METODE PEMBAYARAN ELEKTRONIK BERDASARKAN PADA KRIPTOGRAFI

Nurlina sari Harahap, Muhammad Iqbal
Universitas Pembangunan Panca Budi Medan
nurlinasariharahap68@gmail.com

ABSTRAK

Perkembangan pesat teknologi informasi dan komunikasi di era digital menuntut adanya sistem keamanan informasi yang andal untuk melindungi data dan komunikasi elektronik. Salah satu pilar utama dalam menjaga keamanan tersebut adalah kriptografi. Permasalahan yang muncul adalah masih terbatasnya pemahaman komprehensif mengenai konsep dasar kriptografi, perkembangannya, serta klasifikasi jenis-jenis kriptografi yang digunakan dalam sistem keamanan informasi modern. Penelitian ini bertujuan untuk mengkaji konsep kriptografi secara menyeluruh, meliputi definisi, perkembangan historis, komponen utama, serta klasifikasi kriptografi yang diterapkan dalam keamanan informasi. Metode penelitian yang digunakan adalah studi literatur dengan menganalisis berbagai sumber ilmiah, buku, dan referensi daring yang relevan dengan topik kriptografi. Hasil kajian menunjukkan bahwa kriptografi tidak hanya berfungsi sebagai teknik penyamaran pesan, tetapi telah berkembang menjadi mekanisme keamanan data yang sistematis melalui penerapan algoritma, kunci kriptografi, serta proses enkripsi dan dekripsi. Selain itu, kriptografi diklasifikasikan ke dalam beberapa jenis utama, yaitu kriptografi simetris, asimetris, hashing, dan kriptografi kuantum, yang masing-masing memiliki karakteristik, kelebihan, dan keterbatasan. Pemahaman yang mendalam terhadap konsep dan klasifikasi kriptografi menjadi landasan penting dalam perancangan sistem keamanan informasi yang efektif.

Kata kunci : *electronic payments, cryptography, technology*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam cara manusia bertransaksi, terutama sejak era digitalisasi yang semakin meluas. Di Indonesia, sistem pembayaran elektronik seperti e-payment, mobile banking, dan berbagai metode berbasis QR Code telah menjadi bagian penting dalam aktivitas ekonomi sehari-hari. Menurut laporan Bank Indonesia, transaksi digital terus menunjukkan pertumbuhan signifikan, misalnya dalam layanan QRIS yang mengalami lonjakan pengguna dan volume transaksi secara tahunan, mencerminkan perubahan preferensi masyarakat dari transaksi tunai ke non-tunai karena kecepatan, efisiensi, dan kemudahan penggunaannya[1].

Adopsi transaksi non-tunai di Indonesia semakin meluas dengan hadirnya layanan seperti QRIS (Quick Response Code Indonesian Standard), e-wallet (GoPay, OVO, Dana), dan platform perbankan digital. Pertumbuhan ini tidak hanya terjadi di perkotaan tetapi juga merambah ke sektor UMKM dan ekonomi mikro di berbagai daerah. Data Bank Indonesia dan riset independen menunjukkan bahwa jutaan pengguna telah merasakan manfaat sistem pembayaran digital, yang memungkinkan transaksi tanpa uang tunai yang cepat, aman, dan terintegrasi lintas aplikasi. Namun demikian, pemahaman masyarakat terhadap risiko keamanan masih bervariasi, sehingga edukasi dan literasi digital menjadi aspek penting dalam memperkuat keyakinan penggunaan teknologi pembayaran ini[2].

Di balik pertumbuhan transaksi digital tersebut, ancaman keamanan siber juga semakin kompleks dan berkembang. Risiko seperti phishing, quishing (QR phishing), pencurian data, dan manipulasi QR Code menjadi ancaman nyata yang dapat merugikan pengguna maupun penyedia layanan. Berdasarkan penelitian di Indonesia, serangan quishing menjadi salah satu tantangan utama di sistem pembayaran digital karena pelaku dapat memanfaatkan kode QR palsu untuk mengelabui konsumen dan mencuri data finansial mereka. Kasus-kasus ini sering memicu kerugian finansial hingga puluhan juta rupiah, memperlihatkan bahwa tantangan keamanan bukan sekadar teori tetapi telah berdampak nyata di masyarakat[3].

Ancaman keamanan dalam transaksi elektronik tidak hanya berpengaruh pada kerugian materiil, tetapi juga berdampak pada kepercayaan pengguna dan perlindungan data pribadi. Penelitian akademik menunjukkan bahwa tingkat keamanan aplikasi pembayaran sangat memengaruhi tingkat kepercayaan konsumen dalam bertransaksi. Selain itu, meskipun banyak platform telah mengimplementasikan fitur keamanan seperti biometrik, PIN, dan OTP, risiko phishing dan upaya pencurian data masih menjadi masalah utama yang harus diatasi melalui pendekatan teknologi yang lebih kuat dan edukasi pengguna yang berkelanjutan[4].

Melihat perkembangan transaksi elektronik yang pesat sekaligus ancaman keamanan yang kompleks, semakin jelas bahwa inovasi dalam sistem keamanan pembayaran digital menjadi kebutuhan mendesak. Tidak cukup hanya mempertahankan metode enkripsi konvensional, pendekatan baru seperti integrasi teknologi lanjutan (misalnya blockchain, analisis perilaku pengguna, atau algoritma autentikasi visual) perlu dieksplorasi untuk menghadapi ancaman siber yang semakin canggih. Hal ini penting untuk menjaga

keandalan, kepercayaan, serta memberikan perlindungan maksimal bagi konsumen, pelaku usaha, dan penyedia layanan dalam ekosistem transaksi digital Indonesia yang terus berkembang[5].

Seiring dengan meningkatnya ancaman dalam transaksi elektronik, kriptografi menjadi komponen krusial dalam menjaga keamanan sistem pembayaran digital. Kriptografi adalah ilmu dan teknik penyandian informasi sehingga hanya pihak yang berwenang dapat memahami atau memproses data tersebut. Dalam praktiknya, kriptografi tidak hanya berfungsi untuk menyamarkan data, tetapi juga melindungi kerahasiaan (*confidentiality*), memastikan bahwa hanya pihak yang berizin yang dapat mengakses informasi sensitif seperti data rekening atau kredensial pembayaran. Teknik ini telah menjadi fondasi berbagai protokol keamanan modern yang digunakan dalam transaksi digital, termasuk enkripsi, hashing, dan tanda tangan digital[6].

Salah satu elemen utama dalam kriptografi adalah enkripsi, yaitu proses mengubah data asli (*plaintext*) menjadi bentuk sandi (*ciphertext*) menggunakan algoritma dan kunci tertentu agar tidak dapat dibaca oleh pihak tak berwenang saat dikirim melalui jaringan. Ketika data transaksi dienkripsi, misalnya saat pengguna mentransfer dana melalui mobile banking atau e-wallet, data menjadi terlindungi dari serangan penyadapan atau serangan *man-in-the-middle* yang mencoba membaca atau memodifikasi informasi di tengah jalur komunikasi. Protokol keamanan seperti SSL/TLS yang digunakan di aplikasi dan situs pembayaran digital bergantung pada kriptografi kunci publik untuk membangun saluran komunikasi yang aman antara pengguna dan server.

Selain enkripsi, hashing merupakan teknik kriptografi yang penting dalam konteks keamanan transaksi digital karena berperan dalam menjaga integritas data. Fungsi hash akan mengubah data berukuran beragam menjadi nilai ringkas (*hash value*) yang unik; perubahan sekecil apapun pada data asli akan menghasilkan nilai hash yang sangat berbeda. Dalam sistem pembayaran, hashing digunakan untuk memverifikasi bahwa data transaksi tidak mengalami perubahan selama proses pengiriman atau penyimpanan, sehingga konsistensi dan keaslian transaksi dapat dipastikan[7].

Selanjutnya, tanda tangan digital (digital signature) adalah teknik kriptografi yang memastikan autentikasi dan non-repudiation dalam transaksi elektronik. Dengan menggunakan kunci privat untuk menandatangani data transaksi dan kunci publik untuk memverifikasi tanda tangan tersebut, sistem dapat membuktikan bahwa transaksi benar-benar dilakukan oleh pemilik kredensial yang sah dan tidak dimodifikasi selama proses transmisi. Hal ini sangat penting terutama dalam konteks transaksi keuangan online, di mana kepercayaan antar pihak menjadi prasyarat utama[8].

Dengan demikian, perpaduan teknik kriptografi enkripsi untuk kerahasiaan, hashing untuk integritas, dan tanda tangan digital untuk autentikasi dan non-repudiation membentuk pondasi utama keamanan transaksi elektronik modern. Tanpa mekanisme ini, sistem pembayaran digital akan rentan terhadap berbagai serangan siber yang dapat menyebabkan pencurian data, manipulasi transaksi, atau penyalahgunaan identitas digital. Karena itu, pemahaman dan pengembangan kriptografi secara terus-menerus menjadi kebutuhan penting seiring pertumbuhan pesat transaksi elektronik di masyarakat modern.

Berangkat dari uraian sebelumnya mengenai meningkatnya transaksi elektronik, kompleksitas ancaman keamanan digital, serta peran kriptografi sebagai fondasi perlindungan data transaksi, penelitian ini menjadi penting untuk dilakukan karena menyoroti kebutuhan akan pendekatan keamanan yang lebih adaptif, inovatif, dan berorientasi pada pengguna. Meskipun kriptografi tradisional seperti enkripsi, hashing, dan tanda tangan digital telah terbukti efektif, pada praktiknya masih terdapat celah yang dapat dimanfaatkan pelaku kejahatan siber, terutama melalui rekayasa sosial, phishing, dan manipulasi antarmuka pengguna.

Oleh karena itu, penelitian ini penting untuk mengeksplorasi dan mengkaji metode keamanan alternative seperti kriptografi visual yang tidak hanya memperkuat aspek teknis perlindungan data, tetapi juga meningkatkan keandalan autentikasi dan kemudahan verifikasi secara langsung oleh pengguna. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi teoretis dalam pengembangan ilmu keamanan sistem pembayaran elektronik serta kontribusi praktis sebagai rujukan bagi pengembang sistem dan pemangku kebijakan dalam merancang mekanisme pembayaran digital yang lebih aman, terpercaya, dan sesuai dengan tantangan transaksi elektronik modern.

Berdasarkan uraian latar belakang tersebut, permasalahan utama dalam penelitian ini terletak pada masih tingginya kerentanan keamanan dalam sistem pembayaran elektronik, khususnya yang berkaitan dengan serangan berbasis rekayasa sosial seperti phishing dan manipulasi QR Code, meskipun berbagai teknik kriptografi konvensional telah diterapkan. Kondisi ini menunjukkan adanya kesenjangan antara kecanggihan teknologi keamanan yang tersedia dengan tingkat perlindungan nyata yang dirasakan oleh pengguna. Oleh karena itu, penelitian ini bertujuan untuk mengkaji secara mendalam peran dan keterbatasan kriptografi dalam sistem pembayaran elektronik serta mengeksplorasi potensi penerapan metode keamanan alternatif, khususnya kriptografi visual, sebagai pendekatan yang lebih adaptif dan berorientasi pada pengguna.

Adapun rencana penyelesaian masalah dilakukan melalui kajian konseptual dan analisis literatur terhadap mekanisme keamanan transaksi elektronik, karakteristik ancaman siber yang berkembang, serta studi terhadap prinsip dan implementasi kriptografi

visual. Melalui pendekatan ini, penelitian diharapkan mampu menawarkan kerangka pemikiran dan rekomendasi strategis dalam pengembangan sistem pembayaran digital yang lebih aman, terpercaya, dan sesuai dengan tantangan keamanan transaksi elektronik modern.

2. TINJAUAN PUSTAKA

Sistem pembayaran elektronik berkembang pesat seiring meningkatnya adopsi e-wallet, mobile banking, dan QRIS di Indonesia. Digitalisasi transaksi memberikan kemudahan, efisiensi, dan perluasan inklusi keuangan, namun di sisi lain meningkatkan risiko kejahatan siber seperti phishing, quishing, dan pencurian data. Ancaman ini menunjukkan bahwa sistem pembayaran digital tidak hanya membutuhkan kecepatan dan kemudahan, tetapi juga mekanisme keamanan yang mampu melindungi data dan dana pengguna secara menyeluruh. Oleh karena itu, penguatan sistem keamanan menjadi kebutuhan mendesak untuk menjaga kepercayaan dan keberlanjutan ekosistem pembayaran elektronik[1].

Kriptografi merupakan fondasi utama dalam menjaga keamanan transaksi elektronik melalui mekanisme enkripsi, hashing, dan tanda tangan digital. Teknologi ini berperan dalam melindungi kerahasiaan, integritas, dan autentikasi data transaksi pada sistem pembayaran digital. Implementasi kriptografi simetris dan asimetris telah terbukti efektif dalam mengamankan data keuangan, namun pada praktiknya masih memiliki keterbatasan, terutama dalam menghadapi serangan berbasis rekayasa sosial dan manipulasi antarmuka pengguna. Hal ini menunjukkan bahwa kriptografi konvensional, meskipun kuat secara teknis, belum sepenuhnya mampu mengatasi celah keamanan yang melibatkan interaksi langsung dengan pengguna[9].

Kriptografi visual muncul sebagai pendekatan alternatif yang berfokus pada keamanan berbasis persepsi visual manusia, di mana proses dekripsi dapat dilakukan tanpa komputasi kompleks. Metode ini memungkinkan pengguna melakukan verifikasi secara langsung terhadap informasi atau autentikasi transaksi, sehingga berpotensi mengurangi risiko manipulasi visual seperti quishing dan pemalsuan QR Code. Berbeda dengan kriptografi konvensional yang menitikberatkan pada keamanan sistem, kriptografi visual menambahkan lapisan keamanan yang berorientasi pada pengguna (user-centered security). Novelty penelitian ini terletak pada pengintegrasian kriptografi visual sebagai pelengkap kriptografi tradisional dalam sistem pembayaran elektronik, guna memperkuat autentikasi, meningkatkan kepercayaan pengguna, serta menjawab tantangan keamanan transaksi digital yang semakin kompleks[7].

Berbagai penelitian terdahulu telah membahas keamanan sistem pembayaran elektronik dengan menitikberatkan pada penerapan kriptografi konvensional, seperti enkripsi kunci publik, hashing, dan tanda tangan digital dalam melindungi transaksi keuangan. Sejumlah studi menunjukkan bahwa penerapan protokol keamanan berbasis kriptografi mampu meningkatkan kerahasiaan dan integritas data transaksi, serta menekan risiko serangan teknis seperti penyadapan dan man-in-the-middle attack. Namun, penelitian lain juga mengungkapkan bahwa sebagian besar insiden keamanan pada sistem pembayaran digital justru disebabkan oleh faktor manusia, terutama melalui phishing, quishing, dan manipulasi antarmuka pengguna yang tidak sepenuhnya dapat dicegah oleh mekanisme kriptografi tradisional.

Di sisi lain, beberapa kajian mengenai kriptografi visual masih terbatas pada konteks pengamanan dokumen, otentikasi citra, atau sistem berbasis multimedia, dan belum banyak dieksplorasi dalam implementasi sistem pembayaran elektronik. Keterbatasan tersebut menunjukkan adanya celah penelitian yang membuka peluang untuk mengkaji integrasi kriptografi visual sebagai lapisan keamanan tambahan yang berorientasi pada pengguna, khususnya dalam menghadapi ancaman manipulasi visual pada transaksi digital berbasis QR Code.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian studi kepustakaan (*library research*). Pendekatan ini dipilih karena penelitian berfokus pada pengkajian konseptual dan teoritis mengenai peran kriptografi dalam sistem pembayaran elektronik serta eksplorasi kriptografi visual sebagai pendekatan keamanan alternatif yang berorientasi pada pengguna. Melalui studi kepustakaan, peneliti dapat menelaah secara mendalam perkembangan teori, konsep, dan temuan penelitian sebelumnya yang relevan dengan keamanan transaksi digital, khususnya dalam konteks sistem pembayaran elektronik berbasis QR Code dan aplikasi digital.

Data penelitian berupa data sekunder yang diperoleh dari berbagai sumber ilmiah yang kredibel, meliputi artikel jurnal nasional dan internasional bereputasi, buku referensi, prosiding konferensi, laporan resmi lembaga terkait seperti bank sentral dan institusi keamanan siber, serta sumber daring akademik yang relevan. Literatur dipilih berdasarkan kriteria relevansi dengan topik penelitian, tingkat kredibilitas sumber, serta keterkinian publikasi guna memastikan bahwa data yang digunakan mencerminkan kondisi dan tantangan keamanan sistem pembayaran elektronik terkini.

Proses pengumpulan data dilakukan melalui penelusuran literatur secara sistematis dengan menggunakan kata kunci terkait kriptografi, sistem pembayaran elektronik, keamanan transaksi digital, dan kriptografi visual. Literatur yang telah terkumpul kemudian diseleksi dan diklasifikasikan ke dalam tema-tema pembahasan, seperti konsep dasar kriptografi, mekanisme keamanan pembayaran elektronik, karakteristik ancaman siber, serta prinsip dan penerapan kriptografi visual.

Analisis data dilakukan dengan metode deskriptif-analitis, yaitu mendeskripsikan konsep dan mekanisme keamanan yang dikaji, kemudian menganalisis serta membandingkan karakteristik kriptografi konvensional dan kriptografi visual. Analisis ini bertujuan untuk mengidentifikasi keunggulan, keterbatasan, serta potensi kontribusi kriptografi visual sebagai pelengkap mekanisme keamanan pembayaran elektronik. Keabsahan data dijaga melalui teknik triangulasi sumber dengan membandingkan berbagai referensi yang memiliki perspektif berbeda, sehingga diperoleh pemahaman yang objektif dan komprehensif. Hasil analisis selanjutnya disintesis untuk merumuskan implikasi teoretis dan rekomendasi praktis bagi pengembangan sistem pembayaran elektronik yang lebih aman, adaptif, dan berorientasi pada pengguna.

4. HASIL DAN PEMBAHASAN

4.1. Defenisi Kriptografi

Secara etimologis, istilah kriptografi berasal dari bahasa Yunani, yaitu *kryptos* yang berarti tersembunyi dan *graphien* yang berarti menulis, yang secara konseptual menggambarkan aktivitas "menulis pesan secara tersembunyi". Dalam konteks keilmuan modern, kriptografi dipahami sebagai suatu metode sistematis untuk mengamankan informasi dengan cara mengubah data asli (*plaintext*) menjadi bentuk sandi (*ciphertext*) yang tidak dapat dipahami oleh pihak yang tidak berwenang. Proses pengubahan ini dikenal sebagai enkripsi, yang dilakukan menggunakan algoritma dan kunci tertentu agar informasi tetap terlindungi selama proses penyimpanan maupun transmisi. Sebaliknya, untuk memperoleh kembali informasi asli, pihak yang memiliki otorisasi dan kunci yang sesuai melakukan proses dekripsi, yaitu mengembalikan *ciphertext* ke dalam bentuk *plaintext*[6].

Pada awal perkembangannya, kriptografi digunakan terutama untuk mengamankan pesan tertulis, seperti pemakaian sandi dan kode rahasia dalam kepentingan militer dan diplomasi guna menyembunyikan informasi strategis dari pihak lawan. Fungsi kriptografi pada masa itu masih terbatas pada penyamaran pesan agar hanya dapat dipahami oleh pihak tertentu. Namun, seiring dengan kemajuan teknologi informasi dan komunikasi, ruang lingkup kriptografi mengalami perkembangan yang signifikan. Kriptografi tidak lagi hanya berfungsi untuk melindungi pesan tertulis, tetapi juga diterapkan secara luas dalam konteks digital untuk mengamankan data yang dikirimkan melalui jaringan komputer, menjaga privasi pengguna, serta melindungi sistem informasi dari berbagai bentuk serangan siber. Transformasi ini menjadikan kriptografi sebagai fondasi utama keamanan digital modern, yang berperan penting dalam mendukung keandalan sistem komunikasi, transaksi elektronik, dan layanan berbasis teknologi informasi sebagaimana telah dibahas pada paragraf sebelumnya[10].

Sebagaimana telah dijelaskan sebelumnya, kriptografi berperan sebagai fondasi utama dalam menjaga keamanan informasi di era digital. Untuk dapat menjalankan fungsi tersebut secara efektif, kriptografi tersusun atas beberapa komponen utama yang saling berkaitan dan bekerja secara sistematis. Setiap komponen memiliki peran spesifik dalam memastikan bahwa informasi dapat dikirim, disimpan, dan diproses dengan aman tanpa dapat diakses atau dimanipulasi oleh pihak yang tidak berwenang[11]. Pemahaman terhadap komponen-komponen ini menjadi penting sebagai dasar dalam merancang dan menganalisis sistem keamanan informasi. Komponen pertama dalam kriptografi adalah plaintext, yaitu pesan atau data asli yang ingin dilindungi. Plaintext dapat berupa teks, angka, gambar, maupun data transaksi digital seperti informasi rekening atau detail pembayaran. Pada tahap ini, data masih berada dalam bentuk yang mudah dipahami dan sangat rentan terhadap penyadapan atau pencurian apabila dikirimkan melalui jaringan terbuka. Oleh karena itu, plaintext menjadi objek utama yang harus diamankan sebelum diproses lebih lanjut dalam sistem kriptografi.

Setelah melalui proses pengamanan, plaintext akan diubah menjadi ciphertext, yaitu hasil dari proses enkripsi yang membuat pesan tidak dapat dibaca atau dipahami oleh pihak yang tidak memiliki otorisasi. Ciphertext umumnya tampak sebagai rangkaian karakter acak yang tidak memiliki makna secara langsung. Transformasi ini bertujuan untuk menyembunyikan isi pesan sehingga meskipun data berhasil disadap, informasi di dalamnya tetap terlindungi. Dengan demikian, ciphertext menjadi bentuk aman dari data selama proses transmisi maupun penyimpanan. Komponen penting lainnya adalah kunci (key), yaitu nilai tertentu yang digunakan dalam proses enkripsi dan dekripsi. Kunci berfungsi sebagai elemen rahasia yang menentukan bagaimana data diubah dan dikembalikan ke bentuk aslinya. Dalam kriptografi modern, dikenal dua jenis kunci utama, yaitu kunci simetris, yang menggunakan kunci yang sama untuk enkripsi dan dekripsi, serta kunci asimetris, yang menggunakan sepasang kunci publik dan kunci privat. Pengelolaan kunci yang baik sangat menentukan tingkat keamanan sistem kriptografi, karena keamanan pesan pada dasarnya bergantung pada kerahasiaan kunci, bukan pada algoritmanya[7].

Seluruh proses kriptografi dijalankan berdasarkan algoritma kriptografi serta mekanisme enkripsi dan dekripsi. Algoritma kriptografi merupakan serangkaian aturan atau formula matematis yang menentukan cara mengubah plaintext menjadi ciphertext dan sebaliknya. Proses enkripsi bertujuan untuk mengamankan data dengan mengubahnya ke dalam format yang tidak dapat dibaca, sedangkan proses dekripsi berfungsi untuk mengembalikan ciphertext ke bentuk plaintext agar dapat digunakan kembali oleh pihak yang berwenang. Kombinasi antara algoritma yang kuat, kunci yang aman, serta proses enkripsi dan dekripsi yang tepat menjadikan

kriptografi mampu memberikan perlindungan yang andal terhadap berbagai ancaman keamanan informasi di era digital.

4.2. Jenis-Jenis Kriptografi

Sebagaimana telah dijelaskan sebelumnya, kriptografi tidak hanya terdiri atas komponen-komponen dasar seperti plaintext, ciphertext, kunci, dan algoritma, tetapi juga dapat diklasifikasikan ke dalam beberapa jenis berdasarkan metode pengamanan dan penggunaan kunci. Klasifikasi ini penting untuk memahami karakteristik, kelebihan, dan keterbatasan masing-masing metode kriptografi, sehingga dapat diterapkan secara tepat sesuai dengan kebutuhan sistem keamanan informasi, khususnya dalam konteks transaksi elektronik dan komunikasi digital[9].

Jenis kriptografi yang paling awal dan paling banyak digunakan adalah kriptografi simetris (*symmetric cryptography*). Pada metode ini, kunci yang sama digunakan baik untuk proses enkripsi maupun dekripsi. Artinya, pengirim dan penerima pesan harus memiliki kunci rahasia yang identik agar dapat saling bertukar informasi secara aman. Konsep ini menjadikan kriptografi simetris relatif sederhana dalam implementasi, namun menuntut pengelolaan kunci yang baik agar tidak jatuh ke tangan pihak yang tidak berwenang.

Contoh algoritma yang menerapkan kriptografi simetris antara lain AES (Advanced Encryption Standard) dan DES (Data Encryption Standard). AES saat ini menjadi standar enkripsi global yang banyak digunakan dalam sistem keamanan modern karena tingkat keamanannya yang tinggi dan efisiensi komputasinya. Sementara itu, DES merupakan algoritma yang lebih tua dan kini dianggap kurang aman untuk penggunaan skala besar. Kelebihan utama kriptografi simetris terletak pada kecepatan pemrosesan data, sehingga sangat cocok digunakan untuk mengenkripsi data dalam jumlah besar, seperti pada komunikasi jaringan dan penyimpanan data[12].

Meskipun demikian, kriptografi simetris memiliki kelemahan utama, yaitu permasalahan distribusi kunci. Karena kunci yang sama harus dibagikan kepada pihak penerima, terdapat risiko kebocoran kunci selama proses distribusi, terutama jika dilakukan melalui jaringan yang tidak aman. Tantangan inilah yang mendorong berkembangnya metode kriptografi lain yang mampu mengatasi masalah pertukaran kunci secara lebih aman[9].

Sebagai solusi atas keterbatasan tersebut, dikembangkanlah kriptografi asimetris (*asymmetric cryptography*), yang menggunakan sepasang kunci yang berbeda, yaitu kunci publik dan kunci privat. Kunci publik dapat dibagikan secara bebas kepada siapa saja dan digunakan untuk melakukan enkripsi, sedangkan kunci privat bersifat rahasia dan hanya dimiliki oleh penerima untuk melakukan dekripsi. Dengan mekanisme ini, risiko kebocoran kunci rahasia dapat diminimalkan.

Algoritma yang populer dalam kriptografi asimetris antara lain RSA (Rivest–Shamir–Adleman) dan ECC (Elliptic Curve Cryptography). RSA banyak digunakan dalam sistem keamanan web dan tanda tangan digital, sedangkan ECC menawarkan tingkat keamanan yang setara dengan RSA tetapi menggunakan ukuran kunci yang lebih kecil, sehingga lebih efisien. Keunggulan utama kriptografi asimetris adalah keamanan distribusi kunci dan kemampuannya mendukung autentikasi serta tanda tangan digital, meskipun proses enkripsi dan dekripsinya relatif lebih lambat dibandingkan metode simetris[7].

Selain kriptografi simetris dan asimetris, terdapat pula kriptografi hashing, yang memiliki karakteristik berbeda. Hashing merupakan proses mengubah data masukan menjadi nilai hash dengan panjang tetap menggunakan fungsi satu arah (*one-way function*). Berbeda dengan enkripsi, hasil hashing tidak dapat dikembalikan ke bentuk semula. Oleh karena itu, hashing tidak digunakan untuk menyembunyikan data, melainkan untuk memverifikasi integritas data dan menjaga keamanan informasi sensitif seperti kata sandi.

Contoh algoritma hashing yang umum digunakan adalah SHA-256 (Secure Hash Algorithm) dan MD5 (Message Digest Algorithm). SHA-256 banyak diterapkan dalam sistem keamanan modern karena ketahanannya terhadap serangan kolisi, sedangkan MD5 kini sudah jarang digunakan karena memiliki kelemahan keamanan. Dalam sistem transaksi digital, hashing berperan penting untuk memastikan bahwa data tidak mengalami perubahan selama proses transmisi maupun penyimpanan.

Perkembangan teknologi juga melahirkan konsep kriptografi kuantum (*quantum cryptography*), yang memanfaatkan prinsip-prinsip fisika kuantum dalam proses pengamanan data. Metode ini menggunakan partikel kuantum, seperti foton, untuk mendistribusikan kunci enkripsi sehingga setiap upaya penyadapan dapat terdeteksi secara langsung. Meskipun masih berada dalam tahap pengembangan dan implementasinya belum luas, kriptografi kuantum dipandang sebagai solusi masa depan yang menjanjikan tingkat keamanan jauh lebih tinggi dibandingkan metode kriptografi tradisional[7].

Secara keseluruhan, keberagaman jenis kriptografi menunjukkan bahwa tidak ada satu metode yang sepenuhnya sempurna untuk semua kebutuhan keamanan. Setiap jenis kriptografi memiliki keunggulan dan keterbatasan masing-masing, sehingga sering kali dikombinasikan dalam satu sistem keamanan. Pemahaman terhadap klasifikasi ini menjadi landasan penting untuk mengembangkan pendekatan kriptografi yang lebih inovatif, termasuk penerapan metode kriptografi visual sebagai alternatif atau pelengkap dalam sistem pembayaran elektronik yang aman.

Hasil pembahasan menunjukkan bahwa kriptografi merupakan elemen fundamental dalam sistem keamanan informasi modern. Secara

konseptual, kriptografi tidak hanya dipahami sebagai teknik penyamaran pesan, tetapi telah berkembang menjadi disiplin ilmu yang sistematis dan berbasis algoritma matematis untuk melindungi data dari akses yang tidak sah. Perkembangan makna ini menegaskan bahwa kriptografi memiliki peran strategis dalam menjaga kerahasiaan, integritas, dan keandalan informasi, terutama dalam konteks komunikasi digital dan transaksi elektronik yang semakin kompleks.

Seiring dengan transformasi teknologi informasi, fungsi kriptografi mengalami perluasan yang signifikan. Jika pada masa awal kriptografi hanya berfokus pada pengamanan pesan tertulis dalam kepentingan militer dan diplomasi, maka pada era digital kriptografi telah menjadi fondasi utama dalam melindungi data yang tersimpan maupun yang ditransmisikan melalui jaringan komputer. Peran ini mencakup perlindungan privasi pengguna, keamanan sistem informasi, serta pencegahan terhadap berbagai bentuk serangan siber. Dengan demikian, kriptografi berfungsi sebagai mekanisme pertahanan utama dalam menjaga kepercayaan dan stabilitas sistem digital.

Pembahasan selanjutnya menegaskan bahwa efektivitas kriptografi ditentukan oleh keterpaduan komponen-komponen utamanya, yaitu plaintext, ciphertext, kunci, dan algoritma kriptografi. Plaintext sebagai data asli merupakan objek utama yang harus dilindungi karena kerentanannya terhadap penyadapan. Melalui proses enkripsi, plaintext diubah menjadi ciphertext yang tidak bermakna bagi pihak yang tidak memiliki otorisasi. Transformasi ini menjadi inti dari sistem kriptografi karena memastikan bahwa informasi tetap aman meskipun berada dalam lingkungan jaringan terbuka.

Komponen kunci (key) menjadi faktor krusial yang menentukan tingkat keamanan kriptografi. Keamanan suatu sistem kriptografi modern pada dasarnya tidak bergantung pada kerahasiaan algoritma, melainkan pada pengelolaan dan kerahasiaan kunci yang digunakan. Oleh karena itu, manajemen kunci yang tepat menjadi tantangan tersendiri dalam penerapan kriptografi, khususnya pada sistem berskala besar dan berbasis jaringan global. Hal ini menegaskan bahwa aspek teknis dan manajerial dalam kriptografi harus berjalan secara beriringan.

Berdasarkan metode penggunaan kunci, kriptografi dapat diklasifikasikan ke dalam beberapa jenis utama, salah satunya adalah kriptografi simetris. Metode ini menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sehingga menawarkan kecepatan pemrosesan yang tinggi dan efisiensi komputasi yang baik. Algoritma seperti AES dan DES menjadi contoh penerapan kriptografi simetris, dengan AES saat ini diakui sebagai standar global dalam pengamanan data. Keunggulan ini menjadikan kriptografi simetris sangat cocok untuk melindungi data dalam jumlah besar.

Namun demikian, hasil pembahasan juga menunjukkan bahwa kriptografi simetris memiliki kelemahan mendasar, yaitu pada aspek distribusi kunci. Risiko kebocoran kunci selama proses pertukaran menjadi tantangan serius yang dapat mengancam keamanan sistem secara keseluruhan. Keterbatasan inilah yang mendorong lahirnya kriptografi asimetris sebagai alternatif yang lebih aman dalam hal pertukaran kunci, khususnya pada sistem komunikasi terbuka seperti internet.

Kriptografi asimetris menawarkan solusi dengan menggunakan sepasang kunci yang berbeda, yaitu kunci publik dan kunci privat. Mekanisme ini memungkinkan proses enkripsi dilakukan tanpa harus membagikan kunci rahasia, sehingga meningkatkan tingkat keamanan dalam distribusi kunci. Algoritma seperti RSA dan ECC tidak hanya berfungsi untuk enkripsi data, tetapi juga mendukung autentikasi dan tanda tangan digital. Meskipun memiliki kecepatan pemrosesan yang lebih lambat dibandingkan kriptografi simetris, keunggulan keamanannya menjadikan metode ini sangat relevan dalam sistem pembayaran elektronik dan komunikasi daring.

Selain itu, kriptografi hashing dan kriptografi kuantum melengkapi spektrum metode pengamanan data. Hashing berperan penting dalam menjaga integritas data dan keamanan kata sandi melalui fungsi satu arah, sementara kriptografi kuantum menawarkan paradigma baru dengan memanfaatkan prinsip fisika kuantum untuk mendeteksi penyadapan secara langsung. Keberagaman jenis kriptografi ini menunjukkan bahwa sistem keamanan modern umumnya mengombinasikan berbagai metode untuk mencapai perlindungan optimal. Pemahaman menyeluruh terhadap definisi, komponen, dan klasifikasi kriptografi menjadi landasan penting dalam mengembangkan pendekatan kriptografi yang inovatif dan adaptif terhadap tantangan keamanan digital masa depan.

5. KESIMPULAN

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan bahwa kriptografi merupakan disiplin ilmu yang memiliki peran sangat penting dalam menjaga keamanan informasi di era digital. Secara konseptual, kriptografi berfungsi untuk melindungi data dengan mengubah plaintext menjadi ciphertext melalui proses enkripsi dan mengembalikannya kembali melalui proses dekripsi menggunakan algoritma dan kunci tertentu. Perkembangan teknologi informasi telah memperluas peran kriptografi dari sekadar pengamanan pesan tertulis menjadi fondasi utama dalam sistem keamanan komunikasi, penyimpanan data, dan transaksi elektronik.

Kriptografi tersusun atas beberapa komponen utama yang saling berkaitan, yaitu plaintext, ciphertext, kunci, dan algoritma kriptografi. Keamanan suatu sistem kriptografi sangat bergantung pada pengelolaan kunci yang baik serta kekuatan algoritma yang digunakan. Tanpa integrasi komponen-komponen tersebut secara tepat, sistem keamanan

informasi akan rentan terhadap berbagai ancaman dan serangan siber.

Berdasarkan metode pengamanan dan penggunaan kunci, kriptografi dapat diklasifikasikan ke dalam kriptografi simetris, asimetris, hashing, dan kriptografi kuantum. Kriptografi simetris unggul dalam kecepatan pemrosesan data, kriptografi asimetris menawarkan keamanan distribusi kunci dan autentikasi, hashing berperan dalam menjaga integritas data, sedangkan kriptografi kuantum menghadirkan pendekatan keamanan masa depan dengan tingkat proteksi yang lebih tinggi. Keberagaman jenis ini menunjukkan bahwa tidak ada satu metode kriptografi yang sepenuhnya sempurna untuk semua kebutuhan, sehingga kombinasi berbagai metode sering diterapkan dalam satu sistem keamanan.

Dengan demikian, pemahaman yang komprehensif terhadap definisi, komponen, dan jenis-jenis kriptografi menjadi sangat penting sebagai dasar pengembangan sistem keamanan informasi yang andal dan inovatif. Kesimpulan ini sekaligus menegaskan bahwa kriptografi merupakan elemen strategis dalam mendukung kepercayaan, keamanan, dan keberlanjutan layanan digital di masa kini dan masa mendatang.

DAFTAR PUSTAKA

[1] Bank indonesia, "Menjaga Keamanan di Tengah Kenyamanan Transaksi digital," *bank indonesia*, 2025. https://www.bi.go.id/id/publikasi/ruang-media/cerita-bi/Pages/Menjaga-Keamanan-di-Tengah-Kenyamanan-Transaksi-Digital.aspx (diakses 17 Januari 2026).

[2] S. A. Abdul Rachman, Niken Julianti, "Challenges and Opportunities for QRIS Implementation as a Digital Payment System in Indonesia," *EkBis J. Ekon. Dan Bisnis*, vol. 8, no. 1, hal. 1–13, 2024.

[3] Francisca Bertha Vistika, "QRIS Tumbuh 169%, Sistem Pembayaran Digital Harus Diperkuat Keamanannya," *MOMSMONEY.ID*, 2025.

[4] M. Rabbani, "Digital Payments in Indonesia: Understanding the Effect of Application Security on User Trust," *Indones. J. Comput. Sci.*, vol. 12, no. 5, 2023.

[5] A. N. Z. Abel Yehud Silalahi, "Arrangement of Blockchain Technology as an Effort to Prevent Payment Fraud via the Indonesian Standard Quick Response Code (Qris) Performed by Consumers in Electronic Transactions," *June Law Sci. F.*, vol. 13, no. 2, 2024.

[6] redha, "Kriptografi," *Biro penjamin mutu*, 2024.

[7] "Prinsip-prinsip inti dari kriptografi modern," *IBM*, 2025. https://www.ibm.com/id-id/think/topics/cryptography?utm_source=chatgpt.com (diakses 17 Januari 2026).

[8] Daniel Bintang, "Metode Kriptografi untuk Keamanan Siber yang Efektif," *NET MEDIA*, 2025. https://www.net.or.id/2025/01/Metode-Kriptografi-untuk-Keamanan-Siber-yang-Efektif.html?utm_source=chatgpt.com (diakses 17 Januari 2026).

[9] "Algoritma Kriptografi: Pengertian, Jenis, dan Cara Kerjanya dalam Keamanan Data," *UNESA*, 2025. https://terapan-ti.vokasi.unesa.ac.id/post/algoritma-kriptografi-pengertian-jenis-dan-cara-kerjanya-dalam-keamanan-data?utm_source=chatgpt.com (diakses 17 Januari 2026).

[10] Diporahmat, "Kriptografi," *Wordpress*, 2020. https://seputarksk.wordpress.com/2020/10/20/pertemuan-6/?utm_source=chatgpt.com

[11] Rifki Kuntoro Aldi, "Pengertian Kriptografi dan Hubungannya dengan Enkripsi Data," *Universitas Duta bangsa Surakarta*, 2025. https://fikom.udb.ac.id/id/artikel/detail/pengertian-kriptografi-dan-hubungannya-dengan-enkripsi-data?utm_source=chatgpt.com

[12] "Advanced Encryption Standard," *wikipedia*. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard?utm_source=chatgpt.com