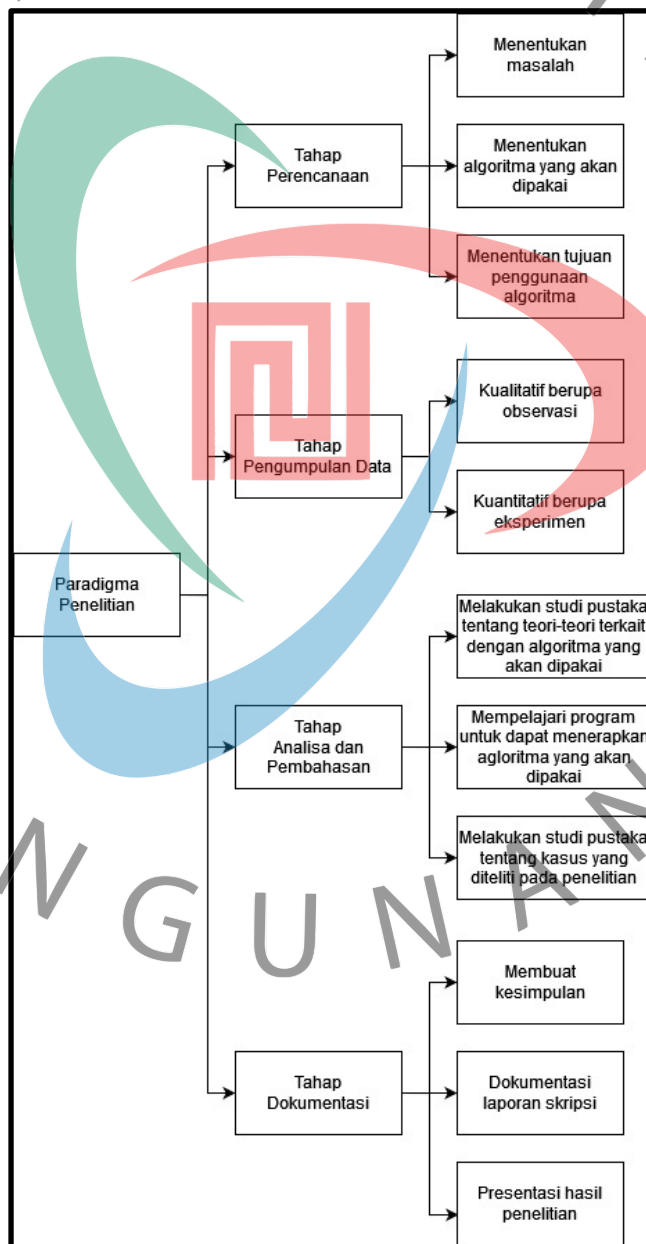


BAB III METODE PENELITIAN

Pada penelitian yang dilakukan, maka penulis menggunakan metode penelitian kualitatif dan kuantitatif (*mixed method*).

3.1. Paradigma Penelitian

Pada bagian ini penulis menggunakan *hierarchy diagram* untuk dapat menjelaskan konsep penelitian yang akan dilaksanakan oleh penulis.



Gambar 3.1. Konsep Penelitian

3.1.1. Tahap Perencanaan

Tahap perencanaan pada penelitian ini berguna untuk menentukan tahap pada awal penelitian. Adapun hal yang dibahas pada tahap perencanaan, sebagai berikut ini.

1. Menentukan masalah

Penulis melakukan riset mengenai hal yang dapat untuk dijadikan sebagai bahan penelitian pada ranah teknologi dan informasi di *era modern* saat ini, seperti *criptography*, *cyber security*, *data security system*, dan *network security*.

2. Menentukan algoritma yang akan dipakai

Penulis melakukan studi pustaka untuk mencari dan mengenali algoritma yang dapat dipakai untuk tujuan kriptografi.

3. Menentukan tujuan penggunaan algoritma

Penulis menentukan tujuan penggunaan algoritma untuk dapat dijadikan sebagai judul penelitian pada skripsi.

3.1.2. Tahap Pengumpulan Data

Tahap pengumpulan data pada penelitian ini merupakan tahapan kedua, di mana data yang telah terkumpul diperlukan untuk mempermudah penelitian yang sedang dilakukan oleh penulis. Pada proses pengumpulan data, metode yang dipakai adalah sebagai berikut ini.

1. Kualitatif

Penulis melakukan metode penelitian kualitatif, berupa observasi sehingga penulis dapat mengumpulkan data yang diperlukan pada riset ini. Di mana data tersebut merupakan hasil dari pengamatan yang dilakukan sendiri oleh penulis selama pengujian menggunakan sistem enkripsi dan dekripsi pada data hasil registrasi *online* peserta pelatihan dan sertifikasi.

2. Kuantitatif

Penulis melakukan metode penelitian kuantitatif, berupa eksperimen sehingga penulis dapat mengumpulkan data yang diperlukan pada riset ini. Di mana data tersebut merupakan hasil pengolahan dari sistem enkripsi dan dekripsi pada data hasil registrasi *online* peserta pelatihan dan sertifikasi.

3.1.3. Tahap Analisa dan Pembahasan

Tahap Analisa dan pembahasan merupakan tahapan ketiga yang mana data yang telah terkumpul dianalisa dan dilakukan pembahasan, sehingga penulis mendapatkan ilmu dan pengetahuan. Adapun hal yang dibahas sebagai berikut ini.

1. Melakukan studi pustaka mengenai algoritma yang akan dipakai

Penulis melakukan studi pustaka tentang teori-teori terkait dengan algoritma yang akan dipakai, pada riset ini maka penulis mempelajari teori-teori tentang algoritma *advanced encryption standard* atau dengan nama lain algoritma *rijndael* dan algoritma *base64*.

2. Mempelajari program untuk implementasi algoritma yang akan dipakai

Penulis mempelajari bagaimana membuat kode program untuk penggunaan algoritma *advanced encryption standard 256 bit* dan algoritma *base64 encoding*, selanjutnya menerapkan kedua algoritma tersebut pada aplikasi *web* yang dibangun oleh penulis, di mana tujuan dari penggunaan kedua algoritma tersebut untuk kriptografi. Pada penelitian ini maka penulis mempelajari kedua algoritma tersebut pada bahasa pemrograman *PHP v8* dengan *framework codeigniter v4*.

3. Melakukan studi pustaka untuk kasus yang diteliti

Penulis mempelajari studi pustaka tentang kasus yang diteliti pada penelitian, seperti pengenalan mengenai kejahatan siber pada peretasan data *user* dari *server*, *data breaching*, dan *data security system*.

3.1.4. Tahap Dokumentasi

Pada tahap keempat maka yang dikerjakan merupakan dokumentasi tertulis yang diwujudkan dalam bentuk laporan penelitian skripsi, yang mana untuk secara jelas dan *detail* dapat memberikan hasil dari penelitian tentang sistem pengamanan data hasil registrasi peserta pelatihan dan sertifikasi menggunakan algoritma *advanced encryption standard* dan algoritma *base64 encoding*.

1. Membuat kesimpulan

Penulis membuat kesimpulan dari penelitian yang telah dikerjakan tentang hasil penerapan pada penggabungan algoritma *AES* dan algoritma *base64* pada sistem aplikasi, dan mengenai hasil dari perancangan kode program

PHP v8 pada *framework codeigniter v4* untuk mengamankan hasil registrasi *online* peserta pelatihan dan sertifikasi menggunakan algoritma *advanced encryption standard 256 bit* dan algoritma *base64 encoding* yang mana hal ini diwujudkan dalam bentuk observasi dan eksperimen.

2. Dokumentasi laporan skripsi

Penulis membuat dokumentasi penelitian skripsi, yang mana isi dari dokumentasi ini didapat pada hasil kesimpulan yang dibuat.

3. Presentasi hasil penelitian

Hasil dari dokumentasi penelitian skripsi yang telah dibuat oleh penulis akan dipresentasikan kepada penguji, di mana untuk memberikan hasil dari penelitian yang telah dikerjakan.

3.2. Metode Penelitian

- Penelitian ini dilaksanakan dengan penerapan metode kombinasi antara kualitatif dan kuantitatif. Aspek kualitatif diwujudkan dengan observasi, dan aspek kuantitatif diwujudkan dengan eksperimen, di mana pengumpulan data merupakan hasil dari input dan output yang masuk ke aplikasi selama operasi. Hal-hal yang menjadi penelitian dalam observasi dan eksperimen adalah sebagai berikut ini.

1. Algoritma kriptografi *advanced encryption standard 256 bit*, dan algoritma *base64 encoding* dalam mengamankan data registrasi *online* peserta, di mana data tersebut berupa *plaintext* yang dienkripsi (*encipher*) menjadi *ciphertext* selanjutnya diencode (*encoding*) menjadi *index base64* dan disimpan ke dalam database dengan tujuan untuk *data security system*.
2. Proses *decoding* data *index base64* yang terdapat dalam database sehingga menjadi *ciphertext* selanjutnya didekripsi (*decipher*) menjadi *plaintext* untuk ditampilkan pada halaman *administrator* dan *user data*.
3. Proses *encoding* dalam *generate token random bytes 32 characters* untuk *account authentication* berupa *link (hyperlink)* yang dikirim oleh sistem melalui pesan *email*.

Data yang diperoleh pada penelitian ini, berupa data hasil enkripsi (*encipher*), dekripsi (*decipher*), *encoding*, dan *decoding* yang terjadi selama pengoperasian sistem pada aplikasi.

3.2.1. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan untuk memperoleh data riset pada penelitian ini merupakan teknik dokumentasi. Teknik dokumentasi merupakan proses memperoleh data melalui dokumen-dokumen pendukung yang secara tidak langsung berhubungan dengan riset yang akan diteliti. Studi pada dokumentasi merupakan proses pengumpulan data dengan mengkaji dokumen tertulis.

Metode dokumentasi yang digunakan untuk memperoleh data, yaitu dari database *system* dan data pada *file excel*. Studi dokumentasi yang dilakukan pada metode penelitian kualitatif merupakan sumber data untuk melengkapi metode pengumpulan data.

Metode dokumentasi termasuk dalam metode pengumpulan data kualitatif dengan menganalisis dokumen-dokumen tertulis. Dokumentasi merupakan salah satu cara yang dapat dilakukan oleh penulis dalam penelitian kualitatif untuk memperoleh sudut pandang, berupa gambaran subjek dari riset. Dengan metode ini, maka penulis dapat memperoleh data dari dokumen yang sudah ada, di mana penulis dapat memperoleh catatan-catatan yang berhubungan secara tidak langsung dengan penelitian yang diteliti, seperti gambaran umum dari data hasil registrasi peserta. Metode dokumentasi yang dilakukan oleh penulis bertujuan untuk mendapatkan data-data yang belum diperoleh pada metode observasi.

Salah satu rangkaian *vital* dalam metode penelitian adalah metode pengumpulan data, yang mana hal tersebut merupakan memperoleh data-data yang dibutuhkan pada penelitian yang diteliti. Oleh karena itu, dalam menunjang keberhasilan penelitian kualitatif, maka tergantung pada ketelitian penulis, dan kelengkapan data yang diteliti menggunakan aspek dokumentasi untuk penerapan algoritma kriptografi berupa *advanced encryption standard*, dan *base64 encoding*.

Adapun langkah-langkah pada pengumpulan data studi dokumentasi adalah sebagai berikut ini.

1. Studi dokumentasi
 - a. Pengumpulan data dilakukan untuk memperoleh data-data yang diperlukan dalam penelitian ini sehingga data tersebut dapat diolah dengan baik oleh penulis, metode pengumpulan data yang dilakukan berupa studi dokumentasi pada database *management system*.

- b. Studi dokumentasi yang dilakukan oleh penulis adalah membuat kode program pada sistem untuk dapat memproses data yang disimpan ke dalam database, yang mana data tersebut harus dienkripsi menggunakan algoritma *advanced encryption standard* dan *decode* menggunakan algoritma *base64*.
- c. Pelaksanaan pengumpulan data dengan studi dokumentasi melibatkan berbagai aktivitas pendukung lainnya dalam hal ini, yaitu merancang kode program untuk penerapan kedua algoritma tersebut sebagai ilmu kriptografi yang mana dapat dikelola untuk *data security system*, *web security*, *cyber security*, dan *network security*.
- d. Data lain yang digunakan oleh penulis, yaitu data-data yang didapat dari *file excel*.

● 3.2.2. Metode Analisis Data

Pada penelitian yang dilakukan dengan metode kualitatif pada tahap observasi berupa data yang masuk ke aplikasi selama operasi, yaitu pengamatan dan pengujian algoritma *advanced encryption standard 256 bit* dan algoritma *base64 encoding* untuk ilmu kriptografi dalam mengamankan data registrasi *online* peserta, di mana penerapan kedua algoritma ini sebagai *double security* pada perancangan *data security system*.

Metode kuantitatif pada tahap eksperimen pengujian aplikasi pada penelitian yang dilakukan, di mana hasil didapat dari output aplikasi *web* menunjukkan bahwa sistem dapat melakukan proses enkripsi, dekripsi, *encoding*, *decoding*, dan *generate token random bytes 32 characters*, di mana *token* tersebut disematkan pada *link (hyperlink)* yang dikirim oleh sistem melalui *email* untuk *account authentication*.

Metode kualitatif pada tahap pengumpulan data yang digunakan untuk memperoleh data riset merupakan studi dokumentasi. Di mana pada penelitian ini, metode dokumentasi yang digunakan untuk memperoleh data, yaitu dari database *system* dan data pada *file excel*. Studi dokumentasi yang dilakukan pada metode penelitian kualitatif merupakan sumber data untuk melengkapi metode pengumpulan data.

Penulis memahami hasil dari output yang terjadi karena penulis telah mempelajari dengan baik implementasi kode program *PHP* yang disertai dengan *framework codeigniter v4* dalam penggunaan algoritma *advanced encryption standard* pada proses enkripsi dan dekripsi, dan algoritma *base64* sebagai proses *encoding* dan *decoding*.

Metode yang digunakan dalam analisis data pada tahap observasi, dan dokumentasi adalah kualitatif, sedangkan pada tahap eksperimen adalah kuantitatif. Metode analisis data pada penelitian ini dilakukan dengan *black box testing*, dan *white box testing*, di mana kedua hal tersebut ditujukan untuk membantu dalam penelitian, dan mempelajari hasil dari kode program yang dirancang pada sistem aplikasi, diwujudkan melalui *validation testing*.

3.2.3. Metode Pengujian Data

- Pengujian data dilakukan pada sisi *client* dan *server*, hal-hal yang menjadi keutamaan adalah sebagai berikut ini.
 1. Pengujian apakah aplikasi beroperasi dengan baik dalam mengolah data registrasi *online* peserta.
 2. Pengujian sistem pada aplikasi dalam mengamankan data registrasi *online* peserta dengan penerapan algoritma *advanced encryption standard* dan algoritma *base64*.
 3. Pengujian proses kerja sistem pada aplikasi dalam proses enkripsi dan dekripsi data.
 4. Pengujian proses kerja sistem pada aplikasi dalam proses *encoding* dan *decoding* data.
 5. Pengujian proses kerja sistem pada aplikasi dalam menjalankan perintah yang diberikan oleh *user*.

Hal tersebut untuk mempelajari apakah unsur kebaruannya tercapai, dan untuk mengenali permasalahan pada sistem berupa *bug* maupun *error*. Metode yang digunakan pada pengujian data, yaitu *white box testing* dan *black box testing*. Pada *white box testing*, maka penulis melakukan pengujian terhadap kode program ketika dioperasikan untuk selanjutnya dijadikan sebagai bahan riset dalam mempelajari kode program *PHP v8* yang telah dirancang dengan *framework codeigniter v4*.

Pada *black box testing*, maka penulis melakukan pengujian terhadap aplikasi *web*, di mana hasil didapat dari output untuk selanjutnya dijadikan sebagai bahan riset dalam mempelajari sistem pada aplikasi yang telah dirancang.

Baik dari *whitebox testing* maupun *black box testing*, menghasilkan data berupa enkripsi (*encipher*), dekripsi (*decipher*), *encoding*, dan *decoding*. Untuk penulis dapat mengenkripsi dan mendekripsi data dari output yang terjadi karena penulis merancang kode program *PHP* pada sistem untuk dapat *generate random cipher key*, yang mana hasil dari *generate random key* tersebut dapat penulis pakai untuk proses enkripsi dan dekripsi data menggunakan kode program *PHP*, selanjutnya penulis merancang kode program *PHP* untuk *encode (encoding) ciphertext* ke dalam *index base64* sehingga hasil enkripsi menjadi sulit untuk diretas karena terdapat 2 fase yang harus dilalui, yaitu *decoding* dan *decrypting*.

● 3.2.4. Metode Penarikan Kesimpulan ●

Penarikan kesimpulan dilakukan dengan cara menilai secara langsung sistem dalam mengamankan dan melindungi data registrasi *online* peserta. Proses penarikan kesimpulan ini memiliki maksud untuk memperoleh pengetahuan dan mengevaluasi data yang ada sebagai bahan riset, sehingga dapat menemukan inti pada penelitian yang dilakukan.

Tahap dalam metode ini merupakan tahap penarikan kesimpulan dari semua data yang telah diperoleh sebagai hasil pada penelitian, sehingga merupakan tahap akhir pada kegiatan penelitian di mana proses pada penarikan kesimpulan adalah bagian yang penting dari pelaksanaan kegiatan penelitian.

Pada tahap ini setelah kegiatan penelitian dilakukan, maka selanjutnya adalah kesimpulan terhadap hasil dari analisis data, dan evaluasi tentang data yang telah diperoleh selama penelitian. Di mana kesimpulan pada penelitian ini adalah memberikan layanan keamanan informasi untuk menjaga supaya pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak, ditujukan sebagai ilmu pengetahuan pada teknologi dan informasi tentang implementasi algoritma *advanced encryption standard* dengan algoritma *base64* sebagai seni ilmu kriptografi dalam mengamankan data pada sistem registrasi *online*, yang mana hal ini sendiri masuk pada ranah *cyber security, network security, data security system, dan web security*.