



Nama : Fiqri Fathurrohman

Nim : 2023080120G

Matkul : Kripto

Analisis Perbandingan Chiper AFGVX dan Enigma dalam Komunikasi Militer Jerman pada Perang Dunia I dan II

1. Pendahuluan

Kriptografi merupakan salah satu disiplin ilmu tertua yang terus berkembang, berperan vital dalam menjaga **kerahasiaan** dan **integritas** data, terutama dalam konteks komunikasi militer dan intelijen. Dalam era digital, di mana ancaman keamanan siber menjadi tantangan utama, peran kriptografi modern (seperti AES dan RSA) sebagai solusi pertahanan data semakin tidak terbantahkan.

Sejarah modern kriptografi secara signifikan diwarnai oleh upaya Jerman dalam mengamankan komunikasinya selama dua konflik global. Pada **Perang Dunia I (PD I)**, militer Jerman mengandalkan *cipher ADFGVX*, sedangkan pada **Perang Dunia II (PD II)**, mereka menggunakan mesin sandi **Enigma**. Meskipun kedua sistem ini merupakan representasi puncak teknologi enkripsi pada masanya, keduanya berhasil dipecahkan oleh pihak Sekutu, yang secara drastis memengaruhi hasil akhir peperangan.

Tujuan dari tinjauan literatur ini adalah untuk menganalisis dan membandingkan secara komprehensif mekanisme, tingkat kerumitan, konteks operasional, serta dampak keberhasilan kriptanalisis *Cipher ADFGVX* (PD I) dan Mesin Enigma (PD II) terhadap komunikasi militer Jerman. Perbandingan ini diharapkan dapat memberikan wawasan mengenai evolusi teknik kriptografi klasik ke arah elektromekanis dan pentingnya faktor kriptanalisis dalam sejarah militer

2. Konsep Dasar Kriptografi

Definisi Dan Tujuan Kriptografi

Secara etimologi, kriptografi berasal dari bahasa Yunani, yaitu *kryptos* (tersembunyi) dan *graphein* (menulis). Secara umum, **kriptografi** adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan mengubah *plaintext* (pesan asli) menjadi *ciphertext* (teks tersandi) melalui proses **enkripsi**, dan mengembalikannya menjadi *plaintext* melalui proses **dekripsi**.

Tujuan utama dari kriptografi dalam keamanan data, baik klasik maupun modern, meliputi:

1. **Kerahasiaan (*Confidentiality*)**: Memastikan pesan hanya dapat dibaca oleh pihak yang berwenang.
2. **Integritas (*Integrity*)**: Memastikan pesan tidak diubah atau dimodifikasi selama transmisi.
3. **Autentikasi (*Authentication*)**: Memastikan keaslian pengirim dan penerima pesan.
4. **Non-repudiasi (*Non-repudiation*)**: Mencegah pengirim menyangkal telah mengirim pesan.

Jenis-Jenis Kriptografi

Kriptografi dibagi menjadi tiga kategori utama berdasarkan kunci yang digunakan:

1. **Symmetric Key (*Kunci Simetris*)**: Menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini cenderung lebih cepat dan efisien.
2. **Asymmetric Key (*Kunci Asimetris/Kunci Publik*)**: Menggunakan pasangan kunci yang berbeda: **kunci publik** untuk enkripsi dan **kunci privat** untuk dekripsi. Kunci publik dapat disebar, sedangkan kunci privat dirahasiakan.
3. **Hash Function (*Fungsi Hash*)**: Mengubah pesan input (panjang bervariasi) menjadi *hash value* atau *message digest* (panjang tetap) yang bersifat satu arah (*one-way*) dan tidak dapat dikembalikan menjadi pesan asli. Fungsi ini digunakan untuk menjamin integritas data dan mengamankan kata sandi.

Tabel 2.1 Perbandingan Jenis Algoritma Kriptografi

Fitur	Kriptografi Kunci Simetris	Kriptografi Kunci Asimetris	Fungsi Hash
Kunci	Satu kunci (sama) untuk enkripsi C dekripsi	Dua kunci (kunci publik C kunci privat)	Tidak menggunakan kunci, tetapi fungsi matematika satu arah
Kecepatan	Sangat cepat (tinggi)	Sangat lambat (rendah)	Sangat cepat (tinggi)
Keamanan	Kuat, bergantung pada kerahasiaan kunci tunggal	Kuat, keamanannya berdasarkan kesulitan pemecahan kunci privat	Kuat, digunakan untuk integritas C autentikasi, bukan kerahasiaan
Aplikasi	Enkripsi data massal (AES, DES)	Tanda tangan digital, pertukaran kunci aman (RSA, ECC)	Verifikasi integritas file, penyimpanan password (SHA, MD5)

3. Tinjauan Penelitian Terdahulu

Penelitian terdahulu yang relevan berfokus pada mekanisme ADFGVX dan Enigma, serta upaya kriptanalisis yang berhasil memecahkan kedua sandi tersebut.

Peneliti s Tahun	Algoritma/Sistem	Konteks/Tujuan Penelitian	Hasil s Temuan	Kelemahan/Keterbatasan
Poulter s Kulp (n.d.)	Cipher ADFGVX	Menjelaskan prinsip kerja dan konteks sejarah Cipher ADFGVX di PD I.	ADFGVX adalah <i>private-key encryption</i> yang menggunakan dua langkah: substitusi Polybius Square, dilanjutkan dengan transposisi keyword (kolom). Digunakan di garis depan parit selama PD I untuk mengamankan komunikasi radio.	Analisis lebih fokus pada deskripsi teknis daripada kriptanalisis mendalam.
Lasry (2018)	ADFGVX C Kriptanalisis Klasik	Mengembangkan metodologi baru untuk kriptanalisis <i>cipher klasik</i> yang	ADFGVX digunakan Angkatan Darat Jerman pada bulan-	Fokus utama adalah metodologi kriptanalisis modern, bukan perbandingan historis.

Peneliti s Tahun	Algoritma/Sistem	Konteks/Tujuan Penelitian	Hasil s Temuan	Kelemahan/Keterbatasan
		menantang menggunakan <i>Local Search Metaheuristics</i> .	bulan terakhir PD I (Juli-Desember 1918). Penelitian ini berhasil mendekripsi 93% dari 668 <i>cryptograms</i> ADFGVX yang tersisa dari arsip PD I, menunjukkan efektivitas metode modern terhadap sandi klasik.	
Manurung s Prabaswari (2024)	Mesin Sandi Enigma	Mengulas sejarah penyebab kekalahan Jerman di PD II melalui keberhasilan peretasan	Kekalahan Jerman di PD II salah satunya disebabkan oleh berhasil diretasnya Mesin Sandi	Hanya menyinggung Enigma sebagai latar belakang historis untuk konsep kerjasama sipil-militer, tidak menganalisis

Peneliti s Tahun	Algoritma/Sistem	Konteks/Tujuan Penelitian	Hasil s Temuan	Kelemahan/Keterbatasan
		sandi militer.	Enigma oleh Alan Turing dari Inggris. Keberhasilan peretasan ini merupakan sinergi antara ilmuwan sipil (Turing) dan militer.	mekanisme Enigma secara detail.

4. Analisi dan Sintesis

Perbandingan antara *Cipher ADFGVX* dan Mesin Enigma menunjukkan sebuah lompatan evolusioner dalam kriptografi militer Jerman, khususnya dalam kerumitan, keamanan, dan konteks operasional.

Perbandingan Kunci dan Mekanisme

1. **ADFGVX (PD I):** Cipher ini merupakan kombinasi dari dua teknik kriptografi klasik: **substitusi polyalphabetic** (menggunakan *Polybius square* dengan kunci substitusi acak 36 karakter) dan **transposisi kolumnar** (menggunakan *keyword transposisi*). Meskipun menggabungkan dua metode, sandi ini masih berbasis **tulisan tangan** (*hand-cipher*) dan dapat dipecahkan secara manual oleh kriptanalisis Perancis, Georges Painvin, pada tahun 1918. Kuncinya terdiri dari kunci substitusi (*Polybius square*) dan kunci transposisi (kata kunci).
2. **Enigma (PD II):** Enigma adalah mesin sandi elektromekanis yang jauh lebih canggih, mengimplementasikan **polyalphabetic substitution** yang sangat kompleks dan berubah-ubah melalui kombinasi rotor, *reflector*, dan *plugboard*.

Jumlah kemungkinan pengaturan kuncinya (keyspace) jauh lebih besar daripada ADFGVX, yang secara fundamental meningkatkan keamanan.

Perbandingan Efektivitas dan Dampak Kriptanalisis

Aspek	Cipher ADFGVX (PD I)	Mesin Enigma (PD II)
Era Penggunaan	Perang Dunia I (1918)	Perang Dunia II
Tipe Cipher	<i>Hand-Cipher</i> (Substitusi + Transposisi)	<i>Machine-Cipher</i> (Rotor Elektromekanis)
Kunci	Kunci Substitusi (Polybius) dan Kunci Transposisi (Kata Kunci)	Pengaturan Rotor, Posisi Awal Rotor, <i>Reflector</i> , dan <i>Plugboard</i>
Kriptanalisis	Dipecahkan secara manual oleh Georges Painvin (Prancis)	Dipecahkan menggunakan mesin elektromekanis (Bombe) dan metode statistika/matematika oleh Alan Turing (Inggris)
Dampak	Memberikan informasi taktis yang berharga kepada Sekutu pada akhir PD I.	Memberikan informasi strategis tingkat tinggi (Ultra) yang dianggap sebagai faktor kunci yang mempercepat kekalahan Jerman dalam PD II.

Secara sintesis, **Enigma** merepresentasikan tren algoritma yang lebih kompleks dan cepat melalui mekanisasi, mengatasi kerentanan *hand-cipher* seperti ADFGVX terhadap analisis frekuensi dan metode manual lainnya. Namun, keberhasilan kriptanalisis **Enigma** oleh Alan Turing menyoroti celah penelitian di bidang kriptografi pada saat itu, yaitu kegagalan dalam mengidentifikasi dan menghilangkan kerentanan prosedural dan operasional, terlepas dari kerumitan matematis mesin itu sendiri. ADFGVX menunjukkan bahwa bahkan kombinasi dua teknik kriptografi klasik masih rentan, sementara Enigma menunjukkan bahwa kerumitan mekanis pun dapat diatasi dengan inovasi teknologi dan kolaborasi (sipil-militer) dalam kriptanalisis.

5. Arah dan Peluan Penelitian

Analisis perbandingan antara ADFGVX dan Enigma memberikan beberapa arah penelitian lanjutan:

1. **Penerapan Kriptanalisis Modern pada *Cipher* Klasik:** Mengembangkan dan menguji efektivitas algoritma *metaheuristics* (seperti yang dilakukan oleh Lasry) atau kecerdasan buatan (AI) untuk memecahkan sandi klasik yang sangat panjang (seperti ADFGVX dan varian Enigma) yang belum terpecahkan secara historis.
2. **Kriptografi Ringan (*Lightweight Cryptography*):** Menganalisis bagaimana prinsip efisiensi yang coba dicapai oleh *hand-cipher* ADFGVX dapat diterapkan dalam pengembangan algoritma kriptografi ringan untuk perangkat dengan sumber daya terbatas (*IoT*), sambil tetap mempertahankan keamanan tingkat Enigma.
3. **Post-Quantum Cryptography (PQC) dan Enigma:** Menggali analogi antara transisi dari kriptografi mekanik ke elektrik (Enigma) dengan transisi saat ini menuju PQC. Penelitian dapat berfokus pada bagaimana kerentanan sistem yang ada (seperti Enigma yang dipecahkan oleh *Bombe*) dapat dijadikan pembelajaran dalam merancang algoritma PQC yang tahan terhadap ancaman komputasi kuantum.
4. **Optimalisasi Keamanan Prosedural:** Mempelajari secara mendalam kesalahan operasional militer Jerman (misalnya, penggunaan *key* yang berulang atau prosedur pesan yang buruk) yang menjadi celah peretasan Enigma, dan merumuskan pedoman keamanan prosedural yang relevan untuk sistem kriptografi modern.

6. Kesimpulan

Berdasarkan tinjauan literatur mengenai sistem kriptografi militer Jerman, disimpulkan bahwa **Cipher ADFGVX (PD I)** dan **Mesin Enigma (PD II)** merupakan dua tahap kunci dalam evolusi keamanan komunikasi.

ADFGVX adalah *hand-cipher* yang memadukan substitusi Polybius dan transposisi kolumnar. Meskipun inovatif untuk masanya, keterbatasannya sebagai sandi manual membuatnya rentan terhadap kriptanalisis frekuensi dan berhasil dipecahkan secara manual. Di sisi lain, **Enigma** adalah mesin sandi elektromekanis yang jauh lebih canggih, yang kegagalannya di PD II bukan hanya karena kerumitan matematis, tetapi juga karena adanya kelemahan dalam prosedur operasionalnya. Dampak pemecahan

Enigma (*Ultra*) secara strategis jauh melampaui ADFGVX, secara signifikan mempercepat berakhirnya PD II.

Oleh karena itu, penelitian selanjutnya dapat difokuskan pada penerapan metode kriptanalisis modern (*metaheuristics* dan AI) pada sandi klasik untuk mengevaluasi efektivitasnya, serta mempelajari kegagalan prosedural Enigma sebagai dasar perancangan sistem kriptografi modern yang aman dari segala aspek (teknis maupun operasional).

7. Daftar Pustaka

LINK Googel Drive

https://drive.google.com/drive/folders/1u5ukkmJAuLvimD7_dZ9Wu21zZaW0XCn?usp=sharing