

Aplikasi Kriptografi dalam Perang Dunia

Ferdy Santoso 13517116
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517116@std.stei.itb.ac.id

Abstrak—Penjagaan rahasia adalah sebuah hal yang sangat penting dan merupakan hal yang dilakukan oleh semua orang. Perang dunia tidak lepas dari dunia penjagaan rahasia, untuk menyampaikan pesan dari satu markas ke markas lain, informasi yang disampaikan haruslah diubah ke bentuk lain supaya informasi yang disampaikan tidak dapat dipahami oleh musuh sehingga rencana perang suatu negara tidak diketahui oleh musuh dan tetap terjaga kerahasiaannya. Makalah ini membahas mengenai teknik-teknik kriptografi yang digunakan pada masa perang dunia pertama dan perang dunia kedua.

Kata kunci—kriptografi, perang, dunia, enkripsi.

I. PENDAHULUAN

Perang dunia adalah sebuah peristiwa yang terjadi di dunia pada tahun 1914-1918 untuk perang dunia 1 dan tahun 1939-1945 untuk perang dunia 2. Perang dunia adalah peristiwa yang menyeramkan dan mencekam karena sangat banyak orang yang menjadi korban jiwa. Di perang dunia 1 korban jiwa mencapai lebih dari 30 juta jiwa dari kedua belah pihak, dan di perang dunia 2 korban jiwa mencapai lebih dari 70 juta jiwa dari kedua belah pihak. Dibalik semua itu, ada orang-orang yang bekerja keras demi menjaga ketahanan negara mereka. Orang-orang yang terlihat menjaga keamanan negara di sektor depan adalah tentara, namun ada orang-orang yang menjaga keamanan negara di sektor belakang yakni para matematikawan.

Para Matematikawan di masa itu adalah orang-orang yang berusaha dengan keras untuk memikirkan cara menyampaikan pesan dari satu markas ke markas lain. Mereka harus memikirkan cara menyampaikan pesan tersebut karena jika pesan tidak dienkripsi terlebih dahulu sebelum disampaikan maka musuh akan mengetahui rencana perang dari negara pengirim pesan, dan jika hal itu terjadi maka negara tersebut dapat kalah dalam perang dan mereka dapat kehilangan lebih banyak korban jiwa.

Salah satu cara untuk menyampaikan pesan tersebut adalah dengan cara mengenkripsi pesan-pesan yang ingin mereka sampaikan menggunakan teknik-teknik kriptografi. Teknik-teknik kriptografi tersebut sangatlah penting untuk dilakukan sebelum penyampaian pesan. Pesan yang belum dienkripsi diubah bentuknya sedemikian rupa sehingga walaupun musuh dapat membaca pesan tersebut mereka tidak dapat mengerti arti dari pesan yang disampaikan karena telah diubah bentuknya.

II. LANDASAN TEORI

A. Bilangan Bulat

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal, misalnya 8, 21, 8765, -34, 0 dan sebagainya. Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02, dan sebagainya.

Muncullah konsep baru dari sifat pembagian bilangan bulat, konsep-konsep itu seperti Aritmetika modulo, Bilangan Prima, dan Kriptografi. Kriptografi merupakan seni mentransformasi sebuah pesan dari suatu bentuk ke bentuk lain supaya arti aslinya tidak terlihat lagi.

Salah satu konsep bilangan bulat yang berguna dalam aritmetika komputer adalah bilangan prima. Bilangan prima adalah bilangan yang hanya habis dibagi oleh 1 dan dirinya sendiri. Bahkan, sembarang bilangan bulat positif dapat dinyatakan sebagai hasil perkalian satu atau lebih bilangan prima.

DEFINISI 1. Misalkan a dan b adalah dua buah bilangan bulat dengan syarat $a \neq 0$. Kita menyatakan bahwa a habis membagi b (a divides b) jika terdapat bilangan bulat c sedemikian sehingga $b = ac$.

Dengan kata lain, jika b dibagi dengan a , maka hasil pembagiannya berupa bilangan bulat. Kadang-kadang pernyataan " a habis membagi b " ditulis juga " b kelipatan a ". Sebagai contoh, 4 habis membagi 12 karena $12 / 4 = 3$ (bilangan bulat) atau $12 = 4 \times 3$. Tetapi 4 tidak habis membagi 13 karena $13 / 4 = 3.25$ (bukan bilangan bulat). Secara umum, jika hasil pembagian bilangan bulat dinyatakan sebagai bilangan bulat juga, maka sembarang bilangan bulat bila dibagi dengan suatu bilangan bulat positif, maka selalu terdapat (1) hasil bagi dan (2) sisa pembagian. Misalnya, $13 / 4$ memberikan hasil bagi 3 dan sisa 1. Kasus khusus, jika a habis membagi b , maka sisa pembagian adalah 0, misalnya $12 / 4$ memberikan hasil bagi 3 dan sisa 0. Perhatikan juga bahwa sisa hasil pembagian selalu lebih besar atau sama dengan nol tetapi lebih kecil dari pembaiL. Sifat ini kita tuangkan dalam Teorema 1 berikut.

TEOREMA 1. Misalkan m dan n adalah dua buah bilangan bulat dengan syarat $n > 0$. Jika m dibagi dengan n maka terdapat dua

buah bilangan bulat unik q (quotient) dan t (remainder), sedemikian sehingga $m = nq + r$ dengan $0 \leq r < n$.

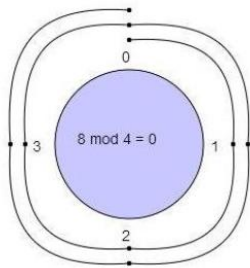
B. Aritmetika Modulo

Aritmetika modulo (modular arithmetic) sangatlah penting dan sangat sering digunakan dalam bidang komputasi dan juga kriptografi. Operator yang digunakan pada aritmetika modulo adalah mod. Operator mod memberikan sisa pembagian. Misalnya 23 dibagi 5 memberikan hasil = 4 dan sisa = 3, sehingga kita tulis $23 \bmod 5 = 3$. Definisi dari operator mod dinyatakan sebagai berikut:

DEFINISI 2. Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0 . Operasi $a \bmod m$ (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m . Dengan kata lain, $a \bmod m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.

8 mod 4 = ?

With a modulus of 4 we make a clock with numbers 0,1,2,3
We start at 0 and go through 8 numbers in a clockwise sequence 1,2,3,0,1,2,3,0



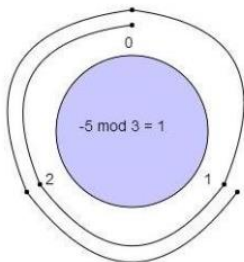
We ended up at 0
so:
 $8 \bmod 4 = 0$

Gambar 1. Contoh 1 Aritmetika Modulo (sumber: Munir, Rinaldi. 2005. Matematika Diskrit, edisi 3.)

Bilangan m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \dots, m - 1\}$

-5 mod 3 = ?

With a modulus of 3 we we make a clock with numbers 0,1,2
We start at 0 and go through 5 numbers in counter-clockwise sequence (5 is negative)
2,1,0,2,1



We ended up at 1
so:
 $-5 \bmod 3 = 1$

Gambar 2. Contoh 2 Aritmetika Modulo (sumber: Munir, Rinaldi. 2005. Matematika Diskrit, edisi 3.)

Kadang-kadang dua buah bilangan bulat, a dan b , mempunyai sisa yang sama jika dibagi dengan bilangan bulat positif m . Kita

katakan bahwa a dan b kongruen dalam modulo m , dan dilambangkan sebagai

$$a \equiv b \pmod{m}$$

(dibaca a kongruen dengan b dalam modulo m)

Jika a tidak kongruen dengan b dalam modulus m maka ditulis

$$a \not\equiv b \pmod{m}$$

Misalnya $38 \bmod 5 = 3$ dan $13 \bmod 5 = 3$, maka 38 kongruen 13 dalam modulo 5. Definisi formal dari kekongruenan dinyatakan sebagai berikut:

DEFINISI 3. Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0 , maka a kongruen b dalam modulo m , jika m habis membagi $a-b$.

Kekongruenan $a = b \pmod{m}$ dapat pula dituliskan dalam hubungan $a = b + km$ yang dalam hal ini sembarang k adalah bilangan bulat. Pembuktiannya adalah sebagai berikut: menurut Definisi 3, $a = b \pmod{m}$ jika $m \mid (a - b)$. Menurut Definisi 1, jika $m \mid (a - b)$, maka terdapat bilangan bulat k sedemikian sehingga $a - b = k$ atau $a = b + km$.

Bilangan bulat positif yang sering digunakan di komputasi adalah bilangan prima. Bilangan prima adalah bilangan bulat positif yang lebih besar dari 1 yang hanya habis dibagi oleh 1 dan dirinya sendiri.

DEFINISI 4. Bilangan bulat positif p ($p > 1$) disebut bilangan prima jika pembagiannya hanya 1 dan p .

Sebagai contoh, 23 adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 23. Karena bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, ... Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap. Bilangan selain prima disebut bilangan komposit (composite). Misalnya 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri. Lahirlah sebuah teorema baru, yakni teorema dasar aritmatika yang isinya adalah sebagai berikut :

TEOREMA 2 (The Fundamental Theorem of Arithmetic). Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.

Teorema 2. menyatakan bahwa baik bilangan prima maupun bilangan komposit, keduanya dapat dinyatakan sebagai perkalian dari satu atau lebih faktor prima. Misalnya :

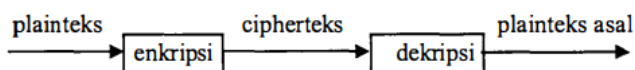
$$\begin{array}{ll} 9 = 3 \times 3 & (2 \text{ buah faktor prima}) \\ 100 = 2 \times 2 \times 5 \times 5 & (4 \text{ buah faktor prima}) \\ 13 = 13 \text{ (atau } 1 \times 13) & (1 \text{ buah faktor prima}) \end{array}$$

C. Kriptografi

Aritmetika modulo dan bilangan prima mempunyai banyak aplikasi dalam ilmu komputer, salah satu aplikasinya yang terpenting adalah kriptografi.

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan menjadikannya menjadi pesan yang tidak mempunyai makna. Zaman sekarang ini kerahasiaan informasi menjadi sesuatu yang penting. Informasi yang rahasia perlu disembunyikan agar tidak diketahui oleh orang yang tidak berhak. Misalnya kriptografi dapat digunakan untuk menyembunyikan kata sandi email kita atau untuk menyembunyikan arti pesan rahasia yang kita tulis. Kriptografi dapat digunakan untuk menyamarkan informasi rahasia itu dari orang atau pihak yang tidak berhak membacanya.

Pesan yang dirahasiakan dinamakan plainteks (plaintext, artinya teks jelas yang dapat dimengerti), sedangkan pesan hasil penyandian disebut cipherteks (ciphertext, artinya teks tersandi). Pesan yang telah disandikan dapat dikembalikan lagi ke pesan aslinya hanya oleh orang yang berhak (orang yang berhak adalah orang yang mengetahui metode penyandian atau memiliki kunci penyandian). Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption) dan proses membalikkan cipherteks menjadi plainteksnya disebut dekripsi (decryption). Gambar 3 memperlihatkan diagram kedua proses yang dimaksud.



Gambar 3. Enkripsi dan Dekripsi (sumber: Munir, Rinaldi. 2005. Matematika Diskrit, edisi 3.)

Pada permulaan tahun 400 SM digunakanlah sebuah alat kriptografi. Pengguna alat ini adalah tentara Yunani kuno. Mereka menggunakan alat yang disebut scytale. Alat ini terdiri dari sebuah pita panjang dari daun papyrus yang dililitkan pada sebatang silinder (Gambar 4). Pesan yang akan dikirim ditulis horizontal (baris per baris). Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia. Untuk membaca pesan, penerima melilitkan kembali silinder yang diameternya sama dengan diameter silinder pengirim. Teknik kriptografi seperti ini dikenal dengan nama transposisi cipher, yang merupakan metode enkripsi tertua.



Gambar 4. Skytale yang digunakan oleh tentara Yunani untuk transposisi pesan. (sumber: Munir, Rinaldi. 2005. Matematika Diskrit, edisi 3.)

III. TEKNIK-TEKNIK KRIPTOGRAFI DALAM PERANG DUNIA

A. Mesin Enigma

Mesin Enigma ditemukan oleh seorang ilmuwan Jerman bernama Arthur Scherbius. Arthur Scherbius bersama dengan teman dekatnya Richard Ritter mendirikan sebuah perusahaan bernama *Scherbius & Ritter*, sebuah perusahaan yang melahirkan berbagai macam inovasi mulai dari turbin hingga bantal. Salah satu proyek *Scherbius & Ritter* adalah membuat sebuah mesin enkripsi untuk tentara Jerman dengan memanfaatkan teknologi abad 20. Dengan ilmu yang telah Scherbius pelajari di *Hanover and Munich* yakni ilmu elektroteknik, ia pun membuat sebuah mesin enkripsi yang ia beri nama *Enigma*. *Enigma* mulai dipasarkan dan digunakan pada tahun 1923, yang lalu dikembangkan kembali dan digunakan sebagai mesin enkripsi utama di perang dunia kedua. Mesin Enigma dikenal sebagai mesin enkripsi yang tidak dapat dipecahkan, walaupun pada akhirnya dapat dipecahkan oleh seorang matematikawan Inggris yang bernama Alan Turing.

1. Struktur Mesin Enigma

Mesin Enigma dibagi menjadi beberapa bagian :

1.1 Keyboard

Keyboard digunakan untuk menginput sebuah huruf ke mesin Enigma. Setelah tombol ditekan, akan ada arus listrik yang mengalir dari huruf yang ditekan ke dalam mesin Enigma.

1.2 Plugboard

Plugboard digunakan untuk menukar huruf yang diinput dengan huruf lain. Jadi arus listrik yang datang dari suatu huruf akan dialirkan ke jalur arus listrik huruf lain. Pasangan pertukaran jalur arus listrik huruf-huruf di plugboard dapat diganti sesuai keinginan user.

1.3 Scrambler

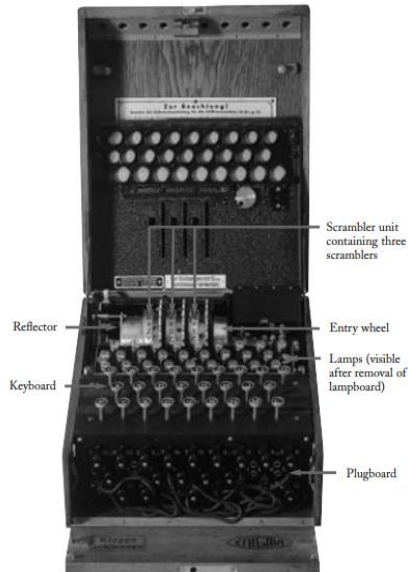
Scrambler digunakan untuk mengganti jalur arus listrik suatu huruf dengan jalur arus listrik huruf lain. Perbedaan scrambler dengan plugboard adalah pola pertukaran jalur di scrambler akan selalu berubah setiap kali pengguna menginput sebuah huruf karena scrambler akan berputar dan mengganti pola pertukaran alurnya, sementara di plugboard pola pertukaran alurnya akan selalu tetap selama pengguna tidak mengganti polanya. Biasanya terdapat 3 scrambler di setiap mesin Enigma.

1.4 Reflector

Reflector digunakan untuk Scrambler digunakan untuk mengganti jalur arus listrik suatu huruf dengan jalur arus listrik huruf lain. Perbedaan reflector dengan plugboard adalah pasangan pertukaran jalur arus listrik di reflector tidak bisa diganti sesuai keinginan pengguna, sementara di plugboard bisa.

1.5 Lampboard

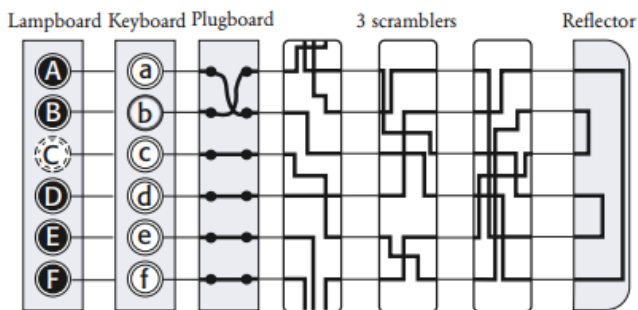
Lampboard digunakan untuk menampilkan hasil enkripsi dari input pengguna, ditandai dengan lampu yang menyala di panel huruf hasil enkripsi.



Gambar 5. Mesin Enigma dengan Kerangka Dalam yang Terlihat. (sumber: Singh, Simon. 2001. *The Code Book*. New York : Delacorte Press).

2. Cara Kerja Mesin Enigma

Untuk memudahkan penjelasan cara kerja mesin enigma kita akan menggunakan studi kasus seperti yang ada di Gambar 6.



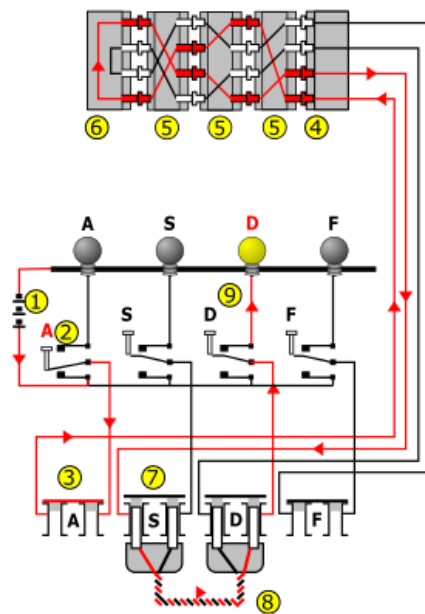
Gambar 6. Diagram Mesin Enigma. (sumber: Singh, Simon. 2001. *The Code Book*. New York : Delacorte Press).

- a) Pengguna menginput sebuah huruf, dalam kasus ini yakni huruf 'b'. Masukan huruf 'b' akan menimbulkan arus listrik yang akan masuk ke mesin Enigma.
- b) Arus listrik akan masuk ke plugboard dan akan

berpindah jalur dari jalur b ke jalur a.

- c) Arus listrik akan melalui scrambler pertama, arus akan berpindah jalur dari jalur a ke jalur f.
- d) Arus akan masuk ke scrambler kedua dan akan berpindah jalur dari jalur f ke jalur e.
- e) Arus akan masuk ke scrambler ketiga dan akan berpindah jalur dari jalur e ke jalur c.
- f) Arus akan masuk ke reflector yang akan menukar jalur dari jalur c ke jalur b.
- g) Arus akan masuk ke scrambler ketiga dan akan berpindah jalur dari jalur b ke jalur f.
- h) Arus akan masuk ke scrambler kedua dan akan berpindah jalur dari jalur f ke jalur e.
- i) Arus akan masuk ke scrambler pertama dan akan berpindah jalur dari jalur e ke jalur c.
- j) Arus listrik akan masuk ke plugboard, dalam kasus ini pengaturan plugboard adalah dari jalur huruf c akan tetap lanjut ke huruf c (tidak berubah jalur).
- k) Arus listrik akan menuju ke lampboard dan panel huruf yang didatangi arus listrik akan menyala, yakni huruf 'c'.

Maka, masukan huruf 'a' akan dienkripsi menjadi huruf 'c'. Selanjutnya scrambler akan berputar yang mengakibatkan pola pertukaran jalur di scrambler menjadi berubah (misal : jalur a tidak lagi dialirkan ke jalur f, namun akan dialirkan ke jalur b).



Gambar 7. Contoh Lain Diagram Mesin Enigma. Dalam kasus ini huruf 'a' akan dienkripsi menjadi huruf 'd'.

(sumber: https://en.wikipedia.org/wiki/Enigma_machine).

Setelah kita mengetahui bagaimana cara mesin Enigma bekerja, kita dapat mencari tahu berapa banyak kombinasi enkripsi huruf yang dapat kita lakukan dengan menggunakan mesin Enigma.

Pertama, orientasi scrambler, ada 3 buah scrambler masing masing memiliki kemungkinan pengaturan sebanyak 26 jumlah pengaturan (karena ada 26 huruf). Maka ada sejumlah $26 \times 26 \times 26$ kemungkinan atau 17.576 kemungkinan.

Kedua, urutan scrambler, karena scrambler pertama, kedua, dan ketiga dapat ditukar-tukar posisinya maka ada 6 kemungkinan urutan penyusunan scrambler. (urutan susunan scrambler : 123,132,213,231,312,321).

Ketiga, plugboard, plugboard pada enigma hanya dapat menukar 6 pasang huruf. Dan kemungkinan menukar huruf dengan plugboard (menukar 6 pasang huruf dari 26) akan sangat besar, yakni sebesar 100.391.791.500 kemungkinan

Total semua kemungkinan pengaturan mesin Enigma adalah : $17.576 \times 6 \times 100.391.791.500$, hasilnya akan berkisar di angka 10.000.000.000.000.000 kemungkinan.

Dapat kita lihat bahwa kemungkinan pengaturan mesin enigma ini sangatlah besar, sehingga mesin Enigma dapat dikatakan mesin enkripsi yang sangat baik.

B. Kode Navajo

1. Sejarah

Pada awal perang dunia 2 seseorang yang bernama Philip Johnston dari Amerika Serikat mengusulkan sebuah teknik kriptografi ke pemerintah Amerika Serikat. Teknik kriptografi ini terinspirasi dari masa kecil Philip Johnston, di masa kecilnya ia dibesarkan di daerah penampungan Navajo di Arizona dan dia telah menyatu dengan budaya Navajo dan telah fasih berbahasa Navajo. Bahasa Navajo sendiri merupakan salah satu bahasa yang digunakan oleh suku asli Amerika Serikat yang pada masa perang dunia 2 mereka ikut serta dalam militer Amerika Serikat. Kelebihan bahasa Navajo adalah bahasa Navajo memiliki tatabahasa yang kompleks.

2. Cara Kerja Kode Navajo

Cara kerja Kode Navajo cukup sederhana. Inti dari Kode Navajo adalah kita membutuhkan seseorang yang fasih berbahasa Navajo sebagai pengirim pesan dan seseorang lain yang juga fasih berbahasa Navajo sebagai penerima pesan, dan kedua orang tersebut berbicara menggunakan radio. Bahasa Navajo yang tidak pernah didengar sebelumnya oleh negara lain mengakibatkan musuh tidak dapat menerjemahkan bahasa Navajo tersebut ke bahasa mereka.

Namun, ada sebuah kendala. Ada beberapa kata di bahasa Inggris yang tidak dapat diterjemahkan ke bahasa Navajo. Maka, solusinya adalah militer Amerika Serikat membuat sebuah kamus untuk kata-kata yang tidak dapat diterjemahkan untuk menghilangkan segala ambiguitas. Contohnya adalah mereka menggunakan nama-nama binatang untuk menggantikan istilah-istilah militer yang spesifik, misalnya

burung hantu (**Da-he-tih-hi**) adalah pesawat tempur, katak (**Chal**) berarti kendaraan yang bersifat amfibi, ikan besi (**Besh-lo**) yang berarti kapal selam, dan istilah-istilah lainnya. Kamus tersebut berisi 274 kata.

Namun, masih ada kendala dalam bahasa Navajo untuk menerjemahkan nama-nama orang atau tempat. Solusinya adalah untuk membuat huruf alfabet yang dikodekan untuk mengeja kata-kata yang sulit, dan huruf-huruf alfabet yang telah dikodekan ini dapat dilihat di Tabel 1. Cara kerjanya adalah untuk menerjemahkan sebuah kata, setiap huruf di kata tersebut dikaitkan dengan sebuah kata dalam bahasa Inggris yang lalu diterjemahkan ke bahasa Navajo. Misalnya untuk menerjemahkan kata *Pacific* akan dieja menjadi “pig, ant, cat, ice, fox, ice, cat,” yang selanjutnya diterjemahkan ke bahasa Navajo menjadi “**bi-sodih, wol-la-chee, moasi, tkin, ma-e, tkin, moasi**”.

ALFABET	KODE BAHASA INGGRIS	KODE BAHASA NAVAJO
A	Ant	Wol-la-chee
B	Bear	Shush
C	Cat	Moasi
D	Deer	Be
E	Elk	Dzeh
F	Fox	Ma-e
G	Goat	Klizzie
H	Horse	Lin
I	Ice	Tkin
J	Jackass	Tkele-cho-gi
K	Kid	Klizzie-yazzi
L	Lamb	Dibeh-yazzi
M	Mouse	Na-as-tso-si
N	Nut	Nesh-chee
O	Owl	Ne-as-jah
P	Pig	Bi-sodih
Q	Quiver	Ca-yeilth
R	Rabbit	Gah
S	Sheep	Dibeh
T	Turkey	Than-zie
U	Ute	No-da-ih
V	Victor	A-keh-di-glini
W	Weasel	Gloe-ih
X	Cross	Al-an-as-dzoh
Y	Yucca	Tsah-as-zih
Z	Zinc	Besh-do-gliz

Tabel 1. Kode Alfabet Navajo. (sumber: Singh, Simon. 2001. *The Code Book*. New York : Delacorte Press).

IV. KESIMPULAN

Kriptografi dapat digunakan untuk menyembunyikan arti asli sebuah pesan sehingga saat dikirimkan ke tempat tujuan jika ada orang yang membaca pesan itu di perjalanan mereka tidak akan tahu arti dari pesan itu.

Kriptografi sangatlah berguna di perang dunia pertama maupun kedua untuk mengenkripsi pesan-pesan yang disampaikan suatu negara dari satu markas ke markas lain. Hal ini dilakukan untuk menjaga kerahasiaan rencana perang tiap-tiap negara.

V. UCAPAN TERIMA KASIH

Pertama, penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa karena berkat rahmat-Nya penulis dapat menyelesaikan makalah yang berjudul “Aplikasi Kriptografi dalam Perang Dunia” ini. Penulis juga mengucapkan terima kasih kepada Pak Rinaldi Munir, Pak Judhi Santoso, dan Bu Harlili selaku dosen mata kuliah IF2120 Matematika Diskrit yang telah membimbing penulis selama satu semester ini.

REFERENSI

- [1] Munir, Rinaldi. 2005. *Matematika Diskrit*. Edisi 3. Bnadung: Informatika Bandung.
- [2] Singh, Simon. 2001. *The Code Book*. New York : Delacorte Press
- [3] Bahr, Howard M. (2004). *The Navajo as Seen by the Franciscans, 1898–1921: A Sourcebook*. Scarecrow Press.
- [4] Adamthwaite, Anthony P. (1992). *The Making of the Second World War*. New York: Routledge.

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, 9 Desember 2017



Ferdy Santoso
13517116