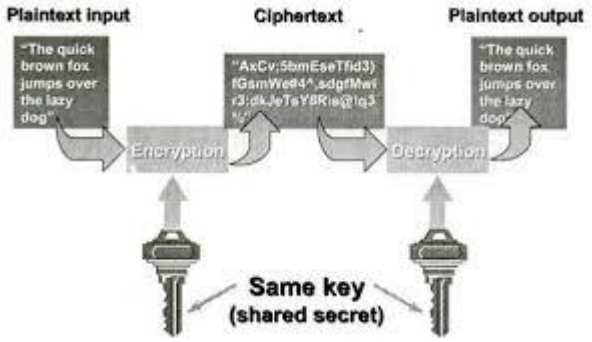
1. Teknik substitusi: Mengganti setiap karakter teks asli dengan karakter lain.
2. Teknik transposisi (permutasi): dilakukan dengan mutasi karakter.

Kriptografi modern memiliki kompleksitas yang sangat tinggi karena dioperasikan menggunakan komputer.

2.4 Algoritma Kriptografi Modern

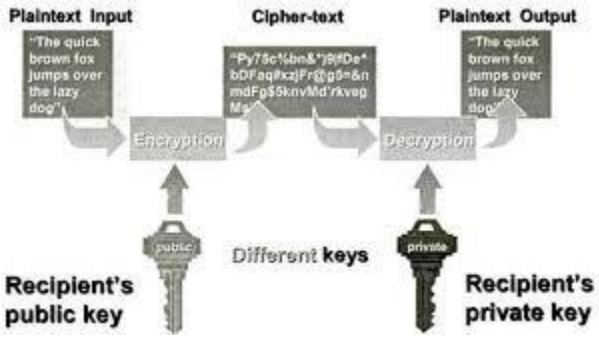
Kriptografi modern merupakan peningkatan dari kriptografi klasik. Dalam kriptografi modern, ada berbagai algoritma yang bertujuan untuk melindungi informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern terdiri dari dua bagian:

1. Algoritma simetris yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi.



Gambar 2. 1 Algoritma Simetris

2. Algoritma asimetris adalah algoritma pasangan kunci, satu digunakan untuk enkripsi dan yang lainnya digunakan untuk dekripsi. Siapa pun yang memiliki kunci publik dapat menggunakannya untuk mengenkripsi pesan, tetapi hanya satu orang saja yang memiliki rahasia kode yang dikirim. Contoh algoritma yang menggunakan kunci asimetris adalah RSA.



Gambar 2. 2 Algoritma Asimetris

2.5 Hill cipher

Hill cipher atau kode hill adalah sistem sandi *polialfabetik.* Artinya, anda dapat memetakan setiap karakter huruf alphabet ke beberapa jenis huruf. Kode ini oleh Lester S. Hill pada tahun 1929. Misalkan m adalah bilangan bulat positif, dan P = C = $(Z_{26})^m$. Ide dari kode hill adalah menggunakan m kombinasi linier dari m huruf alfabet dalam satu elemen teks asli untuk menghasilkan m huruf alfabet dalam satu elemen teks asli.

Dengan asumsi m = 2, Anda dapat menulis suatu elemen teks-asli sebagai x = (x_1, x_2) dan satu elemen teks-kode sebagai y = (y_1, y_2). Dimana y_1, y_2 adalah kombinasi linier dari x_1 dan x_2. Misalkan:

$y_1 = 11x_1 + 3x_2$ . . . . . .(2.1)

$y_2 = 8x_1 + 7x_2$ . . . . . (2.2)

Dapat ditulis dalam notasi matriks sebagai berikut:

$$(y_1, y_2) = (x_1, x_2)\begin{bmatrix}11 & 8\\ 3 & 7\end{bmatrix} \quad \text{. . . . . (2.3)}$$

Secara umum dengan menggunakan matriks K m x m sebagai kunci. Jika elemen pada baris i dan kolom j dari matriks K adalah $k_{i,j}$, maka dapat ditulis K = ($k_{i,j}$).

Untuk x = (x1,…,xm) ϵ P dan K ϵ K, dihitung y = e_K(x) = (y1,…,ym) sebagai berikut:

$$(y_1, y_2,\ldots, y_m) = (x_1, x_2,\ldots, x_m)\begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix} \ldots\ldots\ldots\ldots (2.4)$$

Dengan kata lain, y = xK.

Dikatakan bahwa teks-kode diperoleh dari teks-asli dengan cara transformasi linear. Untuk melakukan dekripsi menggunakan matriks inversi K^{-1}, dekripsi dilakukan dengan rumus x = yK^{-1}.

1. Perkalian matriks memiliki sifat asosiasif, yaitu (AB)C = A(BC).
2. Matriks identitas m x m, yang ditulis dengan I_m, adalah matriks yang berisi 1 pada diagonal utama dan berisi 0 pada elemen lainnya.

   Contoh matriks 2x2:

   $$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

I_m disebut dengan identitas karena AI_m = A untuk sembarang matriks 1 x m dan I_mB = B untuk sembarang matriks m x n.

3. Matriks inversi ddari A (jika ada) adalah A^{-1}dimana $AA^{-1} = A^{-1}A = I_m$.

Dengan menggunakan sifat-sifat matriks diatas, maka:

y = xK . . . . . .(2.5)

yK = (xK) K^{-1} = x(KK^{-1}) = xI_m = x . . . . . .(2.6)

Contoh :

dapat dilihat bahwa matriks enkripsi pada contoh sebelumnya memiliki invers Z_{26}

$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}^{-1} = \begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}$

Karena :

$$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix} = \begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix} = \begin{pmatrix}11*27+8*23 & 11*18+8*11\\ 3*7+7*32 & 3*18+7*11\end{pmatrix}$$

$$= \begin{pmatrix}261 & 286\\ 182 & 131\end{pmatrix}$$

$$= \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

Semua operasi aritmatik dilakukan pada modulo 26. Sebuah contoh untuk memberikan gambaran tentang enkripsi dan dekripsi dalam Hill cipher.

Misalkan kunci yang dipakai adalah :

$K = \begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$

Dari perhitungan di atas diperoleh bahwa :

$K^{-1} = \begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}$

Misalkan untuk mengenkripsi teks-asli JULY ada 2 elemen teks-asli untuk dienkripsi :

1. (9 , 20) = JU
2. (11, 24) = LY

Nilai JU dan LY diperoleh dari tabel substitusi, huruf J bernilai 9 dan U 20 :

Tabel 2. 1 Tabel Substitusi

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Kemudian lakukan perhitungan :

$$(9 , 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60 , 72 + 140) \bmod 26 = (3 , 4) = DE$$

Dan

$$(11 , 24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121+72 , 88+168) \bmod 26 = (11, 22) = LW$$

Sehingga enkripsi “JULY” adalah “DELW”, untuk mendekripsi dilakukan dengan cara :

$$(3 , 4) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \bmod 26 = (9 , 20)$$

Dan

$$(11 , 22) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \bmod 26 = (11, 24)$$

Dekripsi hanya mungkin dilakukan jika matriks K memiliki inversi. Suatu matriks K memiliki inversi jika dan hanya jika determinanya tidak nol. Namun karena Z_{26} maka matriks K memiliki inversi modulo 26 jika dan hanya jika gcd (det K,26)=1.

Untuk matriks A = $(a_{i,j})$ berukuran 2 x 2, nilai determnanya adalah :

$$\det A = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$$

Contoh:

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Maka

$$\det K = \det \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = 11*7 - 8*3 \bmod 26$$

$$= 77\text{-}24$$

$$= 53 \bmod 26$$

$$= 1$$

Kemudian 1-1 mod 26 = 1, sehingga matriks inversinya adalah :

$$K^{-1} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

2.6 *Rivest Shamir Adleman* (RSA)

Pada tahun 1976, peneliti dari kampus MIT *(Massachussetts Institute of Technology)* Cambridge, MA USA membuat algoritma kriptografi kunci publik yang disebut algoritma RSA yang merupakan singkatan dari nama mereka (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Dari berbagai macam algoritma kunci publik yang pernah dibuat, algoritma RSA adalah yang paling populer. Algoritma ini melakukan faktoriasasi yang sangat besar. Oleh karena itu, algoritma RSA dianggap aman. Keamanan RSA terletak pada sulitnya memfaktorkan bilangan bukan prima menjadi bilangan prima. Dalam hal ini r = p*q. Jika r berhasil difaktorkan menjadi p dan q, maka $\phi(r) = (p-1)(q-1)$ dapat dihitung. Selain itu, karena kunci enkripsi PK dideklarasikan (bukan rahasia) maka kunci dekripsi SK dapat dihitung dari persamaan PK.SK $\equiv 1\ (mod\ \phi\ (r))$.

Penemu algoritma RSA menyarankan bahwa panjang nilai p dan q melebihi 100 digit. Oleh karena itu, hasil kali r = p*q akan melebihi 200 digit. Mereka mengklaim bahwa dibutuhkan 4 miliar tahun komputasi untuk menemukan faktor bilangan prima 200 digit (algortima faktorisasi prima yang digunakan adalah algoritma yang tercepat saat ini digunakan, dan kecepatan komputer yang digunakan diasumsikan 1 milidetik). Algoritma RSA untuk memfaktorkan bilangan besar belum ditemukan. Untuk alasan ini, algoritma RSA akan terus digunakan. Algortima RSA direkomendasikan untuk digunakan dalam

pengkodean pesan sampai ada algoritma yang efektif untuk memfaktorkan bilangan bulat menjadi faktor prima (Ariyus, 2008).

Besaran yang digunakan dalam algoritma RSA adalah:

1. *p* dan *q* bilangan prima (*secret*)
2. $r = p * q$ (*non secret*)
3. $\phi(r) = (p-1)(q-1)$ (*secret*)
4. *PK* (*encoding key*) (*non secret*)
5. *SK* (*decoding key*) (*secret*)
6. *X* (*plaintext*) (*secret*)
7. *Y* (*chipertext*) (*non secret*)

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa:

$a^{\phi(r)} \equiv 1 \pmod{r}$. . . . . (2.7)

Yang dalam hal ini:

1. a harus relatif prima terhadap r.
2. $\phi(r)$ = r(1-1/p1)(1-1/p2) … (1-1/pn), yang dalam hal ini p1,p2,…,pn adalah faktor prima dari r.

   $\phi(r)$adalah fungsi yang menentukan berapa banyak bilangan 1,2,3 …, r yang relatif prima terhadap r.

Berdasarkan sifat $a^m \equiv b^m \pmod{r}$ untuk m bilangan bulat ≥ 1 maka persamaan (1) dapat ditulis menjadi:

$a^{m\phi(r)} \equiv 1^m \pmod{r}$

atau

$a^{m\phi(r)} \equiv 1 \pmod{r}$ . . . . . .(2.8)

Bila *a* diganti dengan X maka persamaan (2.8) menjadi :

$X^{m\phi(r)} \equiv 1 \pmod{r}$ . . . . . .(2.9)

Berdasarkan sifat ac ≡ bc (mod r) maka bila persamaan (2.9) dikali dengan X menjadi:

$X^{m^{\phi(r)+1}} \equiv X(\text{mod } r)$ . . . . . .(2.10)

Yang dalam hal ini X relatif prima terhadap r.

Misalkan SK dan PK dipilih sebagai berikut:

SK . PK ≡ 1 (mod ϕ (r)) . . . . . .(2.11)

atau

SK. PK = m ϕ(r)+1. . . . . .(2.12)

Subtitusikan (2.12) ke persamaan (2.10) untuk mendapatkan :

$X^{SK.PK} \equiv X(\text{mod } r)$ . . . . . (2.13)

Persamaan (2.13) dapat ditulis kembali menjadi :

$(X^{PK})^{SK} \equiv X(\text{mod } r)$ . . . . . .(2.14)

yang artinya perpangkatan X dengan PK diikuti dengan perpangkatan dengan SK menghasilkan X semula.

Berdasarkan persamaan (2.14) maka enkripsi dan dekripsi dirumuskan sebagai berikut :

$E_{PK}(X) = Y \equiv X^{PK} \text{ mod } r$. . . . . .(2.15)

$D_{SK}(Y) = X \equiv Y^{SK} \text{ mod } r$. . . . . (2.16)

Karena SK . PK = PK. SK maka enkripsi diikuti dengan dekripsi ekuivalen dengan dekrips diikuti enkripsi:

$E_{SK}(D_{SK}(X)) = D_{SK}(E_{PK}(X)) \equiv X^{PK} \text{ mod } r$. . . . . .(2.17)

$X^{PK} \text{ mod } r \equiv (X + mr)^{PK} \text{mod } r$ untuk sembarang bilangan bulat m, jadi tiap teks asli X, X + r, X + 2r,… menghasilkan teks kode yang sama. Dengan kata lain, perubahannya dari banyak ke satu. Untuk membuat konversi satu-ke-satu, perlu untuk membatasi X dalam himpunan {0,1,2,…,r - 1}sehingga enkripsi dan dekripsi tetap benar seperti pada persamaan (2.14) dan (2.15).

Algoritma pembangkitan kunci untuk algoritma RSA dapat digambarkan sebagai berikut :

1. Tentukan 2 bilangan prima yang diberi nama p dan q. Misal nilai p = 61 dan q = 53
2. Melakukan perhitungan nilai modulus (n) :

$$n = p * q \quad (2.18)$$

$$n = 61 \times 53$$

$$n = 3233$$

3. Melakukan perhitungan nilai totient n :

$$(n) = (p-1)*(q-1) \quad (2.19)$$

$$(n) = (61-1)*(53-1)$$

$$(n) = (60*52)$$