PROPOSAL PENELITIAN

ANALISIS PERBANDINGAN EFEKTIVITAS ALGORITMA KRIPTOGRAFI AES, CHACHA20, DAN ECC DALAM MENGAMANKAN DATA SENSITIF PADA APLIKASI BIMA MOBILE

DISUSUN OLEH:

Lulus Dwiyan Mita

24060121120029

DEPARTEMEN ILMU KOMPUTER/ INFORMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

2023

ABSTRAK

Perkembangan Teknologi Informasi dan Komunikasi saat ini telah menunjukkan kemajuan yang cukup pesat. Hampir berbagai macam sektor kehidupan telah mengimplementasikan suatu infrastruktur IT dalam mendukung berbagai macam hal yang menyangkut operasionalitas suatu perusahaan yang tidak terkecuali dalam sektor keuangan dan perbankan. Salah satu hal yang sangat menonjol dari penerapan suatu IT *value* di industri perbankan adalah adanya layanan *mobile banking*. Suatu aplikasi berbasis perangkat *mobile* tersebut telah menawarkan kemudahan yang sangat signifikan bagi pengguna untuk mengakses layanan perbankan yang salah satunya adalah kecepatan proses transaksi yang dapat dilakukan kapanpun dan dimanapun.

Akan tetapi, kemudahan yang ditawarkan oleh aplikasi *mobile banking* tersebut tidak selamanya menjamin akan adanya keamanan yang absolut. Seiring berjalannya waktu perkembangan teknologi yang cepat juga diiringi dengan munculnya kejahatan siber atau *cybercrime* yang semakin beragam. Salah satu bentuk kejahatan siber tersebut adalah pembobolan *mobile banking* yang bisa dilakukan dengan *phishing, malware*, dan lain sebagainya. Oleh karena itu, perlu adanya suatu sistem proteksi data sensitif pengguna yang salah satunya adalah dengan menerapkan algoritma AES, ChaCha20, atau ECC untuk meningkatkan keamanan aplikasi *mobile banking*.

Tujuan dari penelitian ini adalah untuk melakukan analisis yang mendalam mengenai efektivitas kinerja dari berbagai macam algoritma kriptografi seperti AES, ChaCha20, dan ECC untuk meningkatkan keamanan aplikasi *mobile banking.* Hasil penelitian ini berupa performa efektivitas untuk masing-masing algoritma dari ketiga algoritma yang dianalisis yang mana dalam analisis tersebut akan mencakup beberapa parameter seperti kecepatan enkripsi, kompleksitas algoritma, dan ketahanan terhadap serangan. Algoritma dengan efektivitas terbaik berdasarkan hasil analisis tersebut dapat diimplementasikan pada *mobile banking* untuk peningkatan keamanan, ataupun dilakukan penelitian lanjutan untuk memperoleh algoritma yang lebih baik lagi.

Kata kunci: *Kriptografi, AES, ChaCha20, ECC, Mobile Banking.*

ABSTRACT

The current development of Information and Communication Technology has shown quite rapid progress. Almost various sectors of life have implemented an IT infrastructure to support various things related to the operations of a company, including the financial and banking sectors. One thing that really stands out from the application of IT value in the banking industry is the existence of mobile banking services. This mobile device-based application has offered very significant convenience for users to access banking services, one of which is the speed of the transaction process which can be carried out anytime and anywhere.

However, the convenience offered by the mobile banking application does not always guarantee absolute security. As time goes by, rapid technological developments are also accompanied by the emergence of increasingly diverse cybercrimes. One form of cybercrime is mobile banking hacking which can be done with phishing, malware, and so on. Therefore, it is necessary to have a sensitive user data protection system, one of which is by implementing the AES, ChaCha20, or ECC algorithms to increase the security of mobile banking applications.

The aim of this research is to conduct an in-depth analysis of the effectiveness of the performance of various cryptography algorithms such as AES, ChaCha20, and ECC to improve the security of mobile banking applications. The results of this research are the effectiveness performance for each algorithm of the three algorithms analyzed, which in the analysis will include several parameters such as encryption speed, algorithm complexity, and resistance to attacks. The algorithm with the best effectiveness based on the results of this analysis can be implemented in mobile banking to increase security, or further research can be carried out to obtain an even better algorithm.

Keywords: *Cryptography, AES, ChaCha20, ECC, Mobile Banking.*

DAFTAR ISI

ABSTRAK I
ABSTRACT II
DAFTAR ISI III
DAFTAR GAMBAR IV
DAFTAR TABEL V
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan dan Manfaat 2
1.4 Ruang Lingkup 3
BAB II LANDASAN TEORI 4
2.1 State of the Art 4
2.2 Dasar Teori 4
BAB III METODOLOGI PENELITIAN 7
3.2 Eksperimen dan Pengujian 8
3.3 Analisis Perbandingan Algoritma 8
3.4 Evaluasi dan Validasi Hasil 8
BAB IV RENCANA JADWAL PENELITIAN 9
DAFTAR PUSTAKA 10
LAMPIRAN 1 - PROBLEM TREE 11

DAFTAR GAMBAR

Gambar 5.1 Problem Tree 11

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu Tentang Algoritma Kriptografi 4
Tabel 4.1 Jadwal Penelitian 9

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perbankan adalah salah satu sektor yang cukup penting bagi perekonomian suatu negara. Pengertian bank sendiri menurut Undang-Undang RI nomor 10 tahun 1998 tentang perbankan, bank merupakan perusahaan yang menghimpun dana masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk pinjaman dan bentuk lainnya guna meningkatkan taraf hidup orang banyak. Perbankan melibatkan organisasi, aktivitas bisnis, dan metode serta proses dalam menjalankan aktivitas bisnis. Oleh karena itu, sektor perbankan merupakan sektor yang cukup luas dan kompleks serta memiliki pengaruh yang besar dalam menunjang perekonomian utamanya dalam hal peningkatan kesejahteraan hidup bagi banyak orang.

Seiring berjalannya waktu, perkembangan teknologi yang ada bergerak semakin cepat dan dinamis. Hal ini memunculkan berbagai macam inovasi dalam bidang teknologi yang mengarah pada digitalisisasi di berbagai sektor kehidupan, tidak terkecuali dalam sektor perbankan. Pada masa sekarang banyak bank telah melakukan inovasi dan juga telah melakukan digitalisasi yang cukup masif. Hal ini terlihat dari banyaknya produk perbankan berbasis IT seperti misalnya *Internet Banking* maupun *Mobile Banking*. *Mobile Banking* merupakan layanan elektronik produk keuangan yang dikeluarkan oleh pihak bank untuk menyalurkan produk keuangannya ke nasabah dengan memberikan kemudahan akses, *update* informasi yang cepat, dan transaksi keuangan yang terjadi secara real-time melalui suatu telepon seluler berteknologi GPRS (Nurdin dkk., 2020). Menurut Badan Pusat Statistik pengguna *smartphone* dari tahun ke tahun telah mengalami peningkatan secara kontinu, hal ini terlihat pada tahun 2022 sebanyak 67.88% orang Indonesia telah memiliki ponsel, meningkat sekitar 2.01% jika dibandingkan pada periode yang sama di tahun sebelumya. Peningkatan pengguna ponsel di Indonesia memiliki korelasi positif dengan peningkatan pengguna *mobile banking.* Hal ini didukung oleh adanya fakta berupa laporan Otoritas Jasa Keuangan pada tahun 2020 yang menyatakan jumlah pengguna *e-banking* yang meliputi *mobile banking* di Indonesia meningkat 270% selama dalam jangka waktu empat tahun.

Kemudahan yang ditawarkan oleh aplikasi *mobile banking* mampu menarik minat

banyak orang untuk tertarik menggunakannya. Hal ini tentu bukan tanpa alasan, *mobile banking* mampu meningkatkan efisiensi dan kecepatan serta kemudahan dalam proses transaksi yang menjadi kebutuhan mendesak bagi banyak orang di era sekarang. Namun kenyamanan yang ditawarkan oleh aplikasi mobile banking bukanlah suatu kenyamanan yang mutlak, terdapat juga faktor keamanan yang perlu menjadi perhatian bagi banyak pihak. Semakin canggihnya perkembangan teknologi juga diiringi dengan semakin beragamnya modus serangan siber yang dilakukan oleh *hacker* karena sebenarnya tidak ada suatu sistem yang 100% bisa dikatakan aman, dan pasti terdapat suatu celah yang memungkinkan *hacker* untuk dapat masuk dan melakukan berbagai tindak kejahatan. Berdasarkan data dari *Checkpoint Research* pada tahun 2022, sektor perbankan setiap pekannya mendapatkan 1131 kali serangan siber yang beberapa diantaranya juga menargetkan pencurian data sensitif yang dimiliki oleh nasabah.

Dari berbagai macam problematika tersebut, maka diperlukan suatu solusi yang akan menjadi suatu langkah konkret dalam mengatasi persoalan tersebut, yang salah satunya adalah dengan menerapkan algoritma kriptografi untuk melindungi data sensitif nasabah. Algoritma kriptografi mampu memberikan kontribusi positif dalam hal peningkatan keamanan sistem sehingga mencegah *hacker* untuk mencuri ataupun memodifikasi data sensitif yang dimiliki oleh nasabah. Beberapa algoritma kriptografi yang populer adalah *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA) yang mana algoritma AES memiliki performa efektivitas yang jauh lebih baik berdasarkan penelitian terdahulu (Hakiki dkk., 2019). Fokus penelitian ini adalah analisis perbandingan efektivitas dari tiga algoritma yang akan diuji yaitu AES, ChaCha20 dan ECC untuk mengetahui algoritma dengan efektivitas terbaik yang dapat diterapkan pada aplikasi Bima Mobile.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, rumusan masalah yang akan dibahas dalam penelitian ini adalah bagaimana perbandingan efektivitas dari masing-masing algoritma kriptografi yang mencakup AES, ChaCha20, dan ECC untuk mengamankan data sensitif pada aplikasi Bima Mobile.

1.3 Tujuan dan Manfaat

Tujuan dari dilaksanakannya penelitian ini adalah untuk mengetahui performa efektivitas dari berbagai algoritma kriptografi yang dibandingkan satu sama lain yaitu

AES, ChaCha20, dan ECC pada data sensitif aplikasi *mobile banking* Bank BPD Jawa Tengah yaitu Bima Mobile sehingga didapatkan algoritma dengan efektivitas terbaik dari ketiga algoritma yang dianalisis.

Sementara itu, manfaat yang diharapkan dari adanya penelitian ini adalah adanya peningkatan dalam hal keamanan data sensitif pada aplikasi Bima Mobile untuk mencegah resiko pembobolan yang diakibatkan oleh suatu kejahatan siber sehingga dapat meningkatkan kepuasan dan loyalitas nasabah Bank BPD Jawa Tengah.

1.4 Ruang Lingkup

Adapun ruang lingkup yang akan dibahas dalam penelitian Analisis Perbandingan Efektivitas Algoritma Kriptografi AES, ChaCha20, dan ECC dalam Mengamankan Data Sensitif Aplikasi Bima Mobile adalah sebagai berikut:

1.4.1 Data yang akan digunakan dalam penelitian ini adalah data *dummy atau* sintetis yang representatif terhadap karakteristik umum data nasabah Bank BPD Jawa Tengah yang menggunakan aplikasi Bima Mobile.

1.4.2 Algoritma kriptografi yang digunakan dalam penelitian ini adalah AES, ChaCha20, dan ECC yang akan dianalisis dan dilakukan perbandingan efektivitasnya.

1.4.3 Penentuan algoritma dengan efektivitas terbaik dalam penelitian ini didasarkan pada 3 indikator utama yaitu kecepatan enkripsi, kompleksitas algoritma, dan ketahanan terhadap serangan siber.

BAB II
LANDASAN TEORI

2.1 State of the Art

Beberapa penelitian terdahulu telah membahas perbandingan algoritma kriptografi untuk peningkatan sistem keamanan suatu data atau informasi. Informasi lengkapnya tertera dalam tabel 2.1.

Tabel 2.1 Penelitian Terdahulu Tentang Algoritma Kriptografi

Peneliti	Judul Penelitian	Algoritma	Hasil
Murowe, H., Akbar, L.A.S.I., & Misbahuddin, M (2019)	Perbandingan Kinerja Algoritma Kriptografi RSA dan AES untuk Keamanan Informasi Perangkat Komunikasi Zigbee	Algoritma RSA dan AES	Hasil penelitian ini menunjukkan bahwa algoritma AES memiliki waktu komputasi lebih cepat dan penggunaan resource memori yang lebih sedikit dibandingkan algoritma RSA.

2.2 Dasar Teori

2.2.1 Mobile Banking

Menurut Almaiah et al. 2023, Mobile banking adalah suatu jenis layanan keuangan yang memungkinkan nasabah perbankan dapat menggunakan rekening untuk melakukan suatu transaksi tertentu melalui perangkat seluler yang dimilikinya. Mobile banking telah menjadi layanan yang sangat populer dalam bidang perbankan yang mana banyak orang tertarik untuk menggunakan layanan tersebut dikarenakan fleksibilitas dan kenyamanan yang ditawarkan. Aplikasi *mobile banking* telah memungkinkan pengguna untuk melakukan transaksi apapun, kapanpun, dan dimanapun yang merupakan kebutuhan yang harus dipenuhi bagi masyarakat modern seperti saat ini. *Mobile banking* memiliki potensi besar untuk terus berkembang terutama dalam mewujudkan visi perbankan untuk melakukan ekspansi layanan seluas

mungkin terutama di daerah yang mana infrastruktur perbankan masih sangat terbatas. Manfaat dari adanya mobile banking cukup banyak mulai dari kecepatan dan kenyamanan dalam transaksi, akses diskon dan *reward* yang banyak, kemampuan untuk melacak transaksi keauangan, kelola keuangan yang lebih baik, dan mendukung berbagai aktivitas bisnis dengan lebih aman.

2.2.2 Kriptografi

Kriptografi berkaitan dengan perlindungan informasi dan komunikasi yang ditransfer melalui saluran komunikasi publik untuk mencegah pihak tertentu mencuri atau merusak informasi tersebut yang berpotensi memberikan kerugian besar (Nitaj, Abderrahmane & Rachidi Tajjeddine, 2023).

2.2.3 Algoritma AES

AES adalah algoritma enkripsi yang aman dan fleksibel yang bekerja pada blok data tetap dan didukung oleh NIST. AES memiliki tiga ukuran kunci: 128-bit, 192-bit, dan 256-bit. Algoritmanya melibatkan transformasi seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey dalam beberapa putaran sesuai dengan ukuran kunci (Li Ke,2023). SubBytes mengganti byte blok dengan tabel substitusi. ShiftRows menggeser byte dalam setiap baris blok. MixColumns bekerja pada kolom blok dengan menggunakan matriks. AddRoundKey melakukan XOR blok dengan kunci putaran yang berasal dari kunci utama. Jadwal kunci memperluas kunci utama menjadi kunci putaran untuk setiap putaran algoritma. Keamanan AES bergantung pada ukuran kunci dan jumlah putaran. Semakin besar kunci dan putaran, semakin aman enkripsinya. AES telah diadopsi luas karena keamanan, efisiensi, dan fleksibilitasnya dalam mendukung berbagai ukuran kunci. Implementasinya bervariasi di berbagai platform untuk memenuhi kebutuhan aplikasi seperti perangkat nirkabel dan sistem tertanam.

2.2.4 Algoritma ChaCha20

Algoritma ChaCha20 adalah algoritma aliran sandi yang dirancang untuk enkripsi berkecepatan tinggi dan dikenal karena efisiensi dan keamanannya. Algoritma ini merupakan varian dari algoritma Salsa20 dan menggunakan varian 20 putaran dari fungsi quarter-round, yang dirancang untuk memberikan ketahanan yang kuat terhadap serangan kriptografis yang diketahui. Perbedaan utama antara ChaCha20 dan algoritma blok lainnya adalah penggunaannya terhadap algoritma penjadwalan kunci yang berbeda, yang berkontribusi pada efisiensi dan keamanannya. ChaCha20 dirancang untuk lebih aman dan efisien dibandingkan dengan algoritma blok yang sudah ada seperti AES. Ini menawarkan beberapa keunggulan dibandingkan dengan algoritma blok yang lebih lama, seperti kemampuan untuk

menggunakan enkripsi berbasis nonce, yang memungkinkan penggunaan kunci enkripsi yang lebih aman dan unik untuk setiap sesi, meningkatkan keamanan dengan membuatnya lebih sulit bagi penyerang untuk menebak kunci enkripsi. Selain itu, ChaCha20 mendukung berbagai mode operasi yang berbeda, memungkinkannya digunakan dalam berbagai aplikasi. Kecepatan yang lebih tinggi adalah salah satu keuntungan utama dari algoritma ini, karena dapat mengenkripsi dan mendekripsi data hingga empat kali lebih cepat daripada AES. Selain itu, ChaCha20 lebih aman daripada AES karena jumlah putaran yang lebih besar dan putaran yang lebih kompleks, yang memberikan keamanan yang lebih baik terhadap potensi serangan. Dalam konteks kriptanalisis diferensial, versi perluasan ChaCha20, yang dikenal sebagai Extended ChaCha20 (EChaCha20), telah diusulkan untuk memberikan ketahanan yang lebih kuat terhadap serangan kriptografis yang diketahui, seperti diferensial dan kriptanalisis linear, sehingga meningkatkan kerahasiaan, integritas, dan otentikasi data sensitif. Versi perluasan ini menggunakan lebih banyak putaran dari fungsi quarter-round untuk keamanan yang lebih baik dan telah diuji terhadap serangan kriptanalisis diferensial untuk mengevaluasi keamanannya.

2.2.5 Algoritma ECC

Algoritma Elliptic Curve Cryptography (ECC) menggunakan sifat matematika dari kurva eliptik untuk mengamankan data dengan efisiensi tinggi. Operasi matematika dilakukan pada titik-titik di atas kurva eliptik di medan bilangan tertentu. ECC menyediakan tingkat keamanan setara dengan RSA, namun dengan kunci yang lebih pendek, menghasilkan efisiensi sumber daya komputasi. Keamanan ECC bergantung pada kesulitan permasalahan matematika, seperti masalah logaritma diskret pada kurva eliptik. Algoritma ini banyak digunakan dalam protokol keamanan internet dan aplikasi yang memerlukan pertukaran kunci aman serta enkripsi data.

BAB III

METODOLOGI PENELITIAN

3.1 Pengumpulan Data

Pengumpulan data memiliki peran yang cukup krusial dalam penelitian. Terdapat berbagai metode yang akan dilakukan berkaitan dengan pengumpulan data yang beberapa diantaranya adalah:

3.1.1 Studi Literatur

Studi literatur dalam hal ini berkaitan dengan eksplorasi yang melibatkan pencarian dan pengumpulan data yang dibutuhkan dalam penelitian, biasanya berkaitan dengan penelitian terdahulu. Selain itu, dalam studi literatur ini akan dilakukan juga pengkajian terhadap pengetahuan yang ada, landasan teoritis, metodologi, dan hasil dari penelitian terdahulu yang mungkin masih memiliki celah atau kekurangan. Studi literatur berperan penting dalam kesuksesan penelitian yang terkait dengan penerapan algoritma kriptografi pada aplikasi mobile banking untuk keamanan data sensitif nasabah.

3.1.2 Wawancara (*Interviews*)

Wawancara akan dilakukan dengan melibatkan berbagai pihak terkait seperti *engineer* aplikasi *mobile*, *security engineer,* operator *database,* nasabah, pegawai perbankan, dan direktur bank. Kegiatan tersebut bertujuan untuk mendapatkan data maupun informasi penting yang menunjang penelitian agar dapat berjalan lancar dengan melibatkan kerja sama dari berbagai pihak.

3.1.3 Kuesioner

Kegiatan ini dilakukan dengan menyebarkan suatu formulir yang berisi pertanyaan tertulis ke responden yang dalam hal ini adalah nasabah, untuk mendapatkan saran maupun untuk mengetahui lebih dalam mengenai perspektif pengguna aplikasi terhadap keamanan data.

3.1.4 Observasi

Observasi akan dilakukan terhadap sistem terutama yang berkaitan dengan masuk dan keluarnya data ke atau dari database, respon aplikasi terhadap kesalahan pengguna, kecepatan akses aplikasi, dan fitur keamanan aplikasi yang dapat menjadi acuan atau pertimbangan dalam implementasi algoritma kriptografi ini.

3.2 Eksperimen dan Pengujian

Pada tahap eksperimen ini akan dilakukan persiapan data uji yang telah didapatkan dari tahap sebelumnya yaitu pengumpulan data. Data yang digunakan dalam penelitian ini adalah data sintetis yang dapat menjelasakan karakteristik umum dari data nasabah, hal ini penting untuk tetap memastikan bahwa penelitian yang dilakukan mematuhi prinsip privasi dan etika penelitian serta kepatuhan terhadap undang-undang perlindungan data. Langkah berikutnya adalah pengimplementasian dari masing-masing algoritma AES, ChaCha20, dan ECC pada aplikasi Bima Mobile yang kemudian dilanjutkan dengan uji peretasan yang mencakup beberapa hal seperti uji enkripsi dekripsi, analisis kerentanan, dan pengecekan respon terhadap serangan.

3.3 Analisis Perbandingan Algoritma

Setelah eksperimen dan pengujian algoritma selesai dilakukan, langkah berikutnya adalah melakukan analisis eksperimen dan perbandingan algoritma untuk mengetahui efektivitas dari tiap algoritma yang dalam hal ini akan dilakukan pengukuran kinerja algoritma dan pengaruhnya terhadap aplikasi serta mengidentifikasi kelebihan dan kekurangan tiap algoritma. Setelah itu, menentukan algoritma terbaik dari 3 algoritma yang dianalisis dengan berdasar pada 3 indikator utama yaitu kecepatan enkripsi, kompleksitas algoritma, dan ketahanan terhadap serangan siber.

3.4 Evaluasi dan Validasi Hasil

Setelah ditemukan algoritma dengan performa efektivitas terbaik, maka algoritma tersebut dapat dipilih untuk diimplementasikan dalam aplikasi Bima Mobile sebagai sistem proteksi keamanan data sensitif nasabah. Setelah algoritma terimplementasikan, maka evaluasi akan dilakukan berdasarkan *feedback* pengguna, dan dimungkinkan juga untuk dilakukan penelitian lanjutan dengan algoritma lain kedepannya untuk mendapatkan algoritma dengan performa yang lebih baik.

BAB IV

RENCANA JADWAL PENELITIAN

Penelitian akan dilaksanakan dalam jangka waktu empat bulan sebagaimana yang dijabarkan pada Tabel 4.1.

Tabel 4.1 Jadwal Penelitian

Kegiatan	Bulan															
	1				2				3				4			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Studi Literatur																
Wawancara																
Kuesioner																
Observasi																
Eksperimen																
Analisis Perbandingan Algoritma																
Evaluasi dan Validasi Hasil																

DAFTAR PUSTAKA

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the Role of Perceived Risk, Perceived Security and Perceived Trust on Smart m-Banking Application Using SEM. *Sustainability (Switzerland)*, *15*(13). https://doi.org/10.3390/su15139908

Ghaz, A., Nouioua, N., & Seddiki, A. (2023). Enhancing Biometric Fingerprint Security Through Integrated Watermarking and Cipher Block Chaining Techniques. *Traitement Du Signal*, *40*(3), 981–983. https://doi.org/10.18280/ts.400314

Hakiki, M., Syamsul, L. A., Akbar, I., & Misbahuddin, M. (2019). *PERBANDINGAN KINERJA ALGORITMA KRIPTOGRAFI RSA DAN AES UNTUK KEAMANAN INFORMASI PERANGKAT KOMUNIKASI ZIGBEE*.

Kebande, V. R. (2023). Extended-Chacha20 Stream Cipher with Enhanced Quarter Round Function. https://doi.org/10.1109/ACCESS.2017.DOI

Li, K., Li, H., & Mund, G. (2023). A reconfigurable and compact subpipelined architecture for AES encryption and decryption. *Eurasip Journal on Advances in Signal Processing*, *2023*(1). https://doi.org/10.1186/s13634-022-00963-3

Lima, P. M., da Silva, C. K. P., de Farias, C. M., Carvalho, L. K., & Moreira, M. V. (2022). Event-based cryptography for automation networks of cyber-physical systems using the stream cipher ChaCha20. *IFAC-PapersOnLine*, *55*(28), 58–65. https://doi.org/10.1016/j.ifacol.2022.10.324

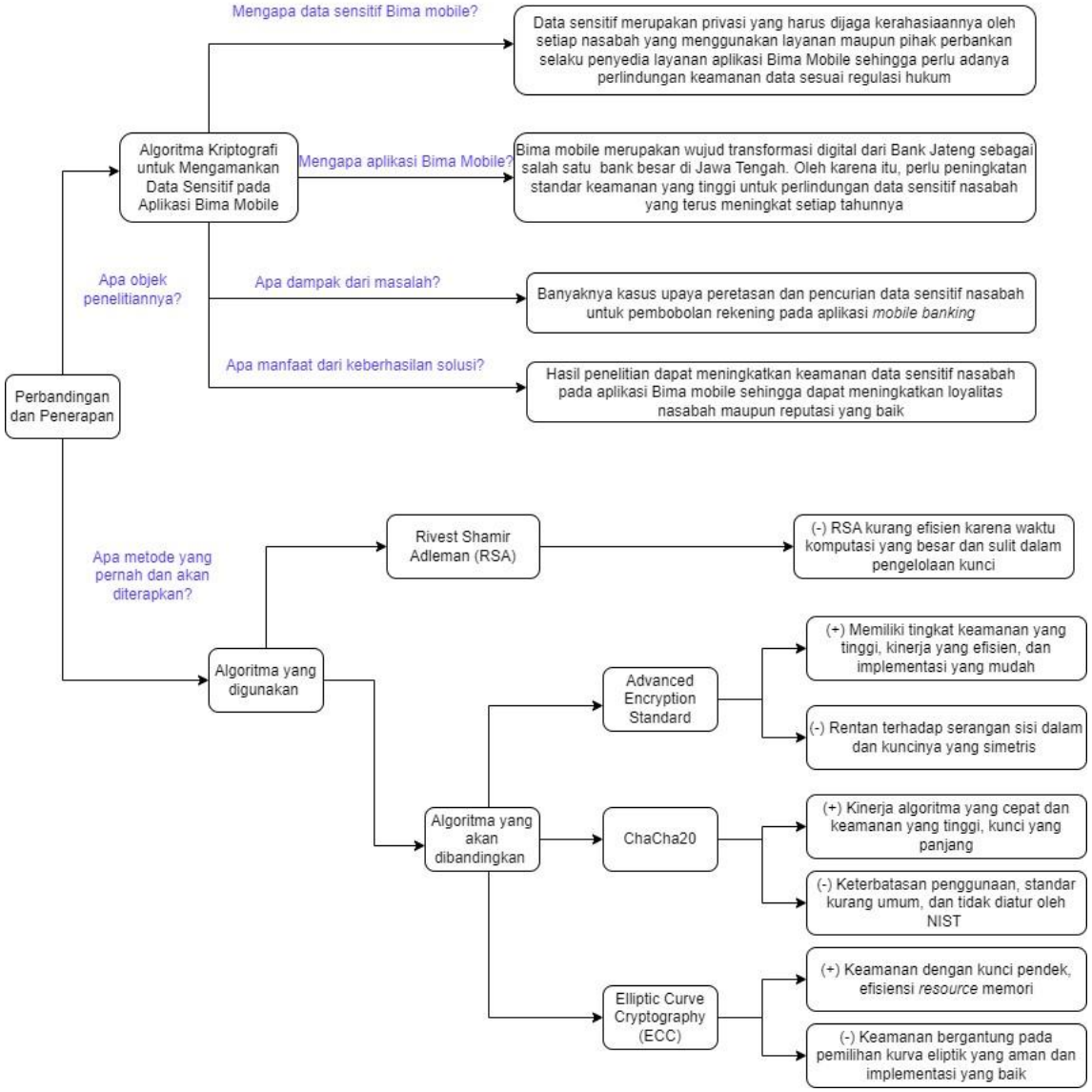
Natanael, D., Faisal, & Suryani, D. (2018). Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC). *Procedia Computer Science*, *135*, 283–291. https://doi.org/10.1016/j.procs.2018.08.176

Nitaj, A., & Rachidi, T. (2023). Applications of Neural Network-Based AI in Cryptography. *Cryptography*, *7*(3). https://doi.org/10.3390/cryptography7030039

Nurdin, N., Musyawarah, I., Nurfitriani, N., Jalil, A., Syariah, J. P., Ekonomi, F., Islam, B., & Palu, I. (2020). Pengaruh Pelayanan Mobile Banking Terhadap Kepuasan Nasabah (Studi Pada Mahasiswa Perbankan Syariah IAIN Palu). *Jurnal Ilmu Perbankan Dan Keuangan Syariah*, *2*(1). https://doi.org/10.24239/jsi.v1

Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. *Alexandria Engineering Journal*, *84*, 275–284. https://doi.org/10.1016/j.aej.2023.10.054

LAMPIRAN 1 - PROBLEM TREE



Gambar 5.1 Problem Tree