Cipher Perang Dunia Ke-2: Enigma vs Typex dan SIGABA, Perbandingan *Cipher* Kedua Belah Pihak dan Kenapa Engima Dapat Dipecahkan Lebih Dahulu

Raden Prana A. – NIM : 13506105

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16105@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang *cipher* yang digunakan pihak-pihak yang berseteru pada perang dunia ke-2, yaitu Enigma *cipher* milik Jerman, Typex *cipher* milik Inggris, dan SIGABA *cipher* milik Amerika Serikat. Enigma *cipher* adalah suatu bentuk *cipher* yang berbasiskan transposisi, dimana *cipher* tersebut akan mengenkripsi plainteks melalui rangkaian substitusi huruf-huruf yang ada pada plainteks. Enigma *cipher* pada aplikasinya menggunakan bantuan suatu mesin berotor untuk membentuk huruf cipherteks yang berubah-ubah. Typex *cipher* adalah suatu *cipher* yang berprinsip sama dengan Enigma, tapi menggunakan lima rotor (lima kali substitusi) dan tidak menggunakan reflektor pada mesinnya. SIGABA *cipher* juga berprinsip sama dengan kedua *cipher* diatas, namun menggunakan rotor lebih banyak (lebih banyak rangkaian substitusi).

Masing-masing *cipher* menggunakan teknik dasar yang sama dalam proses enkripsi, namun masing-masing *cipher* memiliki kelemahan dan keunggulan masing-masing. Pada akhirnya, Enigma *cipher* milik Jerman dapat dipecahkan terlebih dahulu dibanding kedua *cipher* milik sekutu.

***Kata kunci**:* Enigma *cipher*, Typex *cipher*, SIGABA *cipher*, rotor, transposisi, substitusi, Jerman, Sekutu, Inggris, Amerika, enkripsi, dekripsi.

1. Pendahuluan

Pada perang dunia ke-2, terjadi perang antara pihak Fasis, yang terdiri dari Jerman, Italia, dan Jepang melawan pihak Sekutu, yang dipimpin oleh Amerika Serikat, Inggris dan Uni Soviet. Semua pihak yang terlibat dalam perang tersebut menyadari bahwa pentingnya enkripsi dokumen rahasia dari masin-masing pihak untuk menjaga keutuhan strategi perang mereka. Oleh karena itu, mereka menciptakan mesin *cipher* mereka masing-masing. Pertama, pihak Jerman menggunakan Enigma *cipher*, suatu *cipher* yang diciptakan pada tahun 1918 oleh Arthur Scherbius di Berlin. Prinsip dasar dari Enigma adalah mengenkrip sebuah pesan dengan melakukan sejumlah substitutsi secara beruntun. Scherbius sendiri mengusulkan untuk mencapai substitusi-substitusi tersebut melalui sambungan listrik.

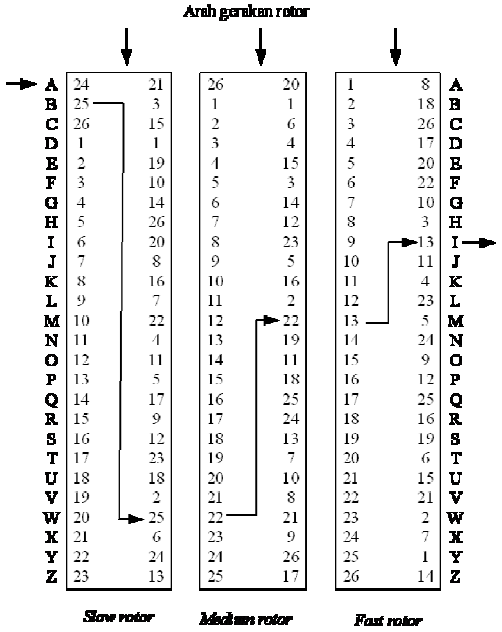
Kedua, pihak Inggris menggunakan Typex *cipher*. Typex *cipher* merupakan adaptasi dari Enigma *cipher* yang mesinnya ada yang tersedia secara komersil. Typex sudah dipakai di Inggris sejak 1937. Seperti Enigma, Typex mengandalkan pergerakan rotor untuk proses subtitusi huruf-huruf pada plainteks. Hanya saja, Typex menggunakan lebih banyak rotor, yaitu lima buah.

Ketiga, pihak Amerika menggunakan SIGABA *cipher*. Mesinnya sering juga disebut ECM Mark II, SIGABA menyerupai Enigma dalam hal penggunaan prinsip dasar enkripsi, dimana terdapat penggunaan rotor untuk mengenkrip tiap karakter pada plainteks menjadi karakter yang berbeda pada cipherteks. Hanya saja, SIGABA memiliki lima belas buah rotor untuk proses enkripsi.

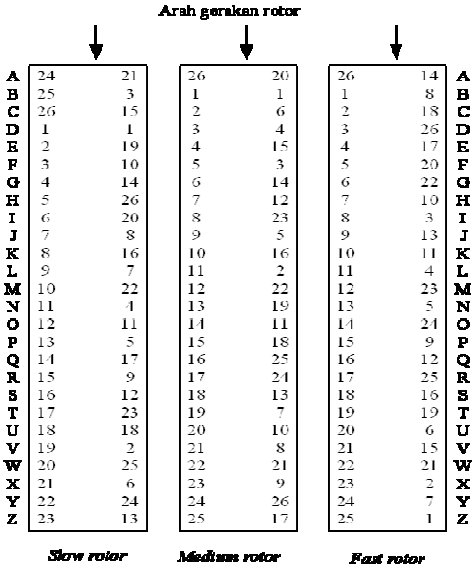
2. Penjelasan Tiap Algoritma

2.1 Enigma *cipher*

Pada Enigma *cipher*, digunakan teknik substitusi huruf berulang. Teknik ini dibantu dengan bantuan rotor sejumlah 3 atau 4 buah yang ada pada mesin Enigma. Hal ini menjelaskan bahwa terdapat 26^3 atau 26^4 kemungkinan huruf cipherteks sebagai pengganti huruf plainteks sebelum terjadi perulangan huruf cipherteks. Setiap kali sebuah huruf selesai disubstitusi, rotor pertama bergeser satu huruf ke atas. Setiap kali rotor pertama selesai bergeser 26 kali, rotor kedua juga melakukan hal yang sama, demikian juga untuk rotor ketiga dan rotor keempat. Contoh, misalkan saat penekanan huruf B pada mesin Enigma:

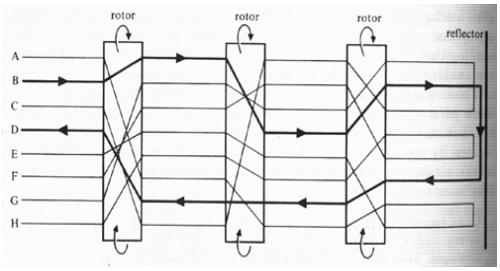


Gambar 1 Kondisi Rotor Pada Penekanan Huruf B



Gambar 2 Posisi Rotor Sesudah Penekanan Huruf B

Pada Enigma yang dipakai Jerman, ada tambahan sebuah reflektor. Reflektor ini dipakai untuk menukar posisi huruf, yaitu dari posisi depan menjadi belakang dan sebaliknya. Dengan menggunakan reflektor ini, Enigma yang digunakan menjadi resiprokal. Misalkan bahwa pada suatu posisi tertentu, huruf A dienkrip menjadi huruf Q, maka pada konfigurasi yang sama, Q akan dienkrip menjadi A. Selain itu, fungsi enkripsi dan dekripsi dapat menggunakan satu alur algoritma yang sama, sehingga tidak memerlukan sebuah fungsi invers.



Gambar 3 Skema Mesin Dengan Reflektor

Dari penjelasan diatas, dapat disimpulkan cara kerja Enigma *cipher* dan mesin Enigma itu sendiri seperti ini:

1. Atur konfigurasi dasar mesin Enigma.
2. Pilih posisi start huruf (terdiri dari 3 huruf), untuk mengenkrip kunci-3-huruf tersebut.
3. Atur rotor pada posisi indikator, kunci pada kunci pesan, lakukan dua kali dan catat lampu mana yang menyala.
4. Atur rotor pada posisi huruf-huruf pada kunci pesan, dan ketikkan pesan yang akan dienkrip

Untuk mendekrip, langkah-langkahnya sebagai berikut:

1. Atur konfigurasi dasar mesin Enigma.
2. Atur rotor pada posisi indikator huruf pada pembukaan pesan.
3. Masukkan enam huruf berikutnya untuk menemukan kunci pesan.
4. Atur rotor pada posisi huruf-huruf kunci. Masukkan cipherteks yang akan didekrip.

2.2 Typex *cipher*

Pada Typex *cipher*, teknik yang digunakan sama dengan Enigma, hanya saja Typex memakai lima buah rotor dan tanpa reflektor. Hal ini mengakibatkan Typex memiliki kemungkinan 26^5 dalam satu kemungkinan huruf cipherteks saja. Penekanan suatu huruf akan mengakibatkan pergeseran rotor berikutnya. Pada Typex, terdapat tiga rotor dinamis dan dua rotor statis, dengan rotor statis itu dapat diatur secara manual dan kurang lebih berfungsi sama seperti rotor dinamis yang dimiliki Enigma.

2.3 SIGABA *cipher*

SIGABA *cipher* menggunakan teori dasar yang sama dengan Enigma untuk mengenkripsi sebuah plainteks. Perbedaannya adalah SIGABA memakai lima belas buah rotor dan tidak memakai reflektor. Kelima belas buah rotor tersebut dibagi menjadi tiga bagian dengan masing-masing memiliki lima buah rotor. Aksi yang dilakukan dua bagian awal mengendalikan pergerakan bagian ketiga. Bagian pertama, bagian utama dari kumpulan rotor tersebut, disebut *cipher* rotor dan memiliki 26 contacts. Pada bagian ini, pergerakan rotor sama dengan yang terjadi pada Enigma.

Bagian kedua disebut juga rotor kontrol. Rotor kontrol menerima empat buah sinyal pada setiap langkah. Setelah melewati rotor kontrol, keluaran akan dibagi ke dalam 10 grup yang ukurannya bervariasi. Tiap grup berkoresponden dengan masukan pada bagian rotor selanjutnya.

Bagian ketiga disebut juga rotor indeks. Setelah melewati rotor indeks, satu sampai empat dari lima lines keluaran akan dinyalakan. Aksi ini akan menyalakan rotor cipher.

3. Keunggulan Dan Kekurangan Masing-masing *Cipher*

3.1 Keunggulan dan Kelemahan Enigma *Cipher*

Keunggulan yang dimiliki Enigma *cipher* antara lain:

1. Kompleksitas kemungkinan huruf cipherteks yang besar (26^3 atau 26^4)
2. Penggunaan teknik *cipher* yang mudah dimengerti.

Kelemahan dari Enigma antara lain:

1. Kunci disimpan secara manual.
2. Dapat dikriptanalisis dengan teknik analisis frekuensi sederhana.
3. Perulangan enkripsi huruf (Pada konfigurasi yang sama, A dienkrip menjadi Q, dengan Q sendiri dienkrip menjadi A).

3.2 Keunggulan dan Kelemahan Typex *cipher*

Keunggulan yang dimiliki Typex *cipher* antara lain:

1. Penggunaan rotor yang lebih banyak.
2. Mesin Typex lebih efisien dibandingkan Enigma

Kelemahan Typex antara lain:

1. Dapat dikriptanalisis dengan teknik analisis frekuensi sederhana.
2. Tidak lebih simpel dari Enigma dalam segi penggunaan oleh *user*.

3.3 Keunggulan dan Kelemahan SIGABA *C*ipher

Keunggulan yang dimiliki SIGABA *cipher* antara lain:

1. Pengubahan karakter bersifat *pseudorandom*.
2. Penggunaan rotor yang cukup banyak.
3. Lebih aman terhadap serangan kriptografi.

Kelemahan SIGABA antara lain:

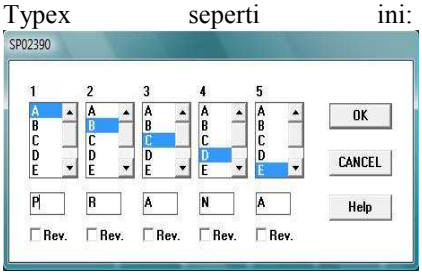
1. Mesin SIGABA tidak praktis, besar, sulit dioperasikan dan rapuh.
2. Pengguna pemula akan kesulitan dalam konfigurasi rotor.

4. Pengujian

4.1 Perancangan Kasus Uji Pengujian Masing-Masing *Cipher*

Berdasarkan tata ancang dan teknik pengujian yang telah dijelaskan, maka dirancang kasus-kasus uji sebagai berikut:

1. Kasus Uji 1
   Kasus Uji 1 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi Enigma. Settingan awal mesin yang digunakan adalah "IV II V | GMY | DN GR IS KC QX TM PV HY FW BJ".
2. Kasus Uji 2
   Kasus Uji 2 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi Typex. Settingan awal pada rotor Typex seperti ini:

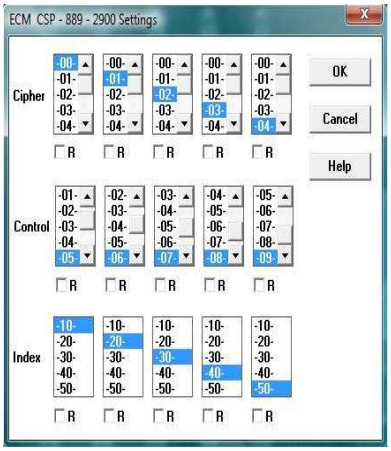


Gambar 4 Posisi Pengaturan Rotor Awal Pada Typex

.

3. Kasus Uji 3

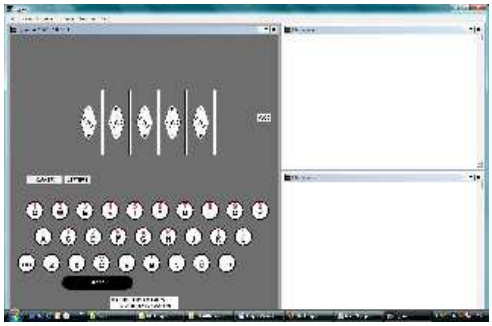
Kasus Uji 3 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi SIGABA. Settingan awal pada proses ini adalah:



Gambar 5 Settingan Awal Rotor

Uji coba akan dilakukan pada tiga jenis simulator, yaitu *software* M3 Enigma, *software* Typex Simulator, serta *software* SIGABA Simulator.

Gambar 6 M3 Enigma Simulator



Gambar 7 Typex Simulator

Gambar 8 SIGABA Simulator

Plainteks yang akan diuji pada ketiga metode tersebut adalah sebagai berikut: “Kirim mata-mata ke daerah perbatasan Jerman-Perancis. Awasi semua tentara yang melewati daerah tersebut. Rencananya akan dilakukan pengiriman senjata secara rahasia melalui daerah tersebut. Siapkan satu kompi tentara untuk mengawal persenjataan tersebut. Sekian. “

4.2 Hasil Pengujian

Dari hasil pengujian Kasus Uji 1, 2, 3, dan 4, diketahui bahwa:

1. Pada uji kasus 1, plainteks didekripsi menjadi FHUF GTYC M-FT UGCH QQAG TDXU IDYE TDGQ SSSJ TM-X JLEW SNZZ YMMJ VNCK OUGE JWSK ZILA WXRL RZZX OHBO TSTB TOKN OKHF OHMF MPHQ TMTX UDGL ERQE YFTV GFOX MFZV YDPG OKHR POEW RTMD CORJ JUAV NFPJ GUAD HKJH FFZU QPKZ LMHS ZVCT ABBE UKQI AIIJ DRYO AJFI DRKV OBMI PLMS CTEW YJFL XJMD NFAK Y. Posisi awal indikator huruf pada “DXP”. Waktu enkripsi sekitar 75 detik. Cipherteks yang dihasilkan juga berhasil didekripsi dengan menggunakan settingan awal yang sama serta posisi awal indikator huruf yang dihasilkan settingan tersebut.
2. Pada uji kasus 2, plainteks didekripsi menjadi FQPAH SUNEZ WTGQV HTNZQ YSLMO CICFP XRVKG WKLCS XTDGP WHRDB PEMZV FTJNM LSDEW QLJBK YFUQN VGOSB SUTUO HOCZP HRPAW TSEIA GLJGP LHJHO LLQWZ ASVML PDJLT ZQYWG NURES KUBJK OCLFC GXJWQ GKDDO YGZUJ GYSUG KZIQJ CQXQZ KKWRH MSOWP NKYUN LBSSO OGGKZ FUJWR DAGER XRIRB EOUUG EVXTV GHBNQ NSKQO FVKKF LSQPP HIQFX MDOIP YHOIC LXQCP NIRVM WILG. Posisi awal indikator huruf pada posisi “A-A-A-A-A”, dan setelah proses enkripsi menjadi “H-X-O-A-A”. Waktu enkripsi kurang lebih 6 detik.
3. Pada uji kasus 3, plainteks didekripsi menjadi PMGMY LYXNX -YXNX LPFLD XFGXS LAFGU XNXVX BLQFG YXB-A GXBOM VLXEX VMLVF YWXLN FBNXG XLJXB KLYFZ FEXNM LDXFG XSLNF GVFUW NLGFB OXBXB JXLXP XBLDM ZXPWP XBLAF BKMGM YXBLV FBQXN XLVFO XGXLG XSXVM XLYFZ XZWML DXFGX SLNFG VFUWN LVMXA PXBLV XNWLP CYAML NFBNX GXLWB NWPLY FBKXE XZLAF GVFBQ XNXXB LNFGV FUWNL VFPMX B. Waktu enkripsi kurang lebih 4-5 detik.

4.3 Analisis Terhadap Hasil Pengujian

Dari ketiga kasus uji tersebut, terlihat bahwa dari segi kecepatan saja, Enigma kalah dari Typex dan SIGABA. Dari segi kompleksitas cipherteks, kurang lebih ketiga metode menghasilkan hasil yang cukup acak dan sulit dipecahkan dengan teknik analisis sederhana. Hanya saja, pada Enigma cukup dengan memasukan konfigurasi rotor serta indikator huruf awal yang tepat akan membuat file cipherteks akan terdekripsi dengan mudah. Pada Typex dan SIGABA, hanya mengetahu konfigurasi rotor saja belum cukup untuk mengembalikan cipherteks ke plainteks, apalagi SIGABA yang pada segmen rotor terakhir menggunakan teknik *pseudorandom*. Untuk Typex, teknik pemecahan cipherteks dapat menggunakan cara yang sama dengan Enigma, hanya saja pemecahan cipherteksnya menggunakan waktu yang jauh lebih lama dari pemecahan cipherteks Enigma.

5. Kesimpulan

Kesimpulan yang dapat diambil dari hasil analisis dan pengujian ketiga *cipher* klasik dari perang dunia ke-2 tersebut adalah:

1. Penggunaan Typex dan SIGABA berdasarkan Enigma, sehingga pakar dari pihak sekutu bisa dengan mudah memecahkan Enigma terlebih dahulu.
2. Kompleksitas algoritma Typex dan SIGABA lebih tinggi daripada Enigma, sehingga pakar Jerman tidak berusaha untuk memecahkannya, karena menganggap Enigma sudah

kebal dari kriptanalisis (yang pada akhirnya terbukti salah, dan Enigma terpecahkan duluan, sehingga mempercepat perkiraan berakhirnya perang dunia kedua).

DAFTAR PUSTAKA

[1] Hart, Brain & Lombard, Michelle. 2006. The Enigma Cipher. *http://starbase.trincoll.edu/~crypto/historical/enigma.html*. Tanggal akses: 12 Maret 2009 pukul 10.27.

[2] Sale, Tony. The Enigma cipher machine. http*://www.codesandciphers.org.uk/enigma/*. Tanggal akses: 12 Maret 2009 pukul 10.26.

[3] Rijmenants, Dirk. 2009. SIGABA CCM. *http://rijmenants.blogspot.com/2009/01/sigaba-ccm.html*. Tanggal akses: 12 Maret 2009 pukul 10.29.

[4] Proc, Jerry. 2008. Typex. *http://www.jproc.ca/crypto/typex.html*. Tanggal akses: 12 Maret 2009 pukul 10.24.

[5] 2008. Typex. *www.espionageinfo.com/Te-Uk/Typex.html*. Tanggal akses: 12 Maret 2009 pukul 10.24.

[6] Munir, Rinaldi. Algoritma Kriptografi Klasik (bagian 5). *Slide Kuliah IF3058 Kriptografi*, Halaman 2-8.

[7] Cryptography Simulators. *http://www.cryptocellar.co.uk*. Tanggal akses: 31 Maret 2009 pukul 23.53.