# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang

Pesatnya perkembangan teknologi informasi telah mendorong transformasi besar dalam sektor perbankan, salah satunya melalui layanan *mobile banking*. Layanan ini memungkinkan nasabah melakukan berbagai transaksi keuangan kapan saja dan di mana saja melalui perangkat seluler tanpa harus mengunjungi kantor cabang. Berdasarkan data Bank Indonesia, volume transaksi *mobile banking* di Indonesia sepanjang tahun 2024 diproyeksikan mencapai 20,56 miliar transaksi dengan nilai sekitar Rp24.486,8 triliun, meningkat sebesar 47% dibandingkan tahun sebelumnya (Kontan, 2024). Peningkatan tersebut menunjukkan bahwa *mobile banking* telah menjadi salah satu sarana utama masyarakat dalam melakukan transaksi keuangan digital.

Seiring dengan meningkatnya penggunaan layanan perbankan digital, risiko terhadap keamanan informasi juga semakin meningkat. Data transaksi yang dikirimkan melalui jaringan internet berpotensi menjadi sasaran berbagai serangan siber yang bertujuan memperoleh, memodifikasi, maupun menyalahgunakan informasi pengguna. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), tercatat sebanyak 102,95 juta anomali trafik serangan siber di Indonesia selama periode Januari hingga Juli 2024 (Fortune Indonesia, 2024). Tingginya aktivitas serangan tersebut menunjukkan bahwa keamanan data dan komunikasi digital masih menjadi tantangan yang perlu mendapatkan perhatian serius.

Dampak serangan siber tidak hanya mengancam kerahasiaan informasi, tetapi juga berpotensi menimbulkan kerugian finansial yang signifikan. Otoritas Jasa Keuangan (OJK) melaporkan bahwa hingga Februari 2025, kerugian masyarakat akibat aktivitas

penipuan transaksi keuangan telah mencapai sekitar Rp700,2 miliar (detikFinance, 2025). Besarnya nilai kerugian tersebut menunjukkan bahwa keamanan transaksi digital merupakan aspek yang sangat penting untuk diperhatikan, terutama pada layanan *mobile banking* yang melibatkan pertukaran data dan informasi keuangan secara daring.

Ancaman terhadap keamanan transaksi digital yang terjadi seperti serangan *Man-in-the-Middle* (MITM). Pada serangan ini, penyerang menempatkan dirinya di antara pihak pengirim dan penerima untuk menyadap, memodifikasi, atau memalsukan data yang ditransmisikan tanpa diketahui oleh kedua belah pihak. Dalam konteks *mobile banking*, serangan MITM dapat menyebabkan perubahan informasi transaksi, seperti nominal transfer, rekening tujuan, maupun identitas pengirim. Akibatnya, integritas dan keaslian data transaksi dapat terganggu sehingga berpotensi menimbulkan kerugian finansial serta menurunkan kepercayaan pengguna terhadap layanan perbankan digital.

Untuk mencegah terjadinya manipulasi data selama proses komunikasi, integritas dan keaslian data menjadi aspek yang sangat penting. Integritas data memastikan bahwa informasi transaksi tidak mengalami perubahan selama proses pengiriman maupun penyimpanan, sedangkan keaslian data memastikan bahwa informasi tersebut benar-benar berasal dari pihak yang berwenang dan bukan hasil pemalsuan oleh pihak lain. Tanpa adanya jaminan terhadap kedua aspek tersebut, transaksi yang diterima sistem tidak dapat dipastikan validitas maupun sumber asalnya.

Untuk melindungi data dari berbagai ancaman keamanan tersebut, diperlukan mekanisme pengamanan yang mampu menjaga kerahasiaan, integritas, dan keaslian informasi. Salah satu teknologi yang digunakan untuk tujuan tersebut adalah kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik pengamanan informasi melalui proses enkripsi, autentikasi, dan verifikasi data. Dalam perkembangannya, kriptografi modern menyediakan berbagai algoritma yang mampu menjaga kerahasiaan, integritas, keaslian, serta *non-repudiation* data pada sistem komunikasi digital (Bader et al., 2020).

Dalam kriptografi modern, seperti AES (*Advanced Encryption Standard*) merupakan algoritma simetris yang banyak digunakan untuk menjaga kerahasiaan data karena memiliki tingkat keamanan yang tinggi serta efisiensi komputasi yang baik. Namun, AES hanya berfungsi untuk menjaga kerahasiaan data dan tidak secara langsung menyediakan mekanisme untuk menjamin integritas maupun keaslian data. Oleh karena itu, diperlukan kombinasi dengan algoritma lain yang mampu melakukan proses autentikasi dan verifikasi data.

Algoritma yang dapat digunakan untuk tujuan tersebut adalah RSA (*Rivest-Shamir-Adleman*) dan HMAC (*Hash-based Message Authentication Code*). RSA merupakan algoritma kriptografi asimetris yang dapat digunakan untuk menghasilkan tanda tangan digital sehingga mampu menjamin keaslian, integritas, serta *non-repudiation* data. Dan juga HMAC yang memanfaatkan fungsi hash dan kunci rahasia bersama untuk menghasilkan kode autentikasi pesan.

Penelitian yang dilakukan oleh Gagan Akhmad Fauzi (Fauzi, 2025) menunjukkan bahwa kombinasi AES dan HMAC mampu menjaga integritas dan keaslian data secara efektif dengan performa yang baik. Penelitian lain menunjukkan bahwa kombinasi AES dan RSA mampu memberikan tingkat keamanan yang tinggi melalui mekanisme tanda tangan digital dan distribusi kunci yang lebih aman. Meskipun demikian, penelitian yang secara khusus membandingkan kombinasi AES-RSA dan AES-HMAC dalam menjamin integritas dan keaslian data pada transaksi *mobile banking* masih relatif terbatas.

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk membandingkan kombinasi algoritma AES-RSA dan AES-HMAC dalam menjamin keaslian dan integritas data pada transaksi *mobile banking*. Perbandingan dilakukan berdasarkan kemampuan kedua metode dalam menjaga keamanan data serta kinerja komputasi yang dihasilkan sehingga dapat diperoleh metode yang lebih optimal untuk diterapkan pada sistem transaksi digital.

## 1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah:

1. Bagaimana algoritma AES dan RSA dalam menjamin keaslian dan integritas data transaksi pada aplikasi *mobile banking*?
2. Bagaimana algoritma AES dan HMAC dalam menjamin keaslian dan integritas data transaksi pada aplikasi *mobile banking*?
3. Metode kriptografi mana yang lebih optimal dalam konteks transaksi finansial dasar pada aplikasi *mobile banking*?.

## 1.3 Batasan Masalah

Untuk memperjelas ruang lingkup penelitian dan menjaga fokus analisis, penelitian ini dibatasi oleh beberapa hal sebagai berikut :

1. Penelitian ini hanya membahas transaksi finansial dasar pada aplikasi *mobile banking*, seperti *transfer* dana dan pembayaran tagihan. Transaksi lain yang lebih kompleks, seperti transaksi investasi atau produk keuangan turunan, tidak dibahas dalam penelitian ini. Hal ini dikarenakan transaksi dasar seperti *transfer* dan pembayaran merupakan jenis transaksi yang paling sering digunakan oleh pengguna *mobile banking*, sehingga lebih relevan untuk menjadi fokus kajian. Selain itu, transaksi kompleks biasanya memiliki alur bisnis dan persyaratan keamanan tambahan yang dapat memperluas ruang lingkup penelitian secara berlebihan.
2. Metode kriptografi yang dianalisis dalam penelitian ini dibatasi pada dua kombinasi, yaitu AES dan RSA, AES dan HMAC. Algoritma kriptografi lain di luar kombinasi tersebut tidak dibahas lebih lanjut. Kedua kombinasi tersebut dipilih karena mewakili skema yang umum digunakan dalam praktik, yaitu kombinasi kriptografi (AES dan RSA) serta kombinasi kriptografi (AES dan HMAC). Dengan membatasi pada dua kombinasi ini, analisis dapat dilakukan secara lebih mendalam tanpa menyebar ke terlalu banyak variasi algoritma.

3. Aspek keamanan yang dianalisis dalam penelitian ini dibatasi pada integritas dan keaslian data. Aspek keamanan lain, seperti kerahasiaan (*confidentiality*) dan non-penyangkalan (*non-repudiation*), tidak dibahas secara mendalam. Pembatasan ini dilakukan karena integritas dan keaslian data merupakan dua aspek yang sangat penting dalam konteks transaksi *mobile banking*, karena berkaitan langsung dengan jaminan bahwa data transaksi tidak dimodifikasi secara tidak sah dan benar-benar berasal dari pihak yang berwenang. Pembatasan ini memungkinkan penelitian untuk fokus pada bagaimana kombinasi algoritma AES dan RSA, AES dan HMAC dapat menjaga kedua aspek tersebut secara lebih rinci.

## 1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menganalisis kombinasi Algoritma AES dan RSA dalam menjamin keaslian dan integritas data transaksi pada aplikasi *mobile banking*.
2. Menganalisis kombinasi Algoritma AES dan HMAC dalam menjamin keaslian dan integritas data transaksi pada aplikasi *mobile banking*.
3. Menganalisis cara kerja AES dan RSA dengan AES dan HMAC dalam konteks transaksi finansial dasar pada aplikasi *mobile banking*.

## 1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah: **1.4 Manfaat Penelitian**
Manfaat yang diharapkan dapat diperoleh dari hasil penelitian ini adalah sebagai berikut:

1. Bagi Pengembang Aplikasi (*Developers*), sebagai referensi kuantitatif dalam mengoptimalkan arsitektur keamanan sistem *mobile banking*.
2. Bagi Peningkatan Keamanan Sistem Transaksi, memberikan kontribusi berupa pemodelan sistem pengamanan data yang berlapis (*defense-in-depth*) melalui pembuktian efivitas komparatif dari kombinasi algoritma.

3. Bagi Peneliti Selanjutnya (*Akademisi*), menjadi sumber pustaka, bahan pertimbangan, serta acuan data kuantitatif yang valid bagi peneliti masa depan yang ingin mengembangkan, menguji, atau membandingkan variasi algoritma kriptografi hibrida lainnya dalam ranah keamanan transaksi finansial digital.