BAB II

TINJAUAN PUSTAKA

2.1. State Of The Art

State of the art adalah bagian dari penelitian dimana penulis melakukan studi literatur dengan mengumpulkan jurnal sebagai bahan referensi pada penelitian ini. State Of The Art pada penelitian ini turut memberikan penjabaran mengenai penelitian terdahulu dan penelitian yang akan dilakukan [3]. Adapun beberapa referensi yang digunakan sebagai berikut;

Disusun oleh Juni Ade Nawer Purba, Debora Sinaga, Saima Ronita Purba, pembahasan pada penelitian ini mengenai proses enkripsi yang dimulai dengan mengubah data audio menjadi data hexa dimana data tersebut diubah menjadi data biner yang kemudian dikelompokan berdasarkan sub-blok bit dimana setiap blok diubah menjadi nilai desimal data-data adalah planning teks yang kemudian akan dilakukan proses komputasi dengan menggunakan paillier cryptosystem. Berdasarkan penelitian diatas paillier cryptosystem dapat digunakan untuk tipe file berupa mp3, dan dapat digunakan pada tipe file seperti gambar, dan video[4].

Di oleh Juni Ade Nawer Purba, Taroni Sokhi Zebua, Rivalry K H, pembahasan pada penelitian ini mengenai proses penerapan Algoritma paillier cryptosystem dengan mengimplementasikannya pada media citra digital pada aplikasi chat [5]. Proses dimulai dari merubah data pesan yaitu gambar menjadi bilangan heksa kemudian diubah menjadi bentuk biner, setiap data biner akan dikelola menjadi sub-blok bit dari sub-blok bit tersebut dilakukan konversi menjadi

data desimal yang mana data data tersebut di enkripsi dan di deskripsi dengan menggunakan Algoritma Paillier Cryptosystem.

Disusun oleh Bukhari Ugbede Umar, Olayemi Mikail Olaniyi, Daniel Oluwaseun Olajide and Eustace Manayi Dogo, pembahasan pada penelitian ini mengenai sistem pemilihan elektronik yang mana didalamnya berisi infrastruktur yang cukup kompleks dalam penelitian ini menggunakan blockchain dimana dengan mengadaptasi Proof of Work. Data data hasil voting akan langsung dieksekusi sebelum masuk ke blockchain sebagai data yang telah terenkripsi pun akan terdeskripsi setelah melewati blockchain [6].

Disusun oleh Pranav Verma, Anish Mathuria, and Sourish Dasgupta, pembahasan pada penelitian ini mengenai penerapan pada sistem rekomendasi dengan memanfaatkan Algoritma Paillier Cryptosystem untuk mengenkripsi data data aktivitas pengguna yang mana data tersebut akan memudahkan sampai 30% derdaskan penelitian yang telah dilakukan dengan beberapa percobaan pada saat pengembangan sistem tersebut [7]

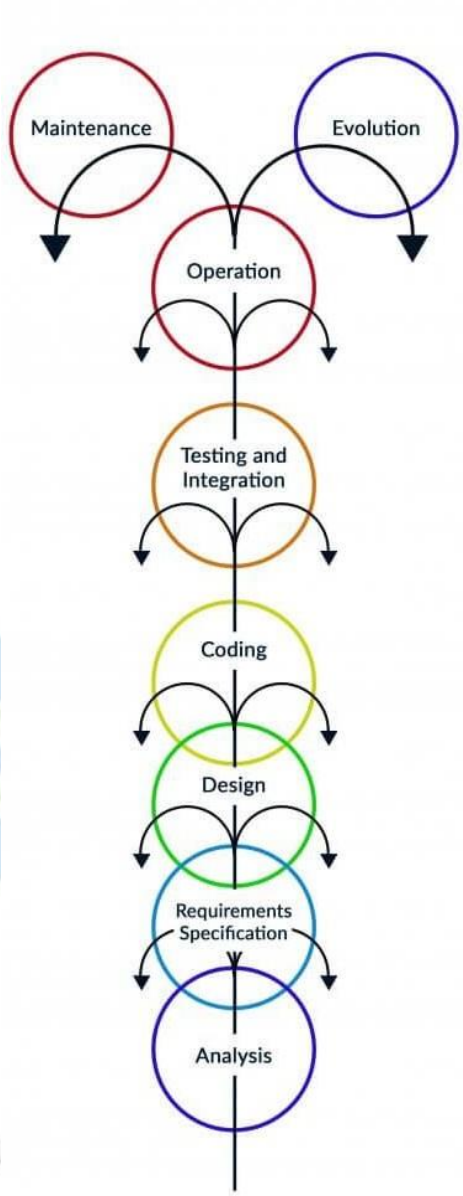
Disusun oleh Kundan Munjala, Rekha Bhati, pembahasan pada penelitian ini mengenai perbandingan dua algoritma dalam melakukan enkripsi dan deskripsi waktu komputasi berdasarkan journal tersebut didapat hasil RSA lebih cepat baik pada proses enkripsi dan deskripsi dikarenakan proses skema homomorfik pada paillier cryptosystem yang lebih komplek dan membutuhkan waktu lebih dibandingkan paillier[1].

Disusun oleh Mohamed-Lamine Messai, Gérald Gavin, Jérôme Darmont, pembahasan pada penelitian ini mengenai perbandingan dari beberapa beberapa skema enkripsi homomorfik (HE) yang terkenal, dari tiga kategori enkripsi homomorfik: Partially HE, Somewhat HE, dan Fully HE, menunjukan bahwa sistem kriptografi Sebagian lebih cepat daripada yang lainnya dalam operasi penambahan dan perkalian. RSA memiliki waktu yang lebih cepat saat pembuatan kunci sementara El-Gamal lebih lama dari Paillier dan RSA [1].

Disusun oleh Bianca Jansen van Rensburg, Pauline Puteaux, William Puech,Jean-Pierre Pedeboy, pembahasan pada penelitian ini mengenai menawarkan sebuah metode baru RDH-ED (reversible data hiding in the encrypted domain) dalam menyembunyikan data pada objek 3D yang terenkripsi secara reversibel berdasarkan sistem Paillier Cryptosystem dengan Skema homomorfik memiliki kemampuan untuk menyembunyikan data dan hasil enkripsi tanpa mengurangi kualitas atau integritas objek[8].

2.2. Fountain

Penulis menggunakan metode Fountain dalam pengembangan perangkat lunak dikarenakan metode ini lebih efektif dalam melakukan penelitian, dimana pendekatan alur kerja perangkat lunak secara sekuensial atau terurut dimana pada tahap awal adalah proses Analisa, kemudian lanjut pada tahap desain, pengkodean, kemudian pengujian dan tahap pendukung/support [3] Adapun tahapan pada Fountain adalah sebagai berikut;



Gambar 2.1 Fountain [3]

1. Analisa Kebutuhan Software

Dalam proses Analisa kebutuhan software berfungsi untuk mengidentifikasi semua kebutuhan yang terkait termasuk didalamnya

adalah dokumentasi dan interface yang diperlukan guna sebagai proses kinerja system [3]

2. Desain

Pada proses desain, penulis menyesuaikan pada kebutuhan sistem akan dibuat terkait rancangan database, software architecture, dan user interface. Penulispun menggunakan Unified Modeling Language (UML) guna menjelaskan maksud rancangan secara mendetail UML yang digunakan adalah Use Case Diagram [9].

3. Coding

Pada tahap ini adalah proses ini adalah salah satu tahapan dalam membangun aplikasi dengan melakukan pengkodean data dengan menggunakan Bahasa pemrogram dan pada penelitian ini Bahasa yang digunakan adalah Java script & PHP.

4. Integration & Testing

Pengujian sistem menggunakan Black Box dengan beberapa kali percobaan guna mendapatkan hasil sesuai yang diharapkan dari rancangan yang telah dibuat, dengan kesesuaian data pada aplikasi.

Proses pemeliharaan penulis mencoba untuk nantinya sistem yang sudah terbentuk dapat di kembangkan dalam keperluar tertentu.

5. Evaluation & Maintenance

Proses pemeliharaan penulis mencoba untuk nantinya sistem yang sudah terbentuk dapat di kembangkan dalam keperluar tertentu

2.3. Citra Digital

Citra digital adalah representasi diskrit dari gambar atau visual yang terdiri dari elemen-elemen kecil yang disebut piksel. Piksel merupakan unit terkecil dalam citra digital yang memiliki nilai intensitas cahaya atau warna yang merepresentasikan bagian kecil dari gambar tersebut. Piksel-piksel ini membentuk matriks dua dimensi yang menggambarkan gambar secara keseluruhan.

Piksel merupakan elemen dasar dalam citra digital. Setiap piksel memiliki intensitas cahaya atau nilai warna yang dapat dinyatakan dalam format grayscale atau RGB (Red, Green, Blue). Dalam citra grayscale, setiap piksel hanya memiliki nilai intensitas keabuan tunggal yang berkisar antara 0 hingga 255. Pada citra RGB, setiap piksel memiliki tiga komponen warna (merah, hijau, biru) yang berkisar antara 0 hingga 255 untuk masing-masing komponen [10]

Resolusi citra digital mengacu pada jumlah piksel yang ada dalam gambar. Resolusi yang lebih tinggi menghasilkan gambar dengan detail yang lebih baik, sedangkan resolusi yang lebih rendah menghasilkan gambar dengan detail yang lebih kasar. Resolusi citra digital dinyatakan dalam pixel per inch (PPI) atau dots per inch (DPI), yang menunjukkan jumlah piksel yang ada dalam satu inci ruang gambar.

Format citra digital mengacu pada cara penyimpanan dan representasi data dalam citra. Format yang paling umum adalah JPEG (Joint Photographic Experts Group) yang menggunakan kompresi dengan kehilangan (lossy compression) untuk mengurangi ukuran file. Format lainnya termasuk PNG (Portable Network Graphics) yang menggunakan kompresi tanpa kehilangan (lossless compression)

untuk menjaga kualitas gambar, serta format TIFF (Tagged Image File Format) yang mendukung penyimpanan citra dengan resolusi tinggi dan tanpa kehilangan.

Bit depth merujuk pada jumlah bit yang digunakan untuk mewakili nilai intensitas atau warna setiap piksel. Bit depth yang lebih tinggi memberikan rentang nilai yang lebih luas dan memungkinkan representasi warna yang lebih halus dan detail, sementara bit depth yang lebih rendah membatasi jumlah warna yang dapat direpresentasikan. Bit depth umumnya bervariasi antara 8 bit (256 warna) hingga 16 bit (65.536 warna) dalam citra digital.

Metadata adalah informasi tambahan yang terkait dengan citra digital. Metadata dapat berisi informasi tentang kamera yang digunakan, tanggal dan waktu pengambilan gambar, koordinat lokasi, dan lainnya. Metadata juga dapat mencakup informasi tentang parameter pemrosesan, seperti kecerahan, kontras, dan saturasi yang digunakan dalam pengolahan citra.

2.4. Kriptografi

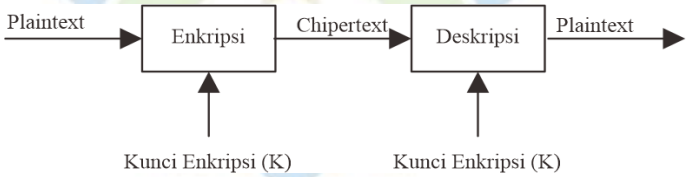
Kriptografi memiliki sejarah Panjang. Informasi sejarah mengenai kriptografi ditulis dalam buku David Khan yang berjudul The codebreakers [11]. Buku tersebut memiliki tebal 1000 halaman yang berbicara awal mula pembentukan sandi-sandi dari bangsa Mesir 4000 Tahun sebelum masehi, hingga penggunaannya sampai ke abad 20.

Kriptografi merupakan suatu Teknik memanipulasi data dengan simbol-simbol tertentu untuk mengamankan data dari pihak yang tidak bertanggung jawab. Proses manipulasi data atau yang biasa dikenal sebagai Teknik komputasi yang

menggunakan metode dari suatu algoritma untuk memproses data yang dapat diolah menjadi suatu data yang sulit dibaca atau dikenali.

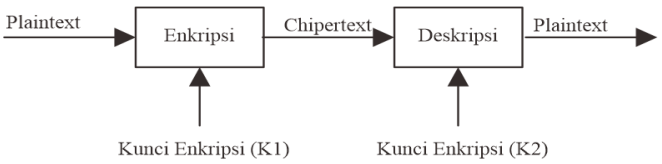
Ilmu kriptografi sejalan dengan kemajuan teknologi. Berdasarkan perkembangannya ilmu kriptografi terbagi menjadi 2 bagian yaitu kriptografi klasik dan kriptografi modern keduanya bersifat kriptologis.

Kriptografi klasik memiliki ciri khusus diantaranya memiliki kunci simetri. Kriptografi simetris atau konvensional kriptografi adalah algoritma yang menggunakan kunci yang serupa pada proses enkripsi maupun deskripsi. Kriptografi klasi memiliki 2 pengelompokan model Teknik yaitu Teknik substitusi dan transformasi.



Gambar 2.2 Kriptografi simetris [7].

Kriptografi Modern memiliki ciri khas dimana kriptografi ini berpola asimetris. Dimana algoritma menggunakan kunci yang berbeda untuk proses enkripsi dan deskripsi [12]. Kunci publik dapat disebarkan secara umum saat proses enkripsi. Prinsip kerjanya jika pengguna memiliki sepasang kunci publik dan kunci pribadi, kunci publik akan mendistribusikan kepada umum, sedangkan kunci pribadi akan disimpan kedalam database.



Gambar 2.3 Kriptografi asimetris [1].

2.5. Paillier Cryptosystem

Paillier Cryptosystem merupakan Algoritma kriptografi yang ditemukan oleh Pascal Paillier pada tahun 1999 yang merupakan bagian dari algoritma asimetris probabilistik guna kriptografi kunci publik. Permasalahan dari perhitungan algoritma ini terletak pada nilai n-residue class dimana nilai ini sangat sulit untuk dikomputasi. Permasalahan ini disebut dengan istilah asumsi Composite Residuos Itu (CR) yang merupakan fundamental dari kriptosistem Paillier [1]. Skema tersebut adalah Additive homomorphic cryptosystem adalah proses diberikannya kunci publik dan enkripsi dari m1 dan m2, seseorang akan mampu menghitung enkripsi dari m1+m2 Adapun keterangan dari notasi-notasi yang dipergunakan pada algoritma ini.

$$Zn - \text{Sekumpulan bilangan Integer n}$$

$$Z * n - \text{Sekumpulan bilangan Integer yang relatif prima terhadap n}$$

$$Z * n^2 - \text{Sekumpulan bilangan Integer yang relatif prima terhadap } n^2$$

1. Proses pembangkitan Kunci

   Faktor bilangan prima pada p dan q Ketika dibangkitkan harus berdasarkan kaidah-kaidah yang umum berlaku dimana p dan q adalah bilangan prima acak supaya n menjadi sangat sulit untuk di faktorkan. Skema selanjutnya dibutuhkan juga nilai $\lambda = \text{lcm}(p-1, q-1)$ dimana kelipatan dari bilangan prima 160 bit, bilangan ini di dapatkan saat pembangkitan bilangan prima acak yang biasa digunakan pada DSA, RSA dan Teknik-teknik lainnya yang berkesesuaian lainnya [7]

   Bilangan basis g yang dipilih secara acak dari elemen-elemen nilai ordernya dapat dibagi, ada yang perlu diperhatikan pada skema ini akan membutuhkan perlakuan yang istimewa (seringnya elemen berupa orde yang paling tinggi pangkat λ/α). Semua proses pembangkitan kunci ini dapat dipermudah dengan menggunakan komputasi mod p^2dan mod q^2dan Chinese-remainder in gmod p^2 dan g mod q^2 pada akhirnya [1]. Adapun Rumus Pembangkitan Kunci adalah sebagai berikut;

   $L(g^{\lambda} \bmod n^2)^{-1} \bmod n$ or $L(g^{\alpha} \bmod n^2)^{-1}$, dapat dikonstankan.

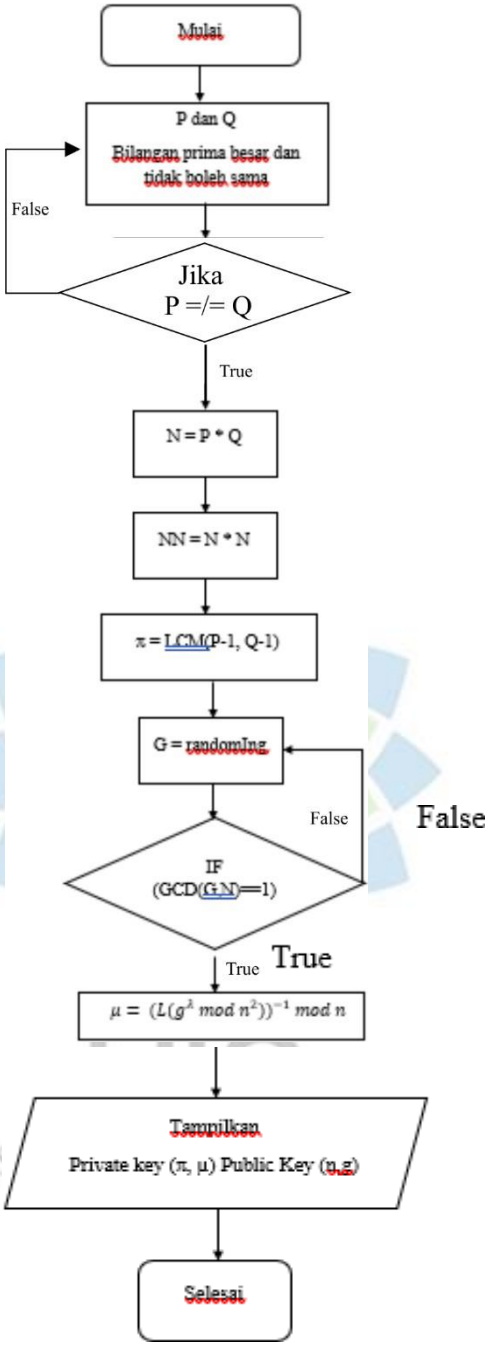
Rumus dari Algoritma Paillier Cryptosystem

1. Pilih bilangan p dan q secara acak
2. Hitung nilai n, dimana n = p * q
3. Hitung nilai λ = lcm (p-1, q-1)
4. Pilih bilangan bulat . g dimana g ϵZ^*_{n2}
5. Perhatikan n agar memenuhi

$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$

Dimana L adalah $L(u) = \frac{u-1}{n}$

6. Kunci Publik adalah (n,g) dan kunci private (λ, μ)



Gambar 2.4 Flowchart Pembangkitan kunci [7]

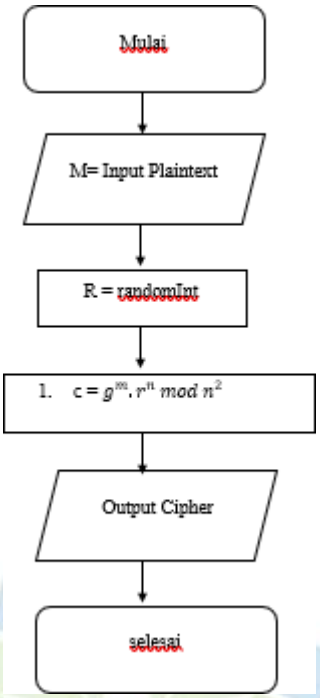
1. Enkripsi

Enkripsi memerlukan eksponensial modular dengan memanfaatkan basis g, proses komputasi dapat dipersingkat dengan memanfaatkan nilai g yang benar, contoh memberikan nilai yang kecil terhadap g, seperti g = 2, akan berdampak lurus dengan waktu pada saat proses komputasi yang lebih signifikan dengan faktor 1/3. jika nilai yang terpilih memenuhi keperluan persyaratan $g \epsilon \beta$.

Bisa saja g dibuat statis dengan menetapkan nilainya sebelum pembangkitan kunci berlangsung melalui beberapa penyesuaian konsep. Terlebih perhitungan perpangkatan untuk basis-basis yang telah desain konstan tadi akan berpengaruh pada percepatan dan memungkinkan mengurangi kebutuhan komputasi. Komputasi ini mengenai r^n dan g^{nr} bisa dilakukan perhitungan pada saat enkripsi berjalan [7].

Rumus Enkripsi

1. Jika m adalah pesan yang akan di enkripsi maka $m \in Z_n$
2. Pilih nilai r . dimana $r \epsilon Z_n^*$
3. Chiperteks c nya adalah $c = g^m . r^n \bmod n^2$



Gambar 2.5 Flowchart Enkripsi [7]

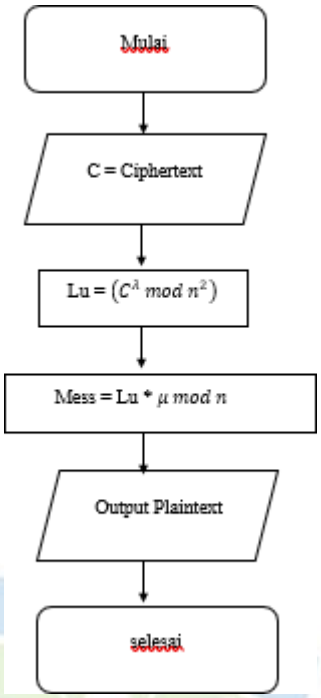
2. deskripsi

Deskripsi adalah bagaimana cara menghitung nilai L(u) dimana u ϵ S_n dapat dihitung berdasarkan komputasi yang rendah, dengan mulai menghitung nilai $n^{-1} \bmod 2^n$ parameter konstan [7].

Rumus Deskripsi

Jika c merupakan chiperteks dimana c ϵZ^*_{n2}

Planiteks m adalah $m = L(C^{\lambda} \bmod n^2).\mu \bmod n$



Gambar 3.5 Flowchart Dekripsi [7]

2.6. Definisi UML

Berangkat dari definisi UML atau Unified Modeling Language Pemodelan untuk memberikan suatu konsep dari sebuah software yang berkorelasi pada suatu objek [8]. Pemodelan menggunakan UML sangat cocok untuk membuat sebuah perangkat lunak yang berorientasi objek (Java, C, Php) selain itu dapat digunakan di Bahasa pemrograman yang prosedural.

Bagian dari UML antara lain:

1. Actor

   Aktor adalah semua entitas yang berinteraksi dengan sistem dari luar, seperti manusia dan benda

2. Class

   Kelas merupakan notasi notasi prioritas dan fundamental dalam UML dimana setiap notasi memiliki atributnya serta operasinya

3. Use case

   Use case bekerja dengan cara menerangkan tipe transaksi anatara pengguna atara sistem satu dengan sistem lainnya, dimana dimulai dari bagaimana sistem digunakan

4. Class Diagram

   Suatu Penjelasan mendetail yang berkaitan pada sebuah objek dan ini merupakan bagian dari sebuah pengembangan berorientasi objek. Singkatnya class diagram merupakan pengembangan dari struktur dan menjelaskan hubungan antara class, packed, objek pada suatu sistem.

5. Activity Diagram

   Pengembangan dari beberapa alur kerja dimana Penjelasan aktivitas awal dari sebuah sistem hingga berakhir secara mendetail.

6. Sequence Diagram

   Tingkat lanjut dari sebuah interaksi objek yang terkait suatu sistem atau tidak disekitar sistem seperti user, display, sound berupa pesan yang dikirim dan divisualisasikan.