Analisis Penerapan Kombinatorika dan Kriptografi Dalam Mesin Enigma

Alex Sander - 13521061[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13521061@std.stei.itb.ac.id

***Abstract*—Komunikasi dan Informasi merupakan 2 faktor terpenting dalam kemenangan perang. Informasi yang disalurkan melalui komunikasi antar sekutu harus sampai tanpa dicegati oleh pihak lawan. Oleh karena itu, pesan yang disalurkan harus dilakukan enkripsi dan dekripsi, yang biasa disebut dengan kriptografi. Kriptografi sudah digunakan sejak jaman dahulu kala dalam perang, namun dalam perang dunia II digunakan suatu kriptografi yang dapat dikirimkan melalui sinyal radio. Pesan yang disampaikan menggunakan kode morse, namun pada masa perang dunia II, kode morse sudah banyak dikuasai oleh massa. Dengan kebutuhan kriptografi yang memadai, pihak Jerman Nazi merancang mesin enigma yang pada masa itu termasuk mesin kriptografi dengan kompleksitas yang sangat tinggi dan tidak dapat dipecahkan oleh tangan manusia. Dengan tingkat enkripsi yang sangat kompleks, Jerman Nazi dapat menyalurkan informasi tanpa menghawatirkan cegatan dari pihak lawan.**

***Keywords*—Kombinatorika, Kriptografi, Enkripsi, Mesin Enigma, Perang Dunia II.**

I. PENDAHULUAN

Kombinatorika merupakan salah satu cabang matematika yang mempelajari sifat-sifat dan cara menghitung cara-cara terhingga. Kombinatorika berkaitan erat dengan cabang-cabang ilmu lain, seperti logika, peluang, kriptografi, ilmu komputer sampai ilmu biologi evolusioner. Kombinatorika dapat menghitung jumlah penyusunan objek-objek tanpa harus mengenumerasi semua kemungkinan susunannya. Salah satu contoh penerapan yang sering dilakukan sehari-hari adalah kombinatorika cabang peluang, dimana kita menganalisis peluang terjadinya serangkaian kejadian.

Komunikasi menggunakan radio merupakan sebuah kebutuhan dalam perang dunia II karena garis peperangan saat itu merentang sepanjang puluhan ribuan kilometer sehingga pesan penting atau instruksi dari atasan sulit untuk dikirimkan menggunakan cara konvensional seperti surat. Komunikasi menggunakan radio menjadi pilihan utama karena kecepatan pesan yang dikirimkan menggunakan sinyal radio adalah 300.000 kilometer per detik, atau lebih dikenal dengan kecepatan cahaya. Dengan kecepatan tersebut, pesan penting mengenai keadaan musuh atau instruksi dari atasan dapat tiba dalam kurang dari satu detik. Oleh karena itu, hampir seluruh komunikasi jarak jauh yang dilakukan pada perang dunia II dilakukan menggunakan sinyal radio.

Meskipun memiliki kelebihan kecepatan penghantar informasi dan jangkauannya sangat luas, sinyal radio mempunya kelemahan yang tidak dapat diabaikan saat digunakan untuk penghantaran informasi perperangan, yaitu sinyal radio dapat diakses semua orang yang memiliki alat untuk memproses sinyal radio. Pihak lawan hanya perlu mengetahui frekuensi yang digunakan untuk mentransmisi informasi, untuk mendapat akses informasi yang dibutuhkan. Oleh karena itu, diperlukan pengaplikasian ilmu kriptografi untuk mengenkripsi informasi yang ingin disalurkan.

Kriptografi dalam pengiriman pesan sudah dipakai dari jaman dahulu kala seperti Caesar chiper yang digunakan pada jaman Romawi kuno. Namun Caesar chiper tidak dapat digunakan pada zaman perang dunia II karena sifatnya yang sangat sederhana dan mudah untuk dipecahkan. Pada jaman perang dunia II, perang bukan hanya perang tank atau perang pesawat, namun ada juga perang informasi sehingga cipher pada jaman tersebut berkembang sangat pesat. Pada zaman tersebut diperlukan sebuah cipher yang sulit untuk dipecahkan oleh musuh, namun harus tetap mudah dan cepat untuk di decrypt oleh sekutu. Oleh karena itu ditemukanlah beberapa mesin cypher terkenal seperti mesin enigma. Mesin enigma merupakan salah satu mesin cypher paling terkenal yang digunakan oleh Nazi Jerman untuk mengodekan pesannya.

Mesin enigma melakukan enkripsi dan dekripsi dengan mekanisme kelistrikan melalui konfigurasi mesin tertentu yang dapat disetujui oleh pihak pengirim dan penerima. Konfigurasi mesin yang ada tidak sederhana, dengan banyaknya kemungkinan susunan bagian-bagian mesin. Tanpa adanya informasi konfigurasi yang benar, hasil dekripsi mesin tidak akan memiliki arti.

Pihak Jerman Nazi menggunakan keunggulan besar dalam mesin enigma ini dengan menghantarkan informasi dengan konfigurasi berbeda setiap harinya. Berdasarkan dokumentasi yang ada, pihak sekutu hanya memiliki waktu sehari untuk mencoba mencari konfigurasi mesin yang digunakan hari tersebut, namun dengan kompleksitas yang tinggi, pihak sekutu tidak dapat sekalipun mendekripsi pesan yang telah dicegati melalui radio. Tanpa informasi, pihak sekutu mengalami kerugian dan kekalah besar yang tidak terduga.

Pertanyaan yang muncul adalah seberapa kompleks mesin enigma ini? Bagaimana cara kerja enkripsi mesin enigma? dan Bagaimana pihak sekutu menyelesaikan masalah ini? Untuk menjawab pertanyaan-pertanyaan tersebut, kita harus memahami istilah-istilah penting yang telah penulis jabarkan

pada bab sebelumnya.

II. TEORI DASAR

1. Kombinatorika

Kombinatorika adalah matematika yang digunakan untuk menghitung penyusunan objek-objek tanpa mengetahui semua kemungkinan penyusunannya. Dalam skala kecil, penyusunan suatu kriteria mudah dijabarkan dan dihitung dengan tangan. Namun seiring membesarnya skala dan kompleks kriteria yang dianalisis, semakin susah untuk dilakukan dengan tangan. Ilmu kombinatorika dapat memudahkan proses ini dengan kaidah-kaidah khusus.

Terdapat beberapa kaidah dan prinsip yang digunakan dalam kombinatorika dasar, yaitu:

a. Kaidah perkalian (rule of product)
b. Kaidah penjumlahan (rule of sum)
c. Prinsip Inklusi Eksklusi
d. Permutasi
e. Kombinasi

Kaidah dasar menghitung merupakan aturan dasar dalam penghitungan dua atau lebih hasil percobaan menjadi satu pernyataan. Kaidah dasar ini dibagi menjadi dua, yaitu kaidah perkalian dan kaidah penjumlahan. Kaidah perkalian digunakan saat menggabungkan dua hasil percobaan dengan hubungan "dan". Kaidah penjumlahan digunakan saat menggabungkan dua atau lebih hasil percobaan dengan hubungan "atau".

Rule of product :
*If A has P(A) element(s), and B has P(B) elements(s), therefore the number of configurations to pick one element from A AND one element from B is P(A) * P(B).*
Rule of sum :
If A has P(A) element(s), and B has P(B) elements(s), therefore the number of configurations to pick one element from A OR B is P(A) + P(B).

Prinsip inklusi ekslusi merupakan prinsip yang digunakan saat hasil-hasil yang ingin disatukan memiliki anggota yang *conjoint* (Irisan anggota). Prinsip ini digunakan untuk menghindari duplikasi perhitungan

.

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Permutasi adalah prinsip pengurutan objek-objek yang memerhatikan urutan objek tersebut. Konsep permutasi digunakan untuk menghitung banyaknya penyusunan objek dengan memerhatikan urutan yang mungkin menggunakan kaidah perkalian. Konsep permutasi dapat dihitung dari penyusunan n objek dalam r ruang objek.

The permutation of n objects in r slots are

$$P(n,r) = \frac{n!}{(n-r)!}, n \geq r \geq 0$$

Permutation notations varies :

$$P(n,r) = {}_nP_r$$

Kombinasi adalah prinsip pengurutan objek-objek tanpa memerhatikan urutan objek tersebut. Konsep kombinasi digunakan untuk menghitung banyaknya penyusunan objek tanpa memerhatikan urutan yang mungkin menggunakan kaidah perkalian. Konsep kombinasi dapat dihitung dari penyusunan n objek dalam r ruang objek.

The combination of n objects in r slots are

$$C(n,r) = \frac{n!}{(n-r)!n!}, n \geq r \geq 0$$

Combination notations varies :

$$C(n,r) = \binom{n}{r} = {}_nC_r$$

Dengan konsep permutasi dan kombinasi, dapat dihitung banyaknya konfigurasi suatu objek dalam serangkaian kriteria tanpa mengetahui semua konfigurasi tersebut.

Salah satu bentuk khusus dari permutasi adalah permutasi dengan anggota yang sejenis. Pada permutasi dengan unsur yang sejenis, perbedaan urutan pada unsur yang sama tidak berpengaruh. Nilai permutasi unsur samar dari n elemen dengan banyaknya elemen ke-1 = a_1, ke-2 = a_2, ke-3 = a_3, ..., ke-n = a_n dapat dihitung sebagai berikut.

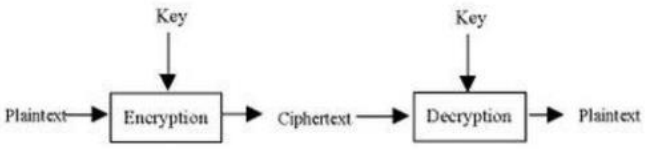
$$Px(n,r) = \frac{P(n,r)}{a_1!a_2!a_3!\ldots a_n!}, n \geq r \geq 0$$

2. Kriptografi

Kriptografi merupakan aplikasi ilmu teori bilangan yang digunakan untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bernama. Tujuan dari kripto grafi adalah agar pesan bersifat rahasia tidak dapat dibaca oleh pihak yang tidak berhak.

Objek yang diproses dalam kriptografi ada dua jenis, yaitu *plaintext* dan *ciphertext*. *Plaintext* atau biasa disebut pesan, adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. *Plaintext* berisi informasi yang ingin disampaikan dari pengirim kepada penerima. *Ciphertext* merupakan pesan yang telah disandikan sehingga tidak memiliki makna lagi. *Ciphertext* merupakan objek yang dikirimkan/diberi kepada penerima pesan untuk diproses.

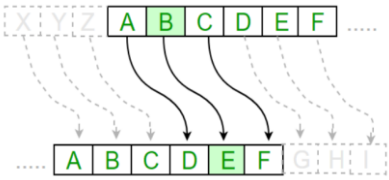
Proses dalam kriptografi dapat dibagi menjadi dua, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi merupakan proses mengubah *plaintext* menjadi *ciphertext* melalui suatu algoritma atau fungsi. Proses dekripsi merupakan proses mengubah kembali suatu *ciphertext* menjadi *plaintext* melalui suatu fungsi yang invers dari fungsi enkripsi.



Gambar 1 : Proses Enkripsi-Dekripsi
Sumber : https://slideplayer.info/slide/14242369/

Fungsi yang digunakan proses enkripsi berbeda-beda,

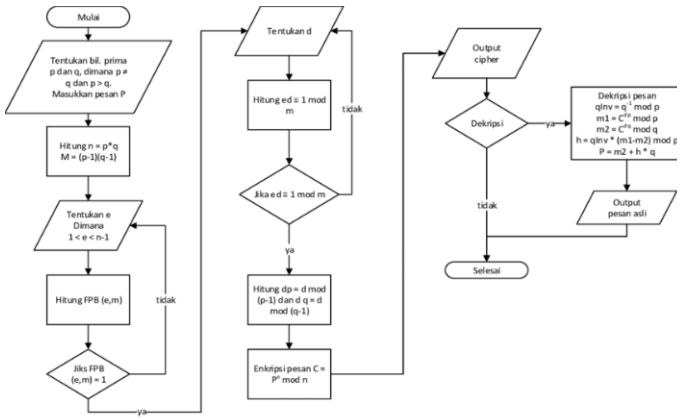
tergantung *cipher* apa yang digunakan. Contohnya pada *Caesar Cipher*, tiap huruf pada plaintext diubah menjadi alfabet n urutan setelah huruf aslinya.



Gambar 2: Diagram *Caesar Cipher* n=3
Sumber : https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

Fungsi enkripsi untuk *Caesar Cipher* n:
$E_n(x) = (x + n)\ mod\ 26$
Fungsi dekripsi untuk *Caesar Cipher* n:
$D_n(x) = (x - n)\ mod\ 26$

Jenis-jenis cipher sudah banyak ditemukan dan pada zaman modern ini tetap digunakan kriptografi untuk enkripsi data. Pada komputer, digunakan algoritma RSA yang menggunakan fitur *public key* dan *private key* yang meningkatkan kompleksitas algoritma enkripsi. Meski dapat dilakukan *brute force decrypting*, tetap akan memakan waktu yang sangat lama karena aplikasi sifat bilangan prima dalam algoritma RSA.

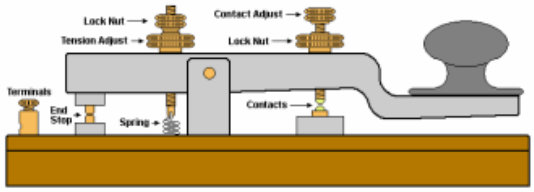


Gambar 3 : Flowchart Proses Algoritma RSA-CRT
Sumber : https://www.researchgate.net/

Algoritma RSA-CRT sudah banyak digunakan sebagai algoritma utama proses enkripsi-dekripsi pada aplikasi yang kita gunakan sehari-hari. Namun, salah satu kelemahan yang dimiliki oleh algoritma ini adalah pihak yang tidak berhak untuk mengakses informasi dapat mendekripsi semua *ciphertext* apabila mendapatkan *private key* pengguna.

3. Transmitter Sederhana

Transmitter sederhana adalah alat komunikasi berbasis sinyal radio yang hanya mampu mengirim sinyal statik on dan off. Cara kerjanya adalah saat tombol ditekan, akan terjadi kontak di bagian *contacts*. Dengan kontak tersebut, akan terhubung listrik sehingga menghasilkan suara.



Gambar 4 : Transmitter Sederhana

Karena hanya memiliki 2 *state*, bersuara dan tidak bersuara, guna transmitter sederhana sangat terbatas. Pesan yang dikirim melalui transmitter ini harus ditranslasikan menggunakan kode yang berbasis suara dan tidak bersuara seperti kode morse, ASCII encoding, dan lain sebagainya.

4. Komunikasi Sinyal Radio Menggunakan Transmitter pada Perang Dunia II

Komunikasi menggunakan sinyal radio pada jaman itu cukup sederhana. Pengirim dan penerima hanya perlu menyamakan frekuensi radio saat pesan itu dikirim dan diterima. Kemudian pengirim hanya perlu mengirim pesan melalui transmiter sederhana. Pesan akan dikirim melalui sinyal radio yang diterima oleh penerima dengan alat penerima sinyal radio.

Gambar 5 : Transmitter dan Reciever Radio Pada Perang Dunia II
Sumber : https://www.radioblvd.com/

Transmitter yang digunakan pada perang oleh Jerman Nazi untuk pesan yang bersifat rahasia menggunakan transmitter sederhana yang hanya dapat mengirimkan signal on-off, yang diterjemahkan menggunkan kode morse.

Pesan yang telah di terjemahkan dari kode morse kemudian harus didekripsikan menjadi pesan yang memiliki arti menggunakan mesin enigma.

5. Kriptografi pada Perang Dunia II

Kriptografi adalah ilmu yang mempelajari mengenai cara mengamankan pesan dari sadapan menggunakan kode rahasia dan juga ilmu yang mempelajari cara memecahkan kode rahasia untuk mendapatkan pesan asli. Kriptografi memiliki peran penting dalam perang dunia II. Dengan kriptografi, perang dunia II dapat dipersingkat dengan cukup banyak. [3]

Pada perang dunia II, setiap negara memiliki metode kriptografinya masing-masing. Salah satu metode kriptografi yang paling terkenal adalah oleh Jerman Nazi. Jerman Nazi menggunakan mesin enigma untuk meng-enkripsi pesan-pesan mereka. Metode ini sangat ampuh, dimana pihak sekutu mengalami kekalahan besar karena pesan mesin enigma tidak dapat dipecahkan oleh pihak sekutu. Di tengah perperangan, seorang matematikawan bertekad untuk membantu negaranya untuk menyelesaikan masalah enigma. Ia mendesain sebuah mesin yang mampu memecahkan mesin enigma. Mesin ini kemudian dinamakan *Bombe Machine*, dimana menjadi inpsirasi dasar pengembangan komputer.

6. Mesin Enigma

Mesin enigma merupakan mesin *cipher* yang dikembangkan untuk keperluan perang, politik dan komunikasi. Mesin ini sangat banyak digunakan oleh Jerman Nazi untuk mengirimkan pesan diantara militernya. Pada masa itu, mesin enigma dianggap sangat amat hingga digunakan untuk enkripsi pesan paling rahasia.

Mesin enigma memilikli mekanisme rotor elektromekanikal yang mengacak setiap huruf yang diinput. Pengirim pesan meng-*input* satu per satu alfabet yang ingin dikirimkan dan untuk setiap huruf akan menyala salah satu alfabet. Alfabet yang menyala merupakan *ciphertext* yang akan dikirimkan kepada penerima pesan.

Gambar 6 : Mesin Enigma
Sumber : https://www.tnmoc.org/bh-2-the-enigma-machine

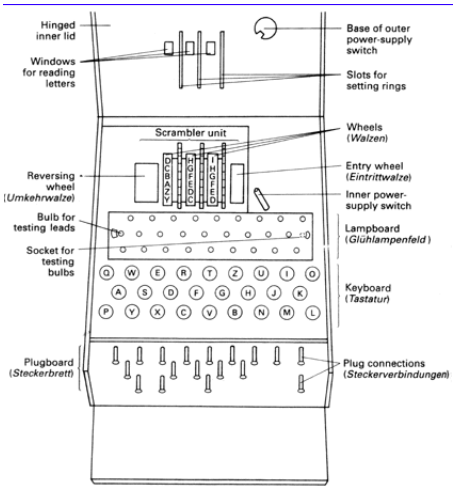
Agar penerima pesan dapat mengubah *ciphertext* kembali menjadi *plaintext*, diperlukan konfigurasi mesin yang digunakan untuk enkripsi. Oleh karena itu, diperlukan kesetujuan kedua pihak dalam konfigurasi mesin. Untuk dekripsi, gunakan konfigurasi mesin yang benar, dan kemudian meng-*input* *ciphertext*. Huruf yang menyala pada mesin merupakan *plaintext* yang dapat dimengerti. Tanpa konfigurasi yang benar, *plainext* yang diterima tidak akan menghasilkan arti yang bermakna.

Dari penjelasan sebelumnya, dapat diamati bahwa mesin enigma melakukan proses enkripsi-kriptografi dengan menggunakan prinsip kombinatorika. Jumlah konfigurasi yang banyak menyebabkan penyadap berkesusahan untuk mendekripsi pesan yang disampaikan.

III. Analisis Penerapan Kombinatorika Dalam Mesin Enigma

A. *Kombinatorika dan Mesin Enigma*

Mesin enigma menjadi salah satu alat enkripsi yang paling terkenal karena proses enkripsi tidak menghasilkan pola sama sekali. Karena tidak adanya pola tersebut, orang-orang pada jaman itu menganggap pesan yang dienkripsikan oleh mesin enigma tidak dapat dipecahkan oleh tangan manusia.



Gambar 7 : Diagram Bagian-Bagian Mesin Enigma
Sumber : https://www.pbs.org/wgbh/nova/decoding/enigmadiagram.html

Ketidakmunculan pola tersebut dikarenakan bagian-bagian yang dimiliki oleh mesin enigma tersebut. Dua bagian yang paling berperan dalam proses enkripsi adalah rotor dan *plugboard* pada bagian depan mesin.

Bagian scrambler unit pada mesin enigma merupakan lapisan pertama dalam mekanisme elektromekanikal di dalamnya. Ketika suatu tombol huruf pada keyboard ditekan, akan ada aliran listrik melewati plug connections menuju Scrambler unit. Aliran listrik ini terhubung atau ditenagai oleh sumber listrik atau baterai yang ada di dalam mesin.

Scrambler unit pada mesin enigma merupakan bagian rotor yang telah disebutkan sebelumnya. Scrambler unit terdiri dari 3 rotor. Masing-masing rotor memiliki 26 gerigi atau 26 *state*. Tiap gerigi ini terhubung pada 26 huruf berbeda, dimana ketiga gerigi ini dapat masing-masing mengubah atau mengenkripsi huruf yang di-*input*.

Agar penerima pesan dapat mendekripsi *ciphertext* yang diterima, ia harus memiliki konfigurasi 3 rotor awal yang digunakan oleh pengirim pesan sebelum pesan dienkripsi. Contohnya, saat pengirim pesan mulai mengenkripsi suatu pesan pada konfigurasi rotor 3-13-17, maka untuk mengdekripsi pesan tersebut, sang penerima pesan harus mengondisikan rotor pada mesinnya sendiri menjadi 3-13-17.

Untuk scrambler unit, disediakan 5 rotor yang dapat disisipkan pada 3 tempat rotor. Dari informasi yang tersedia, dapat dihitung jumlah konfigurasi yang mungkin untuk scrambler unit sendiri.

$$N(Scrambler) = P(5,3) \times 26 \times 26 \times 26$$
$$N(Scrambler) = 60 \times 26 \times 26 \times 26$$
$$N(Scrambler) = 1\,054\,560$$

Dari scrambling unit sendiri, terdapat sejuta konfigurasi yang mungkin, namun pendesain mesin enigma ingin membuat proses enkripsi menjadi semakin aman. Oleh karena itu, mereka mendesain plugboard yang ada didepan mesin.

Konsep kerja plugboard sangat sederhana. Mesin enigma menyediakan 10 kabel yang dapat menghubungkan dua huruf. Setiap kabel menghubungkan satu tombol input dari keyboard menuju suatu huruf lain sebelum dilanjutkan ke scrambler unit.

Bagian yang membuat plugboard menjadi hal yang rumit

adalah banyaknya konfigurasi 10 kabel pada 26 plughole huruf yang disediakan. Dari informasi yang tersedia, dapat dihitung banyaknya konfigurasi yang mungkin untuk plugboard sendiri.

$$N(Plugboard) = \frac{26!}{6!\,10!\,2^{10}}$$

$$N(Plugboard) = 150\,738\,274\,937\,250$$

Dapat dilihat bahwa bagian *plugboard* ini memiliki konfigurasi yang banyaknya 150 juta kali lipat konfigurasi pada scrambling unit sendiri.

Karena aliran listrik berjalan dari keyboard menuju plugboard, kemudian scrambler unit dan akhirnya pada display, maka untuk menghitung jumlah konfigurasi yang mungkin pada mesin enigma menggunakan *rule of product*.

$$N(Enigma) = N(Scrambler) \times N(Enigma)$$
$$N(Enigma) = 150\,738\,274\,937\,250 \times 1\,054\,560$$

$$N(Enigma) = 158\,962\,555\,217\,826\,360\,000$$
$$N(Enigma) \approx 1{,}59 \times 10^{20}$$

Informasi konfigurasi rotor dan *plugboard* yang digunakan oleh Jerman Nazi pada hari tertentu disebarkan dengan pamflet untuk sekte komunikasi. Pamflet ini berisi konfigurasi rotor dan *plugboard* untuk setiap hari untuk sebulan. Dikarenakan pihak sekutu berkesusahan untuk mendapatkan pamflet ini dan informasi yang ada hanya berlaku untuk sebulan, pihak sekutu pun susah mendekripsi informasi militer dari Jerman Nazi.

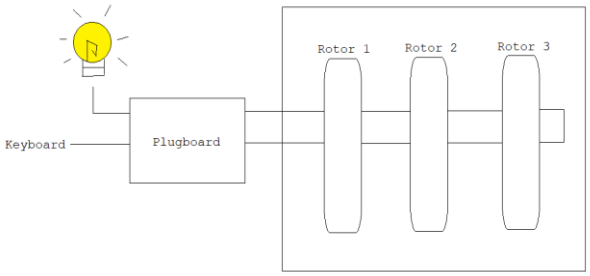
Jumlah konfigurasi yang ada untuk mesin enigma, dianggap tidak mungkin untuk mendekripsikan suatu pesan oleh tangan manusia sendiri. Oleh karena itu, mesin enigma dianggap mesin paling aman untuk mengenkripsikan suatu pesan pada jaman tersebut.

B. Kelemahan pada Mesin Enigma

Seperti yang sudah dijelaskan sebelumnya, mesin enigma memiliki 1,59 x 10^{20} konfigurasi mesin yang mungkin. Angka tersebut sangat besar, dimana siapapun yang memiliki logika dapat mengatakan bahwa mesin enigma tidak dapat dipecahkan dengan tangan. Namun, setelah ditelusuri, mesin enigma memiliki satu pola yang berakibat fatal.

Pola yang sedang yang disebut adalah mesin enigma tidak pernah mengenkripsi suatu huruf menjadi huruf tersebut lagi. Dengan informasi tersebut, pihak sekutu dapat menebak konfigurasi yang mungkin digunakan pada saat itu.

Seperti yang dijelaskan sebelumnya, listrik yang berjalan bermula dari keyboard ke plugboard, kemudian ke scrambler unit. Dalam scrambler unit, listrik bergerak dari rotor 1, rotor 2 dan rotor 3, kemudian kembali lagi dari rotor 3, rotor 2 dan rotor 1. Jadi, dalam scrambler unit ini, *input* keyboard berubah sebanyak 6 kali.



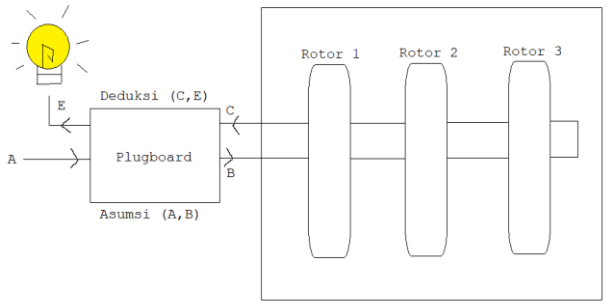
Gambar 8 : Contoh Aliran Listrik Pada Mesin Enigma

Jika kita abaikan bagian scrambler unit, dapat diamati bahwa setiap kali proses enkripsi terdapat 2 koneksi di bagian *plugboard*.

Dengan informasi bahwa setiap input tidak dapat menghasilkan dirinya, pihak sekutu dapat menebak suatu frasa yang mungkin pada suatu pesan dan mencari suatu string yang cocok (*plaintext* dan *ciphertext* tidak memiliki huruf yang sama untuk urutan yang sama).

Dari string tersebut dapat dilakukan penebakan dengan kontradiksi. Misalkan setelah ditebak frasa dan dapat string yang mungkin, kita dapat mengetahui bahwa pada string tersebut huruf A menghasilkan huruf E.

Proses deduksinya dari menganggap *plug* A terhubung pada *plug* huruf lain, misalkan B, dan menganggap bahwa rotor pada posisi 1-1-1. Kita bisa mencari tahu *output* jika *input* B, dengan meng-*input* B pada mesin enigma dengan posisi 1-1-1 tanpa adanya *plugboard* yang tercolok (Tidak ada kabel yang digunakan). Misalkan *input* B menghasilkan *output* C. Dari *output* yang didapatkan, dapat dideduksi bahwa ada dua plug yang tercolok, yaitu (A, B) dan (C, E).



Gambar 9 : Ilustrasi Deduksi berdasarkan Asumsi

Kontradiksi dapat muncul dalam proses ini apabila terdapat suatu huruf yang tercolok dengan dua kabel. Contohnya (A, B) dan (B, F). Ini dikarenakan setiap huruf hanya memiliki satu lubang colokan.

Proses ini dilakukan sampai frasa selesai atau menemukan kontradiksi. Jika frasa selesai, maka konfigurasi yang digunakan sudah benar. Jika bertemu kontradiksi, maka proses ulangi dari awal, dengan asumsi yang bahwa A dengan huruf yang lain (Uji dari B sampai Z) dan uji juga jika A tidak tercolok kabel. Jika semua kasus tersebut tidak lolos uji, maka ulangi semua proses dengan konfigurasi rotor yang berbeda.

Seorang Matematikawan Inggris, Alan Turing, menemukan kelemahan ini, dan mencoba menggunakannya untuk membangun *Bombe Machine*. Mesin ini dapat melakukan semua proses yang telah disebutkan dengan menggunakan aliran listrik. Dengan bantuan aliran listrik, proses uji konfigurasi *plugboard*

yang berbeda dapat dilakukan secara langsung. Jadi, mesin ini dapat menguji semua konfigurasi rotor dalam waktu 20 menit.

Semua proses ini dapat terjadi karena informasi bahwa enigma tidak dapat mengembalikan huruf yang sama dan fungsi rotor yang dapat diuji.

C. Kriptografi yang Aman

Seperti yang telah dibahas semua, kelemahan pada mesin enigma terdapat pada adanya konsistensi mesin untuk tidak mengenkripsikan suatu huruf menjadi huruf yang sama. Hal tersebut mengakibatkan adanya ruang untuk melakukan deduksi konfigurasi yang digunakan mesin.

Agar proses kriptografi dengan metode mesin enigma menjadi aman, perlu dihilangkan fitur enigma ini. Kelemahan ini terbukti dapat diselesaikan dengan adanya mesin *TypeX* yang didesain oleh negara Inggris.

IV. Simpulan

Komunikasi dan informasi merupakan kunci dalam memenangkan perperangan. Dengan bantuan kriptografi yang memadai, suatu pihak dapat menyalurkan informasi penting kepada sesamanya tanpa perlu menghawatirkan adanya penyadapan dari musuh. Kriptografi menggunakan prinsip kombinatorika merupakan salah satu jenis kriptografi yang paling sederhana. Dengan bantuan ilmu kelistrikan, dapat dihasilkan mesin enkripsi-dekripsi yang luar biasa seperti mesin Enigma. Namun, jika adanya pola yang muncul dalam hasil enkripsi makan ada kemungkinan bahwa akan ada solusi untuk memecahkan hasil enkripsi tersebut. Perlu diperhatikan bahwa proses enkripsi yang paling efektif adalah dimana hasil enkripsi yang 100% *random*. Proses enkripsi sudah berkembang jauh. Proses enkripsi-dekripsi dalam keseharian kita sudah sangat aman dengan adanya algoritma RSA-CRT. Namun kita harus tetap waspada dan tetap mengembangkan proses enkripsi karena proses RSA-CRT masih memiliki kelemahannya sendiri.

V. Ucapan Terima Kasih

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena dengan rahmat dan berkat-Nya, penulis dapat menyelesaikan makalah ini dengan baik. Penulis ingin mengucapkan terima kasih kepada kedua orang tua penulis karena sudah mendukung penulis selama masa penyusunan makalah ini. Penulis juga ingin mengucapkan terima kasih kepada Dr. Nur Ulfa Maulidevi, S.T., M.Sc. selaku dosen K1 mata kuliah IF2120 Matematika Diskrit 2022 yang sudah mengajari penulis mengenai dasar dari kombinatorika dan kriptografi sehingga penulis memiliki ide mengenai makalah ini. Penulis juga ingin berterima kasih kepada algoritma referensi google dan youtube yang sudah memberikan referensi mengenai kriptografi selama perang dunia II sehingga penulis berkesempatan untuk mempelajari mengenai kriptografi selama perang dunia II dengan lebih mendalam.

References

[1] Prasad, Kalika 2020. "A Review On Mathematical Strength and Analysis of Enigma", https://arxiv.org/pdf/2004.09982.pdf, di akses 26 November 2022

[2] Nur, Levy Olivia. 2018. "Kriptografi", https://slideplayer.info/slide/14242369/, diakses 26 November 2022

[3] Dr. Dough Lantry, "War of Secrets: Cryptology in WWII", https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/FactSheets/Display/Article/196193/war-of-secrets-cryptology-in-wwii/ , diakses 26 November 2022

[4] Numberphile, "Flaw in the Enigma Code", https://www.youtube.com/watch?v=V4V2bpZlqx8&ab_channel=Numberphile , diakses 26 November 2022

[5] Cryptomuseum, "Typex", https://www.cryptomuseum.com/crypto/uk/typex/index.htm, diakses 26 November 2022

[6] Cryptomusem, "Enigma cipher machines", https://www.cryptomuseum.com/crypto/enigma/index.htm , diakses 26 November 2022

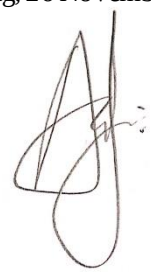
[7] Munir, Rinaldi. 2022. "Kombinatorial (Bagian 1)", https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Kombinatorial-2020-Bagian1.pdf , diakses 26 November 2022

[8] Munir, Rinaldi. 2022. https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Kombinatorial-2020-Bagian2.pdf ,diakses 26 November 2022

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 November 2022



Alex Sander 13521061