BAB I
PENDAHULUAN

1.1. Latar Belakang

Tiap tiap warga negara berhak dan wajib ikut serta dalam usaha pembelaan negara (Undang-Undang Dasar Negara Republik Indonesia, 1945). Sistem pertahanan negara dalam menghadapi ancaman nonmiliter menempatkan lembaga pemerintah di luar bidang pertahanan sebagai unsur utama (Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, 2002).Tindak pidana pencucian uang tidak hanya mengancam stabilitas perekonomian dan integritas sistem keuangan, tetapi juga dapat membahayakan sendi-sendi kehidupan bermasyarakat, berbangsa, dan bernegara berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. PPATK adalah lembaga independen yang dibentuk dalam rangka mencegah dan memberantas tindak pidana pencucian uang (Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, 2010) dan pendanaan terorisme (Undang-Undang Nomor 9 TAHUN 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme, 2013). Pejabat atau pegawai PPATK, penyidik, penuntut umum, hakim, dan setiap orang yang memperoleh Dokumen atau keterangan dalam rangka pelaksanaan tugasnya menurut Undang-Undang ini wajib merahasiakan Dokumen atau keterangan tersebut (Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, 2010). PPATK sebagai lembaga pemerintah yang menjadi *focal point* rezim APUPPT mengelola dokumen dan sistem secara elekronik. Penyelenggara sistem elektronik harus melindungi kepentingan umum dari berbagai jenis gangguan sebagai akibat penyalagunaan informasi elektronik (Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, 2016).

Pertahanan siber dilakukan secara bertingkat dari lingkup perorangan, kelompok kerja, organisasi sampai dengan skala nasional untuk melindungi berbagai kegiatan dan berbagai sektor dari berbagai jenis ancaman dan gangguan (Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, 2014). Perhatian yang khusus diberikan pada sektor yang mengelola infrastruktur informasi kritis seperti pertahanan keamanan, energi, transportasi, sistem keuangan, dan berbagai layanan publik lainnya (Perpres 82 Tahun 2022 tentang Perlindungan Infrastuktur Informasi Vital, 2022). Pemerintah Republik Indonesia dalam menyelenggarakan roda pemerintahannya memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada masyarakat berdasarkan prinsip efektivitas, keterpaduan, kesinambungan, efisiensi, akuntabilitas, inteoperabilitas dan keamanan (Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, 2018). Pemanfaatan teknologi informasi membutuhkan pengamanan dalam rangka menjaga kerahasiaan, keaslian, keutuhan, kenirsangkalan dan ketersediaan informasi (Perka BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, 2021). Pertahanan siber mengandung unsur kebijakan, kelembagaan, teknologi dan infrastruktur pendukung serta sumber daya manusia. Fokus utama pada penelitian ini pada unsur teknologi terutama yang berkaitan dengan penerapan keamanan dengan menggunakan kriptografi, mengingat penulis sedang menjalankan tugas belajar pada program Rekayasa Pertahanan Siber Universitas Pertahanan.

Informasi Intelijen Keuangan adalah informasi rahasia yang merupakan hasil analisis atau hasil pemeriksaan transaksi keuangan seseorang atau korporasi yang patut diduga merupakan hasil tindak pidana yang ditempatkan pada sistem keuangan di Indonesia. Proses analisis atau pemeriksaan yang dilakukan oleh PPATK selanjutnya disampaikan kepada

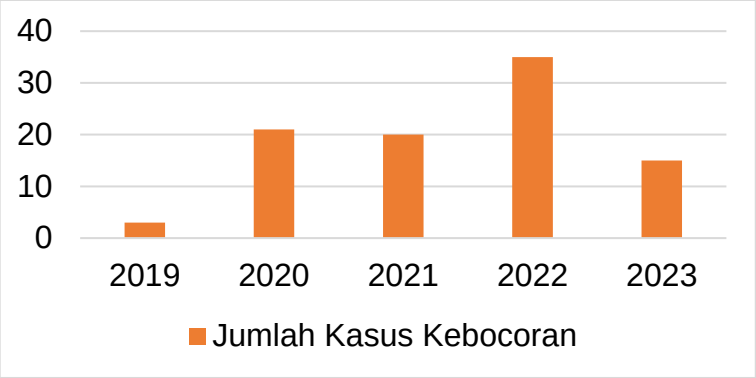
aparat penegak hukum dan pemangku kepentingan lainnya sebagai langkah awal atau informasi intelijen untuk penelurusan lebih lanjut terhadap pemenuhuan unsur-unsur tindak pidana pencucian uang. BIN memiliki wewenang melakukan pemeriksaan aliran dana terhadap Sasaran yang terkait dengan kegiatan yang mengancam kepentingan keamanan nasional meliputi ideologi, politik, ekonomi, sosial, budaya, pertahanan dan keamanan, dan sektor kehidupan masyarakat lainnya dan kegiatan terorisme, separatisme, spionase, dan sabotase yang mengancam keselamatan, keamanan, dan kedaulatan nasional (Undang-Undang Nomor 17 Tahun 2011 Tentang Intelijen Negara, 2011). Pejabat atau pegawai PPATK, penyidik, penuntut umum, hakim, dan setiap orang yang memperoleh Dokumen atau keterangan dalam rangka pelaksanaan tugasnya menurut Undang-Undang ini wajib merahasiakan Dokumen atau keterangan tersebut (Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang, 2010).

PPATK dalam menjalankan proses kerjanya harus mengikuti standard Internasional dari FATF yang berupa rekomendasi 40 + 9 rekomendasi. Dalam rekomendasi tersebut FATF dalam memasukkan negara ke dalam kelompok negara beresiko tinggi dan sanksi ekonomi dan keuangan berupa *black list* seperti negara DPRK dan Iran apabila tidak memenuhi rekomendasi. Indonesia berusaha memenuhi ketentuan internasional FATF yaitu Rekomendasi FATF. Rekomendasi yang ke-33 terkait Statistik menyatakan: *Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation* (International Standards On Combating Money Laundering and The Financing of Terrorism & Proliferation, 2023).

Aplikasi Statistik Pusat Pelaporan Analisis Transaksi Keuangan dikembangkan dengan tujuan utama untuk memenuhi rekomendasi ke-33 FATF yaitu menyediakan data statistik *money laundering* dan pendanaan terorisme yang akurat dan komprehensif. Selain itu dengan adanya aplikasi ini juga diharapkan dapat menjadi salah satu realisasi dari pemenuhan PPATK pada ketentuan Sistem Pemerintahan Berbasis Elekotronik atau SPBE (Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, 2018) dan Satu Data Indonesia (Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia, 2019). Penanganan kejatahan pencucian uang dan pendanaan terorisme melalui proses bertahap pada beberapa instansi pemerintah. Tahap pertama dilakukan oleh PPATK dengan melakukan analisa transaksi keuangan mencurigakan yang disampaikan oleh pihak pelapor dan bisa juga dilakukan oleh penyidik dari hasil tindak lanjut laporan oleh masyarakat maupun kepengembangan kasus yang sedang ditangani. Tahap kedua adalah penyelidikan yang dilakukan oleh Penyidik. Tahap Ketiga adalah Penyidikan yang dilakukan oleh Penyidik. Selanjutnya dilanjutkan tahap keempat yaitu Penuntutan yang dilakukan oleh Kejaksaan atau KPK. Dilanjutkan tahap kelima yaitu putusan pengadilan yang dilakukan oleh Pengadilan dari mulai tingkat pertama hingga Kasasi. Terakhir tahap keenam yang dilakukan oleh Kejasaan yaitu Eksekusi yang dilakukan oleh Kejaksaan. Aplikasi statistik ini tidak hanya berisi data-data agregat yang sifatnya memang umum, tetapi juga berisi data individu yang sangat rahasia termasuk dokumen pendukung dilampirkan dalam aplikasi. Data yang terdapat di dalam *database* aplikasi ini dikategorikan sangat rahasia mengingat tahapan penyelidikan yang diperlukan pengembangan dalam penanganan kasus.

Kebocoran data menjadi ancaman yang nyata pada akhir-akhir ini tidak hanya menimpa sektor swasta, pemerintah bahkan juga menimpa sektor infrastuktur informasi vital. Selama 5 tahun terakhir telah terjadi 94

kasus kebocoran data di Indonesia, yang dapat dirinci seperti pada grafik berikut ini:



Grafik 1.1 Kebocoran Data di Indonesia

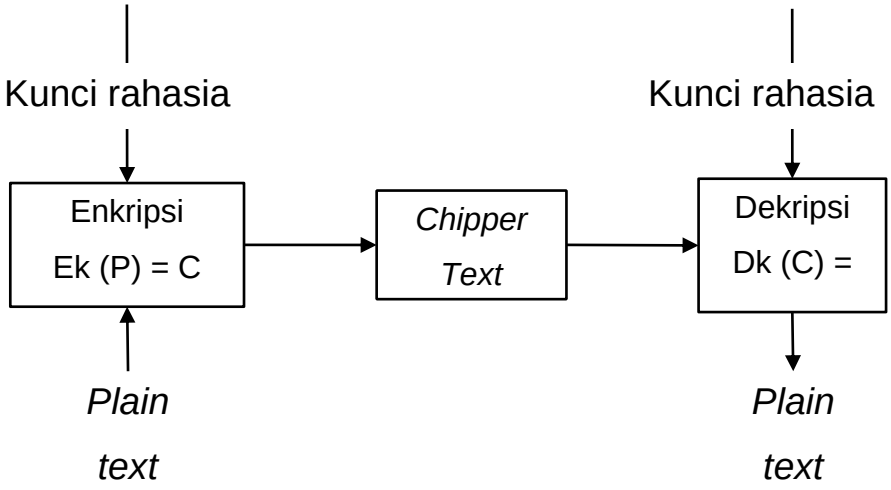
Sumber: Kementrian Komunikasi dan Informatika

Kebocoran data pada sektor swasta terjadi dengan bocornya 19 juta akun data diri konsumen dan 7 juta akun *merchant* Tokopedia (Raihan, 2023). Pada sektor pemerintah kebocoran data BPJS meliputi data NIK, nama, alamat, nomor telepon, dan e-mail dijual di *dark web* (Zaman, Anwar, & Fadlian, 2021) bahkan kerugian negara akibat dari kebocoran data BPJS ini mencapai 600 triliun rupiah (Setiawan & Najicha, 2022). Kemudian kebocoran data pada aplikasi upaya pencegahan dan monitoring penyebaran COVID-19 serta program vaksinasi nasional Peduli Lindungi yang dilansir oleh CNN Indonesia tanggal 4 September 2021 membuat kepercayaan masyarakat terkait aplikasi tersebut menjadi sangat minim (Wijayanto, Daryono, & Nasiroh, 2021). Pencurian dan kebocoran data pada sektor keuangan terjadi pada *bank central* yaitu Bank Indonesia oleh *hacker* Rusia, Conro Ransomware (Kusuma & Rahmani, 2022). Selain pada *bank central* kebocoran data juga terjadi pada Bank Syariah Indonesia (BSI) dengan ukuran mencapai 1,5 TB dengan termasuk didalamnya 15 juta data pengguna dan password (CNN Indonesia, 2023). Kebocoran data paspor juga merupakan insiden yang terjadi menimpa salah satu sektor administrasi pemerintah.

Pada penelitian ini kriptografi digunakan untuk menyamarkan pesan atau data yang terdapat pada *database* sistem aplikasi statistik penanganan

TPPU dan TPPT yang sudah dikembangkan sebelumya tetapi belum menerapkan menerapkan kriptografi pada aplikasinya selain dari autentikasi saja. Oleh karena itu perlu ditambahkan penerapan kriptografi pada database yang sifatnya rahasia untuk melindungi dari ancaman kebocoran data baik dari orang dalam maupun penyusup dari luar. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan menggunakan teknik-teknik matematika yang bertujuan untuk menjaga keamanan informasi seperti kerahasiaan, integritas data, serta autentikasi. Kriptografi sudah ada sejak zaman kuno jauh sebelum abad masehi. Mesir kuno, Cina, India, Romawi, dan Yunani yang sudah lama menggunakan kriptografi untuk menyamarkan pesan dari pihak musuh. Pada penelitian ini kriptografi diterapkan untuk menyamarkan pesan yang ada pada database sistem aplikasi dari ancaman kebocoran data.

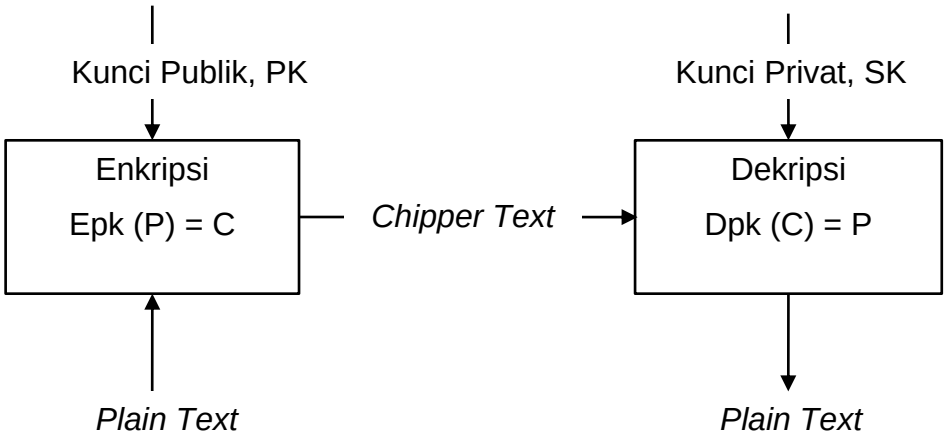
Enkripsi atau *encryption* atau *enciphering* adalah proses menyandikan *plainteks* menjadi *cipherteks* (menurut ISO 7498-2). Sebaliknya dekripsi atau *decryption* atau *deciphering* (menurut ISO 7498-2) adalah proses mengembalikan *cipherteks* menjadi *plainteks* semula. Baik enkripsi maupun dekripsi memerlukan kunci dalam prosesnya. Berdasarkan kuncinya algorima pada kriptografi dibagi menjadi 2 (dua) yaitu kriptografi kunci simetri (*symmetric-key cryptography*) dan algoritma kriptografi kunci nirsimetri (*asymmetric-key cryptography*). Algoritma yang digunakaan untuk melakukan enkripsi database dan file lampiran menggunakan algoritmat AES 256. Sedangkan kriptografi kunci nirsimetri atau kriptografi kunci publik yang akan digunakan adalah algoritma RSA. Untuk memudahkan memahami perbedaan kritografi kunci publik atau nirsimetri dan kriptografi kunci simetri berikut ini gambar perbedaannya. Berikut ini gambar kriptograsi kunci simetri:



Gambar 1.1 Kriptografi Simetris

Sumber:

Dapat dilihat pada Gambar 1.1 diatas bahwa kunci rahasia untuk mengenkripsi dan untuk mendekripsi merupakan kunci yang sama. Berbeda halnya dengan kriptografi kunci asimetri yang digambarkan pada Gambar 1.2 menunjukkan bahwa kunci yang digunakan untuk mengenkripsi dan untuk mendekripsi adalah kunci yang berbeda. Pada kriptografi asimetrik kunci untuk mengenkripsi dinamakan kunci publik yang sifatnya tidak rahasia sedangkan kunci untuk mendekripsi dinamakan kunci privat yang sifatnya rahasia. Kriptografi kunci asimetris dapat digambarkan pada gambar 1.2 berikut:



Gambar 1.2 Kriptografi Nirsimetri

Kriptografi juga akan digunakan untuk mengenkripsi file *attachment* di sistem aplikasi sehingga file tersebut walaupun bisa dibaca tetapi tidak akan mempunyai makna arti apa-apa. Enkripsi file *attachment* ini bertujuan agar file yang disimpan di server tidak dapat diketahui informasi yang terkandung didalamnya oleh pihak pihak yang memang tidak memiliki kewenangan untuk itu misalnya penyerang dari luar maupun orang dalam yang tidak berkepentingan terhadap isi kandungan file tersebut. Pada penelitian yang lain dinyatakan bahwa hasil enkripsi file dengan metode Blowfish dengan kunci 72 bit atau 9 karakter perlu waktu 1,49 x 10^8 tahun untuk membongkarnya dengan kecepatan komputasi 10^6 Kunci tiap detik (Siswo Wardoyo, 2014).

Untuk lebih menguatkan metode enkripsi maka akan digunakan Metode enkripsi *Advanced Encryption Standard* (AES) 256. Dimana metode AES 256 adalah algoritma yang ditawarkan termasuk ke dalam kelompok algoritma kriptografi simetri berbasis *chipher block*. Seluruh rancangan algoritma harus *public* (tidak dirahasiakan) dengan panjang kunci 256 bit. Algoritma dapat diimplementasikan baik sebagai software maupaun hardware. Untuk membongkar enkripsi ini dengan komputer yang paling cepat yang bisa mencoba 1 juta kunci per detik maka perlu waktu 5,4 x 10^{18} tahun untuk mencoba seluruh kemungkinan kunci (Munir, 2019).

1.2. Identifikasi Masalah

Dengan latar belakang yang telah dituliskan sebelumnya penulis mengidentifikasi beberapa permasalahan yang akan diteliti untuk ditemukan pemecahan atas permasalahan tersebut. Adapun beberapa masalah tersebut adalah sebagai berikut :

a. Akhir akhir ini terjadinya kebocoran data pada insfrastuktur informasi vital pemerintah seperti sektor perbankan dan telekomunikasi.
b. Pada saat akan menjalin kerjasama dengan instansi lain sering menjadi pertanyaan tentang jaminaan keamanan data yang akan

dipertukarkan tidak akan bocor kepada pihak lain mengingat data yang dipertukarkan bersifat rahasia.

c. Pada saat terjadi kebocoran data subjek pertama yang ditanya adalah penanggung jawab pengelola teknologi informasi yang memiliki akses ke server aplikasi dan database.
d. Sistem aplikasi dengan database yang dienkripsi dapat menurunkan kecepatan akses yang bisa berdampak pada kurangnya kenyamanan pengguna aplikasi.
e. Metode enkripsi pada database yang lemah dapat dengan mudah ditemukan polanya sehingga dapat ditemukan dengan mudah data yang sebenarnya.
f. File bersifat rahasia yang disimpan di server aplikasi dalam bentuk tidak dienkripsi apabila server diakses oleh peretas maupun pihak internal yang tidak memiliki kewenangan maka dengan mudah file lampiran aplikasi statistik dapat dibaca padahal sejatinya file tersebut sifatnya rahasia.

1.3. Pembatasan Masalah

a. Enkripsi dilakukan pada aspek file dan database saja, enkripsi pada jalur komunikasi diluar pembahasan penelitian ini.
b. Fokus utama penelitian ini pada implementasi kombinasi atau *hybrid cryptography* kunci simetri dan kriptografi kunci publik yaitu menggunakan algoritma enkripsi AES 256 dan RSA.
c. Enkripsi database dilakukan pada level aplikasi yaitu proses enkripsi maupun dekripsi diproses oleh aplikasi berbasis PHP untuk mengenkripsi mapun mendekripsi data pada kolom tertentu di database MySQL.
d. Enkripsi file dokumen dilakukan hanya dalam format dokumen saja yaitu word atau pdf saja, tidak pada jenis file yang lainnya.
e. Pengguna aplikasi pada saat penelitian ini dilakukan masih terbatas pada internal PPATK saja belum digunakan oleh

penegak hukum lain seperti Kepolisian, Kejasaan, KPK, DJBC, DJP jadi belum sampai pada pertukaran data antar instansi.

f. Pengujian kekuatan metode enkripsi seperti analisa frekuensi, kasiski tidak dilakukan pada penelitian ini.

1.4. Rumusan Masalah

Pemerintah perlu melakukan upaya yang ekstra dalam menghadapi ancaman siber yang sedang marak terjadi saat ini. Pertanyaan penelitian dari rumusan masalah meliputi:

a. Bagaimana membuat perimeter untuk mempertahankan kerahasiaan informasi intelijen keuangan pada infrastruktur informasi vital dalam hal ini database mysql aplikasi statistik penanganan kejahatanan TPPU dan TPPT.
b. Bagaimana membuat perimeter untuk mempertahankan kerahasiaan informasi intelijen keuangan pada infrastruktur informasi vital berupa file lampiran yang disimpan pada server aplikasi aplikasi statistik penanganan kejahatanan TPPU dan TPPT.
c. Bagaimana perhitungan metode enkripsi AES dengan panjang kunci lebih panjang 256 bit menjadi lebih rumit dibongkar daripada menggunakan panjang kunci yang 128 bit.
d. Bagaimana cara mengimplementasikan *hybrid* kriptografi simetri dan asimetri pada database dan dokumen rahasia aplikasi statistik penanganan TPPU dan TPPT dari ancaman kebocoran data baik dari internal pengelola teknologi informasi maupun pihak eksternal dengan tidak mengorbankan kenyamanan pengguna aplikasi.
e. Bagaimana caranya untuk membuktikan bahwa metode yang digunakan untuk enkripsi merupakan metode yang sangat kuat sehingga akan sangat sulit dibongkar.

1.5. Tujuan Penelitian

Tujuan penelitian yang ingin dicapai peneliti dengan mempertimbangkan latar belakang, rumusan masalah, dan pertanyaan penelitian adalah sebagai berikut:

a. Memperkuat mekanisme pertahanan siber pada instraktur informasi vital pada sektor administrasi pemerintah yaitu rezim anti pencucian uang dan pendanaan terorisme.
b. Mengimplementasi kombinasi metode enkripsi AES 256 dan RSA pada tabel dan kolom tertentu yang sifatnya rahasia pada sistem aplikasi statistik penanganan perkara tindak pidana pencucian uang dan pendanaan terorisme sebagai upaya memperkuat pertahanan siber.
c. Mengimplementasikan hybrid kriptografi dengan metode enkripsi AES 256 dan RSA pada file lampiran dalam format word atau pdf pada sistem aplikasi yang merupakan dokumen informasi intelijen keuangan yang sangat rahasia.
d. Menguji cobakan hasil implementasi metode enkripsi dan dekripsi pada sistem aplikasi statistik penanganan TPPU dan TPPT.
e. Mengurangi resiko kebocoran data oleh internal pengelola teknologi informasi dalam hal ini Pusat Teknologi Informasi PPATK maupun oleh pihak eksternal yang tidak bertanggung jawab.

1.6. Manfaat Penelitian

Penelitian ini diharapkan memberi manfaat atas implementasi kebijakan para pemangku kepentingan. Penelitian ini diharapkan dapat memberi manfaat baik dari sudut pandang teoritis maupun sudut pandang praktis.

1.6.1 Manfaat Teoritis

Penelitian ini secara teoritis diharapkan dapat memberi manfaat diantaranya adalah sebagai berikut:

a. Dapat mengetahui bagaimana teknik atau cara membangun perimeter pertahanan siber pada bagian paling belakang yaitu database dan file lampiran pada suatu sistem aplikasi.
b. Dapat mengetahui bagaimana cara mengimplementasikan kombinasi atau metode *hybrid* algoritma AES 256 dan RSA pada database sekaligus file attachment pada suatu sistem aplikasi.
c. Dapat mengukur performa aplikasi setelah diimplementasikan enkripsi pada database dan file pada sistem aplikasi statistik penanganan TPPU dan TPPT yang dibangun dengan Bahasa pemrograman PHPdan database MySQL.
d. Dapat menjadi salah satu rujukan teknik pengembangan sistem aplikasi yang aman dari sudut pandang pengamanan database dan pengelolaan file.

1.6.2 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan manfaat level praktis diantaranya sebagai berikut:

a. Mencegah terjadinya kebocoran informasi rahasia yang berasal dari database dan file pada sistem aplikasi statistik penanganan perkara TPPU dan TPPT.
b. Menutup celah kebocoran database dan file rahasia yang dapat dilakukan oleh internal pengelola teknologi informasi PPATK.
c. Mengimplementasikan enkripsi database dan file dengan kondisi performance sistem aplikasi tetap handal.
d. Menjadi role model untuk diimplementasikan pada sistem aplikasi yang lain yang ada di PPATK.
e. Meningkatkan kepercayaan dari sudut pandang teknis untuk menjalin kerjasama pertukaran informasi antar pemangku kepentingan secara elektronik mesin ke mesing dalam hal penanganan TPPU dan TPPT.