Analisis Kombinatorial pada Mesin Enigma

Rizky Elzandi Barik/13515030
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515030@std.stei.itb.ac.id
rizkyebarik@gmail.com

***Abstrak*— Mesin Enigma adalah sebuah mesin pembuat sandi yang berasal dari Jerman. Sandi dihasilkan oleh huruf yang diacak karena susunan rotor dan *plugboard*. Kekuatan sandi dapat dianalisa dengan kaidah-kaidah kombinatorial. Dengan menghitung seluruh kemungkinan konfigurasi pada rotor dan *plugboard*, kita akan mampu menghitung berapa banyak konfigurasi berbeda pada sebuah mesin Enigma. Meskipun begitu, ilmuwan di Bletchley Park berhasil menemukan celah pada mesin Enigma dan memanfaatkannya untuk mempersingkat Perang Dunia II.**

***Keywords*— Enigma, kombinatorial, konfigurasi, Mesin Bombe**

I. PENDAHULUAN

Mesin Enigma adalah sebuah mesin pembuat sandi yang berasal dari Jerman. Penggunaan mesin ini beragam, mulai dari mengamankan data komersial, diplomatik, hingga sandi-sandi militer.

Kerumitan sandi yang dihasilkan oleh mesin ini disebabkan oleh susunan dalam mesin enigma. Mesin enigma yang digunakan oleh militer Nazi Jerman menggunakan kombinasi antara rotor dan *plugboard (Steckerbrett)* dalam mengenkripsi kata-kata input menjadi sandi. Untuk mendekripsi, dibutuhkan mesin enigma yang sama dengan konfigurasi rotor dan *plugboard* yang sama pula.

Gambar 1. Mesin Enigma Model Wehrmacht Menggunakan 3 rotor
Sumber: http://users.telenet.be/d.rijmenants/pics/hires-wehr3.jpg

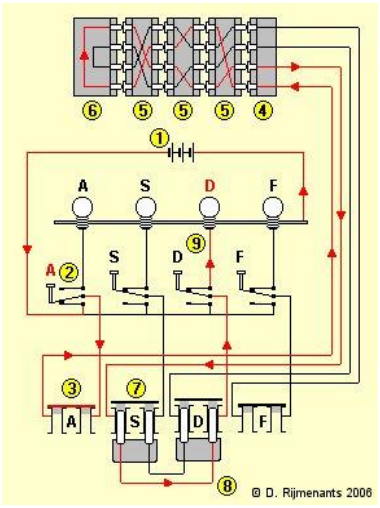
Pada masa Perang Dunia II, Nazi Jerman menggunakan mesin Enigma untuk berkomunikasi jarak jauh. Komando militer yang diubah melah menjadi sandi dengan mesin Enigma dikirim dalam sandi morse menuju pangkalan perang dan kapal-kapal perang Jerman. Pesan-pesan elektronik dapat disadap oleh pihak sekutu, namun tidak bisa dipecahkan karena pihak sekutu tidak mengetahui konfigurasi mesin Enigma yang digunakan oleh pihak Nazi Jerman pada hari itu. Padahal, konfigurasi tersebut berubah setiap harinya. Beruntunglah, para ilmuwan Inggris yang dikarantina di Bletchley Park (Pinggir Kota Milton-Keynes) berhasil membuat mesin bombe untuk memecahkan konfigurasi mesin Enigma yang digunakan pada suatu hari [1].

Kepopuleran mesin enigma pada akhir-akhir ini disebabkan oleh film Hollywood "The Imitation Game", serta penggunaan kata "Enigma" sendiri sebagai nama angkatan HMIF ITB angkatan 2015.

II. PRINSIP KERJA MESIN ENIGMA

Seperti yang telah dijelaskan pada Bab I, sandi dihasilkan oleh huruf yang diacak karena susunan rotor dan *plugboard*. Sinyal dari *keyboard* akan dialirkan melalui sirkuit menuju lampu bohlam yang mewakili huruf-huruf.

Sebelum dapat digunakan, kedua belah pihak yang ingin berkomunikasi harus menggunakan jenis mesin Enigma yang sama dengan konfigurasi yang sama pula. Konfigurasi pada rotor akan berubah setiap pengguna menekan tombol pada *keyboard*. Setiap kali tombol ditekan, rotor paling kanan akan bergerak sekali. Rotor yang berada di tengah akan bergerak setelah rotor kanan bergerak sebanyak 26 kali. Sedangkan rotor kiri akan bergerak sekali tiap rotor tengah bergerak sebanyak 26 kali. Prinsip kerja rotor ini dapat diumpamakan seperti jarum detik, menit, dan jam pada jam analog.



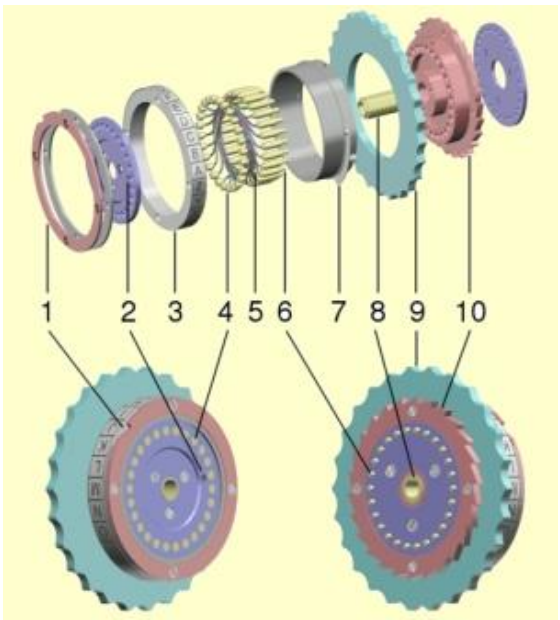
Gambar 2. Sirkuit dalam Mesin Enigma
Sumber: http://users.telenet.be/d.rijmenants/pics/wiring.jpg

Sesuai pada gambar 3, sinyal dari *keyboard* akan dialirkan menuju *plugboard* dan diteruskan menuju rotor. Rotor-rotor akan mengacak sinyal listrik menjadi huruf lain bergantung pada konfigurasi yang digunakan. Sinyal yang masuk melalui tiga buah rotor akan dikembalikan melalui reflektor dan melewati tiga rotor lagi. Setelah keluar dari rotor, sinyal akan menuju *plugboard*. Pada gambar, huruf S dan D terhubung pada *plugboard*. Sinyal yang masuk menuju *plugboard* S akan keluar melalui *plugboard* D dan menyalakan lampu huruf D. Sehingga, pada proses kali ini, huruf A dienkripsi menjadi huruf D [2].

A. *Rotor*

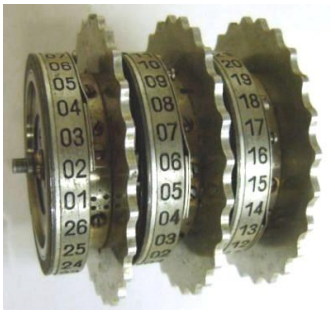
Gambar 3. Letak rotor pada mesin Enigma
Sumber: https://www.youtube.com/watch?v=G2_Q9FoD-oQ

Rotor (atau *walzen* dalam Bahasa Jerman) adalah unsur terpenting dalam mesin Enigma. Pada model *Wehrmacht*, satu set mesin Enigma memiliki 5 jenis rotor yang dinomori dengan angka romawi I-V. Pengguna harus memilih 3 (4 untuk model *Kriegsmarine*) dari 5 buah (8 untuk model *Kriegsmarine*) set rotor untuk dipasangkan pada mesin Enigma yang akan digunakan.



Gambar 4. Struktur dalam rotor
Sumber: users.telenet.be/d.rijmenants/pics/enigmarotorintern.jpg

Tiap rotor memiliki 26 buah takik. Masing-masing takik mewakili satu huruf dalam abjad. Di dalam rotor, terdapat sambungan kawat yang acak (ditunjukkan pada nomor 5 pada gambar 4) yang menyebabkan huruf-huruf input berubah menjadi sandi. Secara keseluruhan, huruf akan mengalami pengacakan sebanyak 7 kali, yaitu 3 kali saat memasuki rotor, 1 kali saat melewati reflektor, dan 3 kali saat keluar dari rotor.



Gambar 4. 3 set Rotor model Wehrmacht
Sumber: http://users.telenet.be/d.rijmenants/pics/wehr3rotors.jpg

B. *Plugboard*

Plugboard (atau *Steckerbrett* dalam Bahasa Jerman) menjadi salah satu fitur mesin Enigma pertama kali pada tahun 1930 pada mesin Enigma model *Wehrmacht* pertama. Fitur ini menjadi pembeda dengan mesin Enigma yang dijual kepada masyarakat sipil untuk digunakan secara komersil. Pada model ini, set mesin Enigma dilengkapi dengan 10 buah kabel. Kombinasi dalam pemasangan kabel pada *plugboard* menyebabkan banyak cara untuk membuat konfigurasi yang berbeda pada mesin Enigma menjadi sangat besar.

Gambar 6. *Plugboard* pada bagian depan mesin Enigma model *Wehrmacht*
Sumber: http://users.telenet.be/d.rijmenants/pics/hires-wehrplugs.jpg

Tanpa kabel yang dipasangkan, arus dari *keyboard* akan langsung menuju rotor dan diteruskan menuju lampu. Sedangkan, dengan memasang kabel, arus dari *keyboard* akan menuju *plugboard*, lalu akan berubah menjadi huruf lain, bergantung pada pasangan huruf tersebut pada *plugboard*, dan diteruskan menuju rotor. Dari rotor, arus akan melewati plugboard sekali lagi dan akan berubah menjadi huruf lain lagi jika kabel dipasangkan pada huruf yang dilewati arus tersebut. Jika kabel tidak dipasang, arus listrik akan langsung diteruskan menuju bohlam.

III. DASAR-DASAR TEORI KOMBINATORIAL

Kombinatorial adalah cabang matematika yang memelajari enumerasi, kombinasi dan permutasi dari himpunan dari elemen-elemen dan relasi matematika yang tanpa mengenumerasi semua kemungkinannya [3]. Salah satu penerapan ilmu kombinatorial adalah dalam mengetahui kekuatan suatu sandi.

A. Kaidah Penjumlahan dan Kaidah Perkalian

Terdapat dua kaidah mendasar yang digunakan dalam ilmu kombinatorial, yaitu kaidah penjumlahan dan kaidah perkalian.

Misalkan, jika ada n buah cara untuk melakukan suatu hal dan m buah cara untuk melakukan suatu hal yang lain, dan dua aksi tersebut tidak dilakukan secara bersamaan, maka terdapat n + m cara untuk melakukan aksi tersebut. Ini disebut kaidah penjumlahan.

Sedangkan, jika ada n buah cara untuk melakukan suatu hal dan m buah cara untuk melakukan suatu hal yang lain, dan dua aksi tersebut dilakukan secara berurutan, maka terdapat n × m cara untuk melakukan aksi tersebut. Ini disebut kaidah perkalian.

Contoh, Andi ingin pergi dari ITB ke Surabaya dengan pesawat terbang. Untuk pergi dari ITB menuju bandar udara, Andi dapat menggunakan 2 buah jenis angkutan kota atau 3 buah jenis bus kota. Sedangkan untuk pergi dari bandar udara Bandung menuju Surabaya, Andi dapat memilih 3 buah jenis penerbangan ekonomi atau 2 buah jenis penerbangan eksekutif.

Dengan kaidah penjumlahan, banyak cara Andi untuk dapat menuju bandar udara dari ITB adalah 5 cara yang diperoleh dari 3 jenis angkutan kota ditambah dengan 2 jenis bus. Sedangkan banyak cara memilih penerbangan dari Bandung ke Surabaya adalah 5, yang diperoleh dari 3 buah jenis penerbangan ekonomi ditambah 2 jenis penerbangan eksekuitf. Jadi, banyak cara Andi untuk pergi dari ITB menuju Surabaya adalah 25 cara dengan kaidah perkalian (diperoleh dari 5 buah cara untuk menuju bandar udara dari ITB lalu dikali 5 buah cara untuk memilih jenis penerbangan dari Bandung menuju Surabaya)[4].

B. Permutasi dan Kombinasi

Permutasi adalah banyak cara mengatur sesuatu dengan memertimbangkan urutan penyusunannya. Permutasi adalah bentuk khusus dari aturan perkalian.

Contoh, banyaknya cara menata buku sejarah, matematika, biologi, dan fisika pada rak buku. Maka, banyak cara untuk menata buku-buku tersebut adalah 4 × 3 × 2 × 1 atau 4! = 24 cara.

Penerapan permutasi pada tingkat yang lebih rumit adalah permutasi r dari n elemen. Misalkan, kita memiliki n buah bola. Permutasi r dari n elemen adalah banyaknya cara memilih n buah bola yang berbeda untuk dimasukkan ke dalam r buah kotak (dalam kasus ini, r ≤ n). Dengan demikian, banyaknya cara untuk memilih n buah bola yang berbeda adalah n(n-1)(n-2)…(n-(r-1)) atau $\frac{n!}{(n-r)!}$. Operasi permutasi r dari n elemen biasanya dituliskan sebagai P(n,r).

Kombinasi adalah bentuk khusus dari permutasi. Jika pada permutasi, urutan dalam penyusunan elemen diperhitungkan, sebaliknya, urutan penyusunan elemen diperhitungkan dalam kombinasi.

Contoh, jika kita memiliki r buah bola yang identik, maka kombinasi r dari n elemen (C(n,r)) adalah banyaknya cara untuk memasukkan bola-bola tersebut ke dalam n buah kotak. Banyaknya cara untuk memasukkan bola-bola tersebut ke dalam kotak adalah $C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{r! \times (n-r)!}$ [5].

IV. ANALISIS KOMBINATORIAL MESIN ENIGMA

Dengan menghitung seluruh kemungkinan konfigurasi pada rotor dan *plugboard*, kita akan mampu menghitung berapa banyak konfigurasi berbeda pada sebuah mesin Enigma model *Wehrmacht*.

Pertama-tama, kita menghitung banyak cara untuk memilih 3 rotor dari 5 rotor. Yaitu P(5,3) = 5 × 4 × 3 = 60 cara.

Selanjutnya, kita menghitung berapa banyak konfigurasi rotor. Tiap rotor memiliki 26 takik. Jadi, berdasarkan kaidah perkalian, dari 3 rotor, kita memiliki sebanyak 26 × 26 × 26 = 17576 cara pemasangan.

Terakhir, kita menghitung berapa banyak cara untuk memasangkan 10 buah kabel pada 26 steker yang ada pada *plugboard*. Misal kita memiliki 1 buah kabel, maka banyak cara untuk memasang kabel tersebut adalah (26x25)/(1!x2^1). (26x25) didapat dari cara memilih sebuah steker dan sebuah steker lain untuk dipasangkan kabel. 1! didapat karena urutan untuk memilih pemasangan kabel tidak berpengaruh. Sedangkan 2^1 didapat karena pemasangan A-B atau B-A tidak berpengaruh pada sandi. Jadi, setiap ada sebuah pemasangan kabel, akan ada pembagi sebesar 2 kali sebanyak kabel yang dipasang, atau sebanyak 2^n. Sekarang, misalkan kita punya dua buah kabel, maka banyak cara untuk memasangkan kabel adalah $\frac{26 \times 25 \times 24 \times 23}{2! \times 2^2}$ cara. Sehingga, banyak cara untuk memasangkan n buah kabel pada *plugboard* mesin enigma adalah $\frac{26!}{(26-2n)! \times n! \times 2^n}$ cara. Jadi, jika kita memiliki 10 buah kabel, maka banyak cara untuk memasangkan kabel-kabel tersebut pada plugboard adalah $\frac{26!}{6! \times 10! \times 2^{10}}$ = 150.738.274.937.250 cara [2].

Dengan kaidah perkalian, maka banyaknya konfigurasi rotor dan *plugboard* adalah $60 \times 17.576 \times 150.738.274.937.250 = 158.962.555.217.826.360.000$ (atau $1{,}59 \times 10^{20}$) cara.

V. CELAH PADA MESIN ENIGMA

Pada tahun 1933, intelijen Polandia berhasil mendapatkan mesin enigma versi militer dengan bantuan orang dalam kantor sandi Jerman yang sedang

membutuhkan uang. Pada tahun 1939, Polandia memberikan replika mesin Enigma kepada militer Inggris dan Prancis. Dengan begitu, pihak sekutu dapat mempelajari cara kerja mesin Enigma agar dapat memecahkan sandi Enigma dengan cepat[1]. Sejarahwan memprediksi, dengan dipecahkannya Enigma, Perang Dunia II dipersingkat hingga 2 tahun dan menyelamatkan sekitar 14 juta jiwa manusia.

A. Celah pada Mesin Enigma

Keunggulan mesin Enigma adalah, pengacakan huruf akan berubah setiap kita menekan tombol. Kita tidak akan pernah tahu huruf apa yang akan muncul setiap kita menekan tombol, kecuali kita mengetahui susunan pengacakan pada internal rotor dan susunan kabel pada *plugboard*. Dua huruf yang sama berurutan (contohnya pada kata 'wasser') tidak akan menghasilkan sandi yang mengandung dua huruf yang sama berurutan, tidak seperti yang terjadi pada *Caesar's Cipher*.

Namun, kekurangan mesin enigma adalah, huruf input tidak akan dienkripsi menjadi huruf itu sendiri. Hal ini cukup mempersempit ruang pencarian sehingga memudahkan para ilmuwan yang bekerja di Bletchley Park.

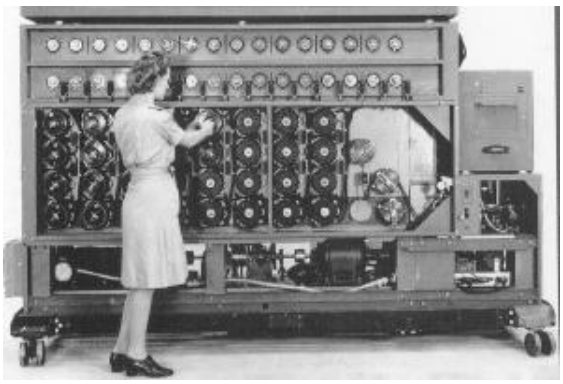
B. Memecahkan Sandi Enigma

Setiap pukul 6 pagi, militer Jerman akan mengirimkan pesan. Tiap pesan akan diawali dengan berita cuaca. Berita tersebut merupakan format harian dalam mengirimkan sandi enigma melalui radio.

Dengan menyadap sandi enigma, para ilmuwan di Bletchley Park akan mencari frasa yang kemungkinan menjadi kata-kata seperti "laporan cuaca" atau "Heil Hitler" pada deretan sandi yang diperoleh. Dengan memanfaatkan kelemahan enigma, yaitu, huruf tidak akan dienkripsi menjadi dirinya sendiri, para ilmuwan akan mencoba mencari kata 'Heil Hitler', yang biasa berada pada akhir tiap pesan, pada sandi yang telah dienkripsi. Setelah itu, para ilmuwan akan mencoba satu per satu kemungkinan hubungan kabel pada *plugboard*. Jika semua kemungkinan pada plugboard tidak cocok, maka percobaan yang sama akan dilakukan dengan mencoba konfigurasi rotor yang berbeda hingga mengganti dengan rotor nomor lain, dengan banyak cara untuk memilih seluruh konfigurasi rotor dan pemilihan rotor adalah $60 \times 17576 = 1.054.560$ cara.

Tentu saja algoritma *Brute Force* seperti ini akan memakan waktu yang sangat lama jika dilakukan dengan kertas dan pensil. Oleh karena itu, matematikawan Inggris, Alan Turing membangun sebuah mesin yang bernama mesin Bombe untuk mengotomasi proses *Brute Force* tersebut.

Langkah pertama dalam algoritma Brute Force ini adalah dengan mengasumsikan sebuah sambungan kabel pada *plugboard*, misal A-B. Karena kita telah mengetahui susunan dari tiap rotor, kita akan tahu huruf apa akan dienkripsi menjadi apa. Setelah itu, kita akan mengenumerasi seluruh sambungan kabel yang lain yang diakibatkan oleh pemasangan kabel pada A-B. Kita akan melakukan hal tersebut hingga seluruh frasa yang kita gunakan cocok dengan sandi yang muncul atau hingga muncul sebuah kontradiksi. Kontradiksi yang dimaksud adalah apabila sambungan kabel pada A-B mengakibatkan sambungan lain misal T-A. Hal ini disebut kontradiksi karena A tidak mungkin tersambung dengan B dan T secara bersamaan. Jika muncul kontradiksi seperti itu, maka kita akan mencoba sambungan kabel lainnya, misal A-C.



Gambar 7. Mesin Bombe
Sumber: users.telenet.be/d.rijmenants/pics/enigmarotorintern.jpg

Alan Turing berhasil menemukan sesuatu yang mempercepat kerja mesin Bombe. Yaitu, jika kita menemukan kontradiksi, maka seluruh hasil deduksi kita atas kemungkinan sambungan kabel-kabel yang diakibatkan oleh sambungan kita pada A-B sebelumnya akan salah. Dengan kata lain, sambungan-sambungan tersebut dieliminasi dari kemungkinan. Sehingga, jika kita menemukan sambungan yang sama pada percobaan-percobaan setelahnya, maka kita akan beralih untuk mencoba dengan sambungan selanjutnya.

Dengan digunakannya mesin Bombe, tiap percobaan dapat dilakukan secepat putaran rotor-rotor pada mesin bombe. Dengan mesin Bombe, sandi enigma mampu dipecahkan dalam waktu kurang dari 20 menit setiap pagi[6].

Komandan U-Boat Jerman, Karl Donitz tidak selalu menggunakan mesin enigma yang sama. Dia berulang kali memperbarui spesifikasi mesin enigma yang digunakan agar sandi-sandi yang dikirim lebih sulit dipecahkan. Terkadang, mesin bombe yang sama tidak dapat memecahkan sandi pada mesin Enigma yang baru. Namun tidak cukup di situ, sandi-sandi yang dikirim juga dienkripsi lagi dengan metode-metode lain yang ditulis dalam sebuah buku. Sebab, operasi militer yang dilakukan oleh Angkatan Laut Jerman cukup penting, yaitu menghadang kapal-kapal dari Amerika yang membawa logistik untuk kebertahanan Inggris di Perang Dunia II.

Di balik itu, kesuksesan mesin Bombe Alan Turing juga memberi dampak yang besar pada keberjalanan perang. Selain itu, langkah yang dilakukan militer sekutu setelah mengetahui pergerakan Jerman dieksekusi dengan sangat hati-hati agar militer Jerman tidak curiga jika sandi mereka telah dipecahkan. Kelengahan ini yang tidak disadari oleh

militer Jerman. Mereka jatuh di jurang kekalahan tanpa menyadarinya.

VI. KESIMPULAN

Dalam perang, kerahasiaan pesan adalah kunci utama dalam meraih kemenangan. Dengan mengenali kelemahan musuh, kita dapat membuat solusi yang ampuh dalam mengeksploitasi kelemahan musuh tersebut.

Kekuatan sandi merupakan bidang yang menarik di dalam matematika. Bidang ini mungkin akan terus berkembang setiap saat. Tidak hanya dalam perang, keamanan sandi juga penting dalam enkripsi penyaluran informasi di dunia maya, seperti pada layanan pesan instan.

Bidang kekuatan sandi ditunjang oleh salah satu cabang ilmu matematika, yaitu kombinatorial. Dengan menerapkan aturan-aturan pada ilmu kombinatorial, kita dapat menguji kekuatan sandi yang kita gunakan.

VII. UCAPAN TERIMA KASIH

Pertama, syukur yang sebesar-besarnya saya ucapkan kepada Allah SWT. sehingga makalah ini dapat selesai tepat pada waktunya tanpa ada kendala yang berarti. Selanjutnya, terima kasih yang sebanyak-banyaknya saya ucapkan kepada dosen IF2120 Matematika Diskrit saya, Bapak Rinaldi Munir. Dengan bimbingan dan kasih sayang beliau, makalah ini dapat diselesaikan sebagai mana mestinya, berdasarkan apa yang sudah diajarkan selama satu semester perkuliahan. Tak lupa ucapan terima kasih untuk kedua orang tua serta teman-teman saya yang selalu memberi dukungan moral sehingga saya masih dapat menimba ilmu di Teknik Informatika ITB ini.

Tak cukup di sini, masih banyak ilmu yang belum saya dapatkan. Untuk itu, saya harap, makalah pertama saya ini dapat menjadi pembelajaran dalam menimba ilmu dan pembuatan tulisan-tulisan saya selanjutnya.

DAFTAR PUSTAKA

[1] Cryptomuseum.com, History of Enigma, http://www.cryptomuseum.com/crypto/enigma/hist.htm, diakses pada 2 Desember 2016.

[2] Dirk Rijmenants, users.telenet.be, Technical Details of the Enigma Machine, http://users.telenet.be/d.rijmenants/en/enigmatech.htm diakses pada 3 Desember 2016.

[3] Wolfram Mathworld, Combinatorics, http://mathworld.wolfram.com/Combinatorics.html diakses pada 3 Desember 2016.

[4] Brilliant.org, Rule of Sum and Rule of Product, https://brilliant.org/wiki/rule-of-sum-and-rule-of-product-problem-solving/, diakses pada 4 Desember 2016.

[5] Rinaldi Munir, "Diktat Kuliah IF2120 Matematika Diskrit", Program Studi Teknik Informatika ITB, 2006.

[6] Numberphile, Flaw in the Enigma Code, https://www.youtube.com/watch?v=V4V2bpZlqx8, diakses pada 6 Desember 2016

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, 8 Desember 2016

Rizky Elzandi Barik / 13515030