



ITS
Institut
Teknologi
Sepuluh Nopember

TUGAS AKHIR - KI141502

OPTIMASI KASISKI EXAMINATION PADA STUDI KASUS SPOJ THE BYTELANDIAN CRYPTOGRAPHER (ACT IV)

FREDDY HERMAWAN YUWONO
NRP 5113100040

Dosen Pembimbing I
Rully Soelaiman, S.Kom, M.Kom

Dosen Pembimbing II
Wijayanti Nurul Khotimah, S.Kom., M.Sc

JURUSAN TEKNIK INFORMATIKA
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya, 2017

(Halaman ini sengaja dikosongkan)

TUGAS AKHIR - KI141502

**OPTIMASI KASISKI EXAMINATION PADA STUDI KASUS
SPOJ THE BYTELANDIAN CRYPTOGRAPHER (ACT IV)**

FREDDY HERMAWAN YUWONO
NRP 5113100040

Dosen Pembimbing I
Rully Soelaiman, S.Kom, M.Kom

Dosen Pembimbing II
Wijayanti Nurul Khotimah, S.Kom., M.Sc

JURUSAN TEKNIK INFORMATIKA
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya, 2017

(Halaman ini sengaja dikosongkan)

UNDERGRADUATE THESIS - KI141502

**OPTIMIZATION KASISKI EXAMINATION ON STUDY CASE
SPOJ THE BYTELANDIAN CRYPTOGRAPHER (ACT IV)**

FREDDY HERMAWAN YUWONO
NRP 5113100040

Supervisor I
Rully Soelaiman, S.Kom, M.Kom

Supervisor II
Wijayanti Nurul Khotimah, S.Kom., M.Sc

Department of INFORMATICS
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya, 2017

(Halaman ini sengaja dikosongkan)

LEMBAR PENGESAHAN
OPTIMASI KASISKI EXAMINATION PADA STUDI
KASUS SPOJ THE BYTELANDIAN CRYPTOGRAPHER
(ACT IV)

TUGAS AKHIR

Diajukan Guna Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Bidang Studi Algoritma Pemrograman
Program Studi S1 Jurusan Teknik Informatika
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

FREDDY HERMAWAN YUWONO
NRP: 5113100040

Disetujui oleh Dosen Pembimbing Tugas Akhir :

Rully Soelaiman, S.Kom, M.Kom
NIP: 197002131994021001	(Pembimbing 1)

Wijayanti Nurul Khotimah, S.Kom., M.Sc
NIP: 198603122012122004	(Pembimbing 2)

SURABAYA
Desember 2017

(Halaman ini sengaja dikosongkan)

OPTIMASI KASISKI EXAMINATION PADA STUDI KASUS SPOJ THE BYTELANDIAN CRYPTOGRAPHER (ACT IV)

Nama : **FREDDY HERMAWAN YUWONO**
NRP : **5113100040**
Jurusan : **Teknik Informatika FTIf**
Pembimbing I : **Rully Soelaiman, S.Kom, M.Kom**
Pembimbing II : **Wijayanti Nurul Khotimah, S.Kom.,
M.Sc**

Abstrak

Pada Era Digitalisasi ini, tingkat kebutuhan masyarakat akan informasi semakin meningkat. Hal ini menyebabkan pertukaran informasi menjadi sangat mudah. Hal ini membuat informasi yang bersifat sensitif dapat terjadi kebocoran informasi kepada pihak - pihak yang tidak berkepentingan. Kebocoran informasi terbagi menjadi 2 apabila dilihat dari keutuhan informasi yang didapat, yaitu sebagian dan seutuhnya. Kebocoran informasi yang bersifat sebagian, membuat pihak-pihak yang tidak berkepentingan tetapi yang meminginkan informasi tersebut, berusaha untuk mendapatkan informasi yang utuh dari potongan-potongan informasi yang telah didapatkan.

Permasalahan dalam buku tugas akhir ini adalah permasalahan untuk mendapatkan plain text sebanyak-banyaknya dari ciphertext dan batas atas panjang kunci pada metode enkripsi yang menggunakan teknik Vigenere Cipher. Dalam permasalahan ini diberikan plain text dan ciphertext , akan tetapi terdapat informasi yang hilang pada keduanya. Diberikan batas atas panjang kunci, dimana batas atas ini belum tentu panjang kunci yang sesungguhnya.

Tugas akhir ini mengimplemntasikan Kasiski Examination

yang dimodifikasi untuk dapat menyelesaikan permasalahan yang ada, tetapi membutuhkan waktu yang sangat lama. Perlu adanya optimasi yang digunakan untuk mempercepat solusi yang ada dengan menggunakan pruning pada proses Kasiski Examination.

Kata-Kunci: *plain text , ciphertext , Kasiski Examination, optimasi.*

OPTIMIZATION KASISKI EXAMINATION ON STUDY CASE SPOJ THE BYTELANDIAN CRYPTOGRAPHER (ACT IV)

Name : FREDDY HERMAWAN YUWONO
NRP : 5113100040
Major : Informatics FTIf
Supervisor I : Rully Soelaiman, S.Kom, M.Kom
Supervisor II : Wijayanti Nurul Khotimah, S.Kom.,
M.Sc

Abstract

In this Digitalization era, the level of community needs for information is increasing. This make exchanging the information very easy. This makes the sensitive information leakage to the third party. The leakage of information divided into 2 when viewed from the integrity of information they get. First they get all information or second they only get a partial of information. Partial information leakage, make unauthorized party to reconstruct the information they get from all piece information they have already obtain.

The problem in this thesis book is the problem to get plaintext as much as possible from the ciphertext and upper bound of key length. The encryption method is using the Vigenere Cipher technique. Given the plaintext and ciphertext, but there is missing information in both of them. Given the upper bound of key length, that is not real key length.

In this thesis implement modified the Kasiski Examination to solve the problem, but it still take a lot of time to solve it. There need to optimization used to speed up the existing solutions by pruning the existing solution.

Key Note: Plaintext, Ciphertext, Kasiski Examination,

optimization.

KATA PENGANTAR

Puji Syukur kepada Tuhan yang Maha Esa, atas berkatNya penulis dapat menyelesaikan buku berjudul **Optimasi Kasiski Examination pada Studi Kasus SPOJ The Bytelandian Cryptographer (Act IV)**.

Selain itu, pada kesempatan ini penulis menghaturkan terima kasih sebesar-besarnya kepada pihak-pihak yang tanpa mereka, penulis tidak akan dapat menyelesaikan buku ini:

1. **Tuhan Yesus Kristus**- atas segala berkat, limpahan karunia, kesempatan dan rancangan jalanNya-lah penulis masih diberi nafas kehidupan, waktu, tenaga dan pikiran untuk menyelesaikan buku ini.
2. **Alm. Papa** yang selalu menguatkan, menasehati, dan luar biasa sabar dalam mengingatkan penulis agar tidak lupa menjaga kesehatan dan selalu bersyukur selama masa studi.
3. **Mama dan saudara** yang selalu memberikan saran, dukungan, doa dan tidak lupa untuk selalu bersyukur selama masa studi.
4. **Yth Bapak Rully Soelaiman** sebagai dosen pembimbing I yang telah banyak memberikan ilmu, bimbingan, nasihat, motivasi, serta waktu diskusi sehingga penulis dapat menyelesaikan tugas akhir ini; dan
Yth Ibu Wijayanti Nurul Khotimah sebagai dosen pembimbing II yang memberi bimbingan, saran teknis dan administratif, diskusi dan pemecahan masalah dalam pembuatan dan penulisan buku tugas akhir.
5. **Teman-teman Sarjana Komedi** yang telah mengingatkan, memberikan semangat dan inspirasi untuk terus melanjutkan tugas akhir di saat penulis kehilangan semangat.
6. **Teman-teman S1 Teknik Informatika 2013** yang membantu, menyemangati dan bertukar pikiran dengan penulis selama pengerjaan tugas akhir ini.
7. **Teman-teman S1 Teknik Informatika bukan 2013**, yang

telah banyak membantu, menyemangati dan bertukar pikiran dengan penulis selama pengerjaan tugas akhir ini, terutama pada Steven, Theo, Daniel, dan Glenn.

8. Serta semua pihak yang tidak tertulis, baik yang membantu dalam proses pengujian, membantu memikirkan saat ada masalah, dan lainnya yang telah turut membantu penulis dalam menyelesaikan Tugas Akhir ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kekurangan. Oleh karena itu, penulis berharap kritik dan saran dari pembaca sekalian untuk memperbaiki buku ini ke depannya. Semoga tugas akhir ini dapat memberikan manfaat yang sebaik-baiknya.

Surabaya, Nopember 2017

Freddy Hermawan Yuwono

DAFTAR ISI

ABSTRAK	iii
ABSTRACT	v
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xiii
DAFTAR KODE SUMBER	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan	3
1.5 Metodologi.....	3
1.6 Sistematika Penulisan	4
BAB II LANDASAN TEORI	7
2.1 Definisi Umum.....	7
2.1.1 Polyalphabetic Cipher	7
2.1.2 Ciphertext.....	8
2.1.3 Plaintext	8
2.1.4 Secret Key	8
2.1.5 Kasiski Examination	8
2.1.6 Intersection	9
2.2 Deskripsi Permasalahan	9
2.3 Contoh Kasus Permasalahan	12
2.4 Penyelesaian Masalah The Bytelandian Cryptographer (Act IV).....	15
BAB III DESAIN	19
3.1 Desain Umum Sistem	19
3.2 Desain Algoritma	19
3.2.1 Desain fungsi SOLVE	20
3.2.2 Desain Fungsi VALIDITY	22

BAB IV IMPLEMENTASI	23
4.1 Lingkungan Implementasi	23
4.2 Rancangan Data	23
4.2.1 Data Masukan	23
4.2.2 Data Keluaran	24
4.3 Implementasi Algoritma	24
4.3.1 <i>Header</i> yang Diperlukan.....	24
4.3.2 <i>Preprocessor Directives</i>	25
4.3.3 Variabel Global	26
4.3.4 Implementasi Fungsi Main.....	26
4.3.5 Implementasi Fungsi SOLVE.....	27
4.3.6 Implementasi Fungsi VALIDITY.....	29
BAB V UJI COBA DAN EVALUASI	31
5.1 Lingkungan Uji Coba	31
5.2 Uji Coba Kebenaran	31
5.3 Analisa Kompleksitas Waktu	33
BAB VI PENUTUP	35
6.1 Kesimpulan.....	35
6.2 Saran.....	35
DAFTAR PUSTAKA	37
BAB A Hasil Uji Coba Kebenaran pada Situs SPOJ.....	39
BIODATA PENULIS.....	45

DAFTAR TABEL

Tabel 2.1 Contoh <i>Kasiski Examintaion</i>	9
Tabel 2.2 Contoh 1.....	12
Tabel 2.3 Contoh 2.....	13
Tabel 2.4 Contoh 3.....	14
Tabel 2.5 Hasil dari Contoh 3.....	14
 Tabel 5.1 Kecepatan Maksimal, Minimal, dan Rata-Rata dari Hasil Uji Coba Pengumpulan 30 Kali pada Situs Pengujian Daring Spoj	 32

(Halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

Gambar 2.1 Aturan <i>Polyalphabetical Cipher</i>	7
Gambar 2.2 Deskripsi Permasalahan pada SPOJ <i>The Bytelandian Cryptographer (Act IV)</i>	10
Gambar 2.3 Deskripsi Format Masukan dan Keluaran pada SPOJ <i>The Bytelandian Cryptographer (Act IV)</i>	11
Gambar 3.1 Gamba Fungsi Main	19
Gambar 3.2 Gambar Fungsi SOLVE.....	21
Gambar 3.3 Gambar Fungsi VALIDITY.....	22
Gambar 1.1 Hasil Uji Coba pada Situs Penilaian SPOJ..	39
Gambar 1.2 Grafik Hasil Uji Coba pada Situs SPOJ Sebanyak 30 Kali	39
Gambar 1.3 Hasil Pengujian Sebanyak 30 Kali pada Situs Penilaian Daring SPOJ (1).....	40
Gambar 1.4 Hasil Pengujian Sebanyak 30 Kali pada Situs Penilaian Daring SPOJ (2).....	41
Gambar 1.5 Peringkat yang lebih tinggi dari program ini (1).....	42
Gambar 1.6 Peringkat yang lebih tinggi dari program ini (2).....	43

(Halaman ini sengaja dikosongkan)

DAFTAR KODE SUMBER

IV.1	<i>Header</i> yang diperlukan	24
IV.2	Preprocessor Directives	25
IV.3	Variabel Global	26
IV.4	Fungsi main	26
IV.5	Fungsi SOLVE	28
IV.6	Fungsi VALIDITY	29

(Halaman ini sengaja dikosongkan)

BAB I

PENDAHULUAN

Pada bab ini akan dipaparkan mengenai garis besar Tugas Akhir yang meliputi latar belakang, tujuan, rumusan dan batasan permasalahan, metodologi pembuatan Tugas Akhir, dan sistematika penulisan.

1.1 Latar Belakang

Ketergantungan seseorang terhadap informasi tidak terlepas dari kebutuhan manusia akan informasi yang berada disekitarnya. Informasi yang diterima seseorang pada masa sekarang dapat melalui media fisik dan media digital. Media fisik seperti koran dan majalah, sedangkan media digital seperti facebook dan twitter. Media-media tersebut sanggup untuk menyebarkan informasi sangat cepat, sehingga orang-orang dengan cepat mengetahui informasi yang berada disekitarnya.

Pada zaman modern ini suatu informasi, terutama yang bersifat rahasia menjadi semakin rentan akan penyalahgunaan informasi tersebut. Oleh Karena itu, informasi ini disimpan akan disimpan pada tempat-tempat yang aman dan penulisan dari informasi ini pada umumnya menggunakan sandi yang hanya dimengerti oleh orang-orang yang berkepentingan terhadap informasi tersebut.

Informasi digital yang beredar di dunia maya pun tidak lepas dari penyalahgunaan informasi. Dibutuhkan suatu teknik penyandian terhadap data yang dimiliki agar data yang bersifat rahasia itu tidak diketahui dengan orang – orang yang tidak berkepentingan. Teknik penyandian terhadap data digital dapat dibagi menjadi 2 jika melihat dari teknik penyandiannya yaitu *symmetric cipher* dan *asymmetric cipher*. Teknik *symmetric cipher* dapat dibagi menjadi menjadi 4 bagian jika dilihat dari penyubtitusiannya yaitu *Caesar cipher*, *monoalphabetic cipher*, *polyalphabetic cipher*, *one time pad*. Pada dasarnya

pendeskripsian dari data yang terenkripsi dengan penyediaan *symmetric cipher* dengan cara mengetahui kuncinya dan tipe dari penyubstitusiannya.

Dalam Tugas Akhir ini penulis akan mencoba mendeskripsikan informasi terbut dengan menggunakan metode *symmetric cipher* dan teknik substitusinya menggunakan *polyalphabetic cipher*. Salah satunya dengan menggunakan modifikasi *Kasiski Examination*, akan tetapi dalam permasalahan ini apabila hanya menggunakan *Kasiski Examination* waktu yang dibutuhkan sangatlah besar, oleh karena itu penulis mengoptimasi metode yang telah ada.

1.2 Rumusan Masalah

Rumusan masalah yang diangkat dalam tugas akhir ini adalah sebagai berikut:

1. Melakukan implementasi algoritma untuk menyelesaikan masalah pendeskripsian *ciphertext* yang diperoleh dari *polyalphabetic cipher*.
2. Bagaimana hasil dari kinerja algoritma yang digunakan untuk melakukan pendeskripsian *polyalphabetic cipher*

1.3 Batasan Masalah

Dari permasalahan yang telah diuraikan di atas, terdapat beberapa batasan masalah pada tugas akhir ini, yaitu:

1. Bahasa pemrograman yang akan digunakan adalah bahasa pemrograman C/C++.
2. Batasan maksimum panjang dari *ciphertext* sebesar 1,000,000 karakter.
3. Batasan maksimum panjang dari batas atas *key* sebesar 100,000 karakter.

4. *Dataset yang digunakan adalah dataset pada problem SPOJ The Bytelandian Cryptographer (Act IV).*

1.4 Tujuan

Tujuan dari pengerjaan Tugas Akhir ini adalah:

1. Melakukan implementasi algoritma untuk menyelesaikan masalah SPOJ *The Byteland Cryptographer (act IV)*.

1.5 Metodologi

Langkah-langkah yang ditempuh dalam pengerjaan Tugas Akhir ini yaitu:

1. **Penyusunan proposal Tugas Akhir**

Pada tahap ini dilakukan penyusunan proposal Tugas Akhir yang berisi permasalahan dan gagasan solusi yang akan diteliti pada SPOJ *The Bytelandian Cryptographer (Act IV)*.

2. **Studi literatur**

Pada tahap ini dilakukan pencarian informasi dan studi literatur mengenai pengetahuan atau metode yang dapat digunakan dalam penyelesaian masalah. Informasi didapatkan dari materi-materi yang berhubungan dengan algoritma yang digunakan untuk penyelesaian permasalahan ini, materi-materi tersebut didapatkan dari buku, jurnal, maupun internet.

3. **Desain**

Pada tahap ini dilakukan desain rancangan algoritma yang digunakan dalam solusi untuk pemecahan SPOJ *The Bytelandian Cryptographer (Act IV)*

4. **Implementasi perangkat lunak**

Pada tahap ini dilakukan implementasi atau realiasi dari rancangan desain algoritma yang telah dibangun pada

tahap desain ke dalam bentuk program.

5. Uji coba dan evaluasi

Pada tahap ini dilakukan uji coba kebenaran implementasi. Pengujian kebenaran dilakukan pada sistem penilaian daring SPOJ sesuai dengan masalah yang dikerjakan untuk diuji apakah luaran dari program telah sesuai.

6. Penyusunan buku Tugas Akhir Pada tahap ini dilakukan penyusunan buku Tugas Akhir yang berisi dokumentasi hasil pengerjaan Tugas Akhir.

1.6 Sistematika Penulisan

Buku Tugas Akhir ini bertujuan untuk mendapatkan gambaran dari pengerjaan Tugas Akhir ini. Secara garis besar, buku Tugas Akhir terdiri atas beberapa bagian seperti berikut ini:

Bab I Pendahuluan

Bab ini berisi latar belakang masalah, tujuan dan manfaat pembuatan Tugas Akhir, permasalahan, batasan masalah, metodologi yang digunakan, dan sistematika penyusunan Tugas Akhir.

Bab II Dasar Teori

Bab ini berisi dasar teori mengenai permasalahan dan algoritma penyelesaian yang digunakan dalam Tugas Akhir dan deskripsi permasalahan yang digunakan dalam Tugas Akhir.

Bab III Desain

Bab ini berisi desain algoritma yang digunakan dalam penyelesaian permasalahan.

Bab IV Implementasi

Bab ini berisi implementasi berdasarkan desain algoritma yang telah dilakukan pada tahap desain.

Bab V Pengujian dan Evaluasi

Bab ini berisi uji coba dan evaluasi dari hasil implementasi yang telah dilakukan pada tahap implementasi.

Bab VI Kesimpulan dan Saran

Bab ini berisi kesimpulan dari hasil pengujian yang dilakukan, dan membahas saran beserta *further enhancements* untuk pengembangan algoritma lebih lanjut.

Daftar Pustaka

Merupakan daftar referensi yang digunakan untuk mengembangkan Tugas Akhir.

Lampiran

Merupakan bab tambahan yang berisi hal-hal terkait yang penting dalam aplikasi ini.

(Halaman ini sengaja dikosongkan)

BAB II

LANDASAN TEORI

Bab ini akan membahas mengenai dasar teori dan literatur yang menjadi dasar pengerjaan tugas akhir ini. Pada subbab 2.1 membahas mengenai definisi umum yang digunakan dalam memecahkan permasalahan ini. Pada subbab 2.2 membahas mengenai deskripsi permasalahan. Pada subbab 2.3 membahas mengenai contoh permasalahan. Pada subbab 2.4 membahas mengenai penyelesaian masalah secara lengkap.

2.1 Definisi Umum

Pada subbab ini membahas definisi-definisi yang digunakan sebagai dasar untuk memahami permasalahan ini dan pemecahannya.

2.1.1 Polyalphabetic Cipher

Polyalphabetic Cipher merupakan salah satu teknik untuk menenkripsi dengan menggunakan substitusi huruf untuk menyubtitusikannya. Secara garis besar yang dimaksud dengan *polyalphabetic cipher* memiliki 2 aturan dasar yang harus dipenuhi yaitu :

1. Memiliki satu set aturan substitusi *monoalphabetic cipher* yang digunakan.
2. Sebuah kunci mengatur suatu aturan tertentu yang dipilih untuk mengatur transformasi yang dilakukan.

Untuk memperjelas aturan diatas, dapat dilihat pada gambar 2.1.

$$\begin{aligned} C &= C_0, C_1, C_2, \dots, C_{n-1} = E(K, P) = E[(k_0, k_1, k_2, \dots, k_{m-1}), (p_0, p_1, p_2, \dots, p_{n-1})] \\ &= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \dots, (p_{m-1} + k_{m-1}) \bmod 26, \\ &\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \dots, (p_{2m-1} + k_{m-1}) \bmod 26, \dots \end{aligned}$$

Gambar 2.1 Aturan *Polyalphabetical Cipher*

Salah satu turunan dari *polyalphabetic cipher* adalah teknik *Vigenere Cipher* yang menjadi dasar permasalahan yang diangkat dalam tugas akhir ini.[2]

2.1.2 Ciphertext

Ciphertext adalah suatu pesan / teks acak yang dihasilkan dari suatu algoritma kriptografi. Contoh dari *Ciphertext* dalam kasus *polyalphabetical cipher* adalah "RTPPRKGFI" yang merupakan hasil enkripsi dari "PLAINTEXT" dan menggunakan kunci "CIPHER".[3]

2.1.3 Plaintext

Plaintext Plaintext adalah data original sebagai inputan dari suatu metode enkripsi yang akan dilakukan[3]. Biasanya merupakan suatu rangkaian kata yang masih dapat dipahami artinya atau hasil keluaran dari suatu algoritma kriptografi yang akan dienskripsi lagi.

2.1.4 Secret Key

Secret Key atau yang lebih dikenal dengan *key* adalah suatu inputan dari algoritma enkripsi yang akan menentukan suatu transformasi dan substitusi yang akan dilakukan oleh algoritma enkripsi[3]. Dalam kasus *polyalphabetical cipher* pada permasalahan yang diangkat dalam tugas akhir ini, panjang kunci yang digunakan setidaknya 1.

2.1.5 Kasiski Examination

Kasiski Examination merupakan suatu teknik yang digunakan untuk mendeskripsikan secara paksa suatu *ciphertext* yang menggunakan teknik substitusi, baik itu *polyalphabetical cipher* maupun *monoalphabetical cipher*. Teknik menggunakan

kelemahan yang ditimbulkan oleh teknik substitusi itu sendiri, yaitu apabila suatu *subtring* dari *plain text* dan *subtring* dari suatu set kunci yang berulang terdapat yang berulang, maka dapat dipastikan untuk menebak panjang huruf / karakter kunci yang digunakan. Sebagai contoh dapat dilihat pada table 2.1.

<i>plain text</i>	c	r	y	p	t	o		i	s		s	h	o	r	t	
kunci	a	b	c	d	e	a	b	c	d	e	a	b	c	d	e	a

Tabel 2.1 Contoh *Kasiski Examintaion*

Dari table 2.1 yang ada dapat disimpulkan bawah *plain text* "crypto" dan kunci "abcdea" berulang. Sehingga setidaknya dapat disimpulkan bahwa panjang kuncinya mungkin 4 karakter. [4]. Hal ini yang menjadi dasar pengerjaan permasalahan yang diangkat dalam tugas akhir ini.

2.1.6 Intersection

Intersection adalah himpunan A dan Himpunan B dimana ada bagian dari A juga merupakan bagian dari B. Sehingga dapat ditulis

$$A \cap B = \{x : x \in A \text{ dan } x \in B\}$$

Sebagai contoh *intersection* antara $\{1, 2, 3\}$ dan $\{1, 4, 5\}$ adalah $\{1\}$. [5]

2.2 Deskripsi Permasalahan

Permasalahan yang diangkat dalam tugas akhir ini diangkat dari suatu permasalahan yang terdapat pada suatu situs penilaian daring atau *online judge* SPOJ yaitu *The Bytelandian Cryptographer (Act IV)* dengan nomer soal 20 dengan kode soal CRYPTO4. Deskripsi soal yang asli menggunakan bahasa Inggris dapat dilihat pada 2.2.[1]

Permasalahan pada The Bytelandian Cryptographer (Act IV) diberikan pesan dengan panjang N huruf, huruf yang digunakan adalah huruf kapital latin dari A sampai dengan Z, yang dapat ditafsirkan menjadi bilangan bulat dari 0 sampai dengan 25. Diberikan kunci untuk mentransmisikan pesan yang diketahui oleh kedua belah pihak yang terdiri dari M bilangan bulat. Dengan menggunakan kunci yang ada bahwa pada index ke i dari pesan pada index x_i akan di enkripsikan ke dalam bentuk index ke i dari pesan hasil enkripsi y , yang mengikuti aturan

$$y_i = x_i + k_{1+(i-1) \bmod M \bmod 26}$$

Diketahui *plain text* dan *ciphertext* yang diberikan hanya berupa potongan-potongan dari kedua pesan tersebut. Dicari bagaimana menkonstruksi ulang pesan yang telah didapat sehingga bisa membentuk *plain text* yang asli dari pesan yang telah didapatkan sebanyak-banyaknya.

CRYPTO4 - The Bytelandian Cryptographer (Act IV)

no tags

The Bytelandian Cryptographer has been requested by the BBFO to put forward an encryption scheme which would allow the BBFO to communicate with its foreign associates. After some intensive studies, he has decided upon the Vigenere cipher. Messages written using 26 upper case characters of the Latin alphabet: A, B, ..., Z which are interpreted as integers 0, 1, ..., 25 respectively. The secret cypher for transmitting a message is known to both sides and consists of n integers k_1, k_2, \dots, k_n . Using this cypher, the i -th number x_i of the input message x is encrypted to the form of the i -th number of the output message y , as follows:

$$y_i = (x_i + k_{1+(i-1) \bmod n}) \bmod 26.$$

You are trying to find out the content of a message transmitted by the BBFO. By a lucky stroke of fortune, your spies managed to intercept the message in both its plaintext and encrypted form (x and y respectively). Unfortunately, during their dramatic escape the files they were carrying were pierced by bullets and fragments of messages x and y were inadvertently lost. Or were they? It is your task to reconstruct as much of message x as you possibly can.

Gambar 2.2 Deskripsi Permasalahan pada SPOJ *The Bytelandian Cryptographer (Act IV)*

Format masukan pada baris pertama diberikan T ujicoba kasus. Pada baris selanjutnya diberikan M batas atas panjang kunci. Pada baris selanjutnya diberikan *plain text*. Pada baris

selanjutnya di berikan *ciphertext*, *plain text* dan *ciphertext* menggunakan karakter A sampai dengan Z yang dapat ditafsirkan kedalam bilangan bulat 0 sampai dengan 25 dan '*' (sebagai karakter yang hilang).

Format keluaran yang dihasilkan adalah 1 baris yang mengandung *plain text* dan '*' apabila nilai dari karakter tersebut tidak dapat ditentukan. Deskripsi mengenai Format masukan dan keluaran beserta dengan contohnya dalam bahasa Inggris dapat lihat pada gambar 2.3

Input

The first line of input contains a single integer $t \leq 200$ denoting the number of test cases. t test case descriptions follow.

For each test case, the first line contains one integer m which is some upper bound on the length of the cypher ($1 \leq m \leq 100000$). The second line of input contains the original message x , while the third line contains the encrypted message y . The messages are expressed using characters 'A'-'Z' (interpreted as integers 0-25) and '*' (denoting a single character illegible due to damage). The total length of the input file is not more than 2MB.

Output

For each test case output a single line containing the original message x , with asterisks '*' in place of only those characters whose value cannot be determined.

Example

```
Input:
4
1
A*X*C
**CH*
4
*B***A
AAAAAA
6
*B***A
AAAAAA
4
*AA*****
AAAAAAAAAA

Output:
A*XHC
*BA*BA
*B***A
*AA**A****
```

Gambar 2.3 Deskripsi Format Masukan dan Keluaran pada SPOJ *The Bytelandian Cryptographer (Act IV)*

Batasan permasalahan *The Bytelandian Cryptographer (Act IV)* adalah sebagai berikut:

1. $T \leq 200$

2. $1 \leq M \leq n \leq 100,000$
3. Panjang *input file* tidak melebihi dari 2MB.
4. Lingkungan penilaian Intel Pentium G860 3GHz.
5. Batas Waktu: ≤ 17 detik
6. Batas Sumber Code : 50000B
7. Batas Memory : 1536 MB.

2.3 Contoh Kasus Permasalahan

Dalam Permasalahan yang diangkat ini huruf A sampai dengan Z ditafsirkan sebagai 0 sampai dengan 25. Contoh 1. Diketahui M bernilai 1 yang menunjukkan batas atas dari panjang kunci. Diketahui *plain text* adalah $A * X * C$ dan *ciphertext* adalah $**CM*$.

<i>index</i>	0	1	2	3	4
<i>plain text</i>	A	*	X	*	C
<i>ciphertext</i>	*	*	C	M	*
Selisih yang diketahui			5		
Hasil	A	*	X	H	C

Tabel 2.2 Contoh 1

Dari table 2.2 diketahui bahwa batas atas panjang kuncinya 1, oleh karena itu pasti panjang kuncinya 1. Tujuan awal adalah mendapatkan *plain text* sebanyak banyaknya dari *ciphertext* dan batas atas panjang kunci yang telah diberikan. Oleh karena panjang *ciphertext* yang diketahui hanya 2, sedangkan salah satu *ciphertext* digunakan untuk menghitung selisih yang diketahui, maka dari tabel 2.2 hanya mendapatkan 1 plaintext saja. Langkah-langkah yang digunakan adalah menyimpan seluruh hasil selisih dari *plain text* dan *ciphertext* yang diketahui. Pada tahap ini index 2 dengan selisihnya 5. Mencari *ciphertext* yang lain yang *plain text* masih kosong. Pada contoh ini index 3 saja.

Dari yang telah diketahui dapat disimpulkan bahwa index 3 ini nilai *plain text* adalah H, karena dapat panjang kunci pasti 1 dan index $3\%1$ adalah 0 dan tidak ada *collision* yang terjadi. Sehingga index 3 dapat diisi dengan cara *ciphertext* pada index 3 dikurangi dengan 5 dan hasil yang diperoleh adalah "H".

Contoh 2. Diketahui bahwa M bernilai 4 yang menunjukkan batas atas dari panjang kunci. Diketahui *plain text* adalah *B***A dan *ciphertext* adalah AAAAAA. Dalam Contoh ini panjang kuncinya bisa dari 1 sampai dengan 4.

<i>index</i>	0	1	2	3	4	5
<i>plain text</i>	*	B	*	*	*	A
<i>ciphertext</i>	A	A	A	A	A	A
Selisih yang diketahui		25				0
Panjang Kunci 1	tidak bisa karena ada yang <i>collision</i>					
Panjang Kunci 2	tidak bisa karena ada yang <i>collision</i>					
Panjang Kunci 3	*	B	A	*	B	A
Panjang Kunci 4	tidak bisa karena ada yang <i>collision</i>					

Tabel 2.3 Contoh 2

Melanjutkan dari tabel 2.2 untuk melihat adanya *collision* yang terjadi pada indeks selisih *plain text* dan *ciphertext* yang diketahui. Dari table 2.3 dapat diketahui pada indeks 1 selisih antara *plain text* dan *ciphertext* adalah 25 dan indeks 5 selisih antara *plain text* dan *ciphertext* adalah 0. Pada tabel 2.3 dapat dilihat bahwa panjang kunci 1 tidak bisa digunakan, alasannya adalah terjadinya *collision* pada selisih yang diketahui dan nilai dari indek yang bertabrakan itu berbeda. Indeks 1 dan 5 apabila dimodulo 1 hasilnya adalah 1 dan nilai dari indeks yang bertabrakan itu berbeda. Hal ini juga terjadi pada panjang kunci 2, dimana indeks 1 dan 5 dimodulo 2 adalah 1, dan nilai dari indeks 1 dan 5 berbeda. Hal serupa juga terjadi panjang kunci 4, dimana indeks 1 dan 5 dimodulo hasilnya 1 dan nilai dari indeks

yang bertabrakan itu berbeda. Apabila indeks yang bertabrakan itu memiliki nilai yang sama maka dapat dibentuk jawabannya. Seperti yang terjadi pada tabel 2.4. Sehingga hasil yang terbentuk hanya terdapat pada panjang kunci 3. Hal ini terjadi karena pada indeks yang telah diketahui selisihnya tidak terjadi *collision*. Dibuktikan dari $1\%3 = 1$ dan $5\%3 = 2$.

Contoh 3. Diketahui bahwa M bernilai 4 yang menunjukkan batas atas dari panjang kunci. Diketahui *plain text* adalah *AA***** dan *ciphertext* adalah AAAAAAAAAA. Indeks akan dihitung mulai dari 0.

<i>index</i>	1	2	3	4	5	6	7	8	9	10
<i>plain text</i>	*	A	A	*	*	*	*	*	*	*
<i>ciphertext</i>	A	A	A	A	A	A	A	A	A	A
Selisih yang diketahui		0	0							

Tabel 2.4 Contoh 3

<i>index</i>	1	2	3	4	5	6	7	8	9	10
<i>plain text</i> awal	*	A	A	*	*	*	*	*	*	*
Panjang kunci 1	A	A	A	A	A	A	A	A	A	A
Panjang kunci 2	A	A	A	A	A	A	A	A	A	A
Panjang kunci 3	*	A	A	*	A	A	*	A	A	*
Panjang kunci 4	*	A	A	*	*	A	A	*	*	A
Hasil Akhir	*	A	A	*	*	A	*	*	*	*

Tabel 2.5 Hasil dari Contoh 3

Pada Contoh ini kalau dilihat pada indeks selisih yang telah diketahui, terjadi bahwa panjang kunci 1 sampai dengan 4 dapat tercipta sedangkan pada contoh sebelumnya tidak bisa. Hal ini juga dipengaruhi oleh karena isinya itu sama. Walaupun terjadi *collision* pada indeks yang selisih yang diketahui, tetapi kalau

hasilnya sama maka hal itu jawaban untuk setiap panjang kunci bisa terbentuk. Keempat panjang kunci tersebut benar terhadap pesan tersebut. Hasil keluaran yang diinginkan hanya 1 saja tetapi keempat-empatnya benar, oleh karena itu perlu dilakukan *intersection* atau perpotongan dari himpunan keempat kunci tersebut. Perpotongan itu menghasilkan ,A,A,,A,,,,,. Terdapat bagian bagian yang kosong yang dapat diisi dengan *. Sehingga hasil akhirnya dapat dilihat pada tabel 2.5 pada bagian hasil akhir.

2.4 Penyelesaian Masalah The Bytelandian Cryptographer (Act IV)

Permasalahan *The Bytelandian Cryptographer (Act IV)* dapat diselesaikan dengan menggunakan *Kasiski Examination* dan *Intersection*. Untuk menyelesaikan masalah ini perlu ditafsirkan bahwa karakter A sampai dengan Z menjadi 0 sampai dengan 25, karena untuk memudahkan perhitungan mencari selisih dan merekonstruksi *plain text* dari *ciphertext* dan karakter kunci. Berikut ini tahapan-tahapan untuk menyelesaikan masalah ini:

1. Menyimpan posisi indeks karakter, dimana pada indeks tersebut baik *ciphertext* maupun *plain text* tidak bernilai '*', beserta menyimpan hasil perhitungan selisih antara *ciphertext* dan *plain text* .[6].
2. Menyimpan posisi indeks, apabila /*ciphertext* diketahui dan *plain text* tidak diketahui. Untuk mengurangi *running time* dari program[6].
3. Pada Tahapan ini adalah modifikasi dari *Kasiski Examination*, apabila menggunakan *Kasiski Examination* pada umumnya yang hanya mencari posisi berulang dari suatu sub kalimat dalam suatu kalimat tidak bisa digunakan untuk menyelesaikan permasalahan ini. Oleh karena itu dirubah menjadi mengiterasi M dari 1 sampai

dengan M , yang akan digunakan untuk membagi selisih yang diketahui antara *plain text* dan *ciphertext* sebesar posisi iterasi yang telah berjalan. Melihat apakah dalam blok-blok yang telah terbentuk ini terdapat *collision* dan indeks yang saling bertabrakan memiliki value yang sama atau tidak, apabila sama maka tidak terjadi tabrakan sebalik jika terjadi tabrakan maka harus mencari panjang kunci yang baru. Mengiterasi panjang kunci dari $\frac{M}{2} + 1 \leq N \leq M$, alasannya dimulai dari $\frac{M}{2} + 1$ tidak dari 1 karena apabila suatu panjang kunci bernilai benar maka kelipatan dari panjang kunci itu pun juga pasti benar dan untuk mempersingkat waktu *running time* yang seharusnya terjadi. Yang mendasari ini adalah dari tabel 2.3 pada bagian 2.2. Pada bagian ini dilakukan untuk mencari panjang kunci yang benar dengan cara mengiterasi hasil yang diperoleh pada tahap 1 dimodulo dengan posisi iterasi yang dilakukan, apabila tidak terjadi konflik maka panjang kunci tersebut benar jika sebaliknya yang terjadi maka panjang kunci tersebut tidak salah. Contohnya dapat dilihat pada contoh 2 pada bagian 2.2. Pada bagian ini memungkinkan bahwa bisa jadi lebih dari 1 panjang kunci yang bernilai benar. Contohnya seperti yang terjadi pada table 2.4 pada bagian 2.2.

4. Melakukan *intersection* terhadap himpunan dari kunci yang telah di hasilkan[6]. *intersection* yang dilakukan berada didalam perulangan panjang kunci pada waktu generate setiap karakter yang terdapat dalam penyimpanan tahap 2 pada panjang kunci tersebut dengan ketentuan:
 - (a) Panjang kunci harus benar
 - (b) Apabila terdapat indeks yang tidak dapat dipastikan isinya maka posisinya harus di buang dari penyimpanan dan hasilnya pasti '*'

Sehingga untuk setiap *textcase* kompleksitasnya

$$\mathcal{O}(T * \frac{M}{2} * (N + S))$$

Dimana n adalah panjang karakter *plain text* atau *ciphertext*, $\frac{M}{2}$ adalah batas atas kunci dibagi dengan 2, N adalah jumlah posisi karakter yang terdapat pada tahap 2, dan S adalah jumlah posisi karakter yang terdapat pada tahap 1. Pada kondisi *worst case* $T * (N + S) = 1.000.000$, sedangkan $\frac{M}{2}$ adalah 50.000. Hasilnya 50 miliar perulangan, dengan asumsi 1 detik adalah 1 miliar perulangan maka waktu yang dibutuhkan adalah 50 detik. Oleh karena itu hal ini tidak mungkin bisa dilakukan begitu saja, diperlukan pruning pada sumber kode yang ada untuk memangkas waktu eksekusi program.

(Halaman ini sengaja dikosongkan)

BAB III

DESAIN

Pada bab ini akan dijelaskan mengenai desain algoritma yang digunakan untuk menyelesaikan permasalahan pada Tugas Akhir ini.

3.1 Desain Umum Sistem

Sistem pertama kali akan menjalankan fungsi MAIN terlebih dahulu. Desain dari fungsi main sendiri dapat dilihat pada gambar 3.1. Didalam fungsi main akan di panggil fungsi SOLVE yang digunakan untuk menyelesaikan permasalahan yang diangkat pada tugas akhir ini dan didalam fungsi SOLVE akan terdapat fungsi VALIDITY yang digunakan untuk mengecek kebenaran suatu panjang kunci yang sedang diproses. Secara garis besar fungsi Main.

Algorithm 1 Gambar Fungsi Main

```
1: function MAIN
2:    $T \leftarrow INPUT$ 
3:   while  $T \neq 0$  do
4:      $T = T - 1$ 
5:      $m \leftarrow input$  ▷ masukkan batas atas dari kunci
6:      $message[] \leftarrow input$  ▷ masukkan plaintext
7:      $cipher[] \leftarrow input$  ▷ masukkan ciphertext
8:     SOLVE( $message, cipher, m$ )
9:   end while
10: end function
```

Gambar 3.1 Gamba Fungsi Main

3.2 Desain Algoritma

Pada bagian ini akan dibahas secara rinci mengenai fungsi-fungsi yang digunakan dalam sistem.

3.2.1 Desain fungsi SOLVE

Fungsi ini digunakan untuk menyelesaikan permasalahan yang diangkat pada tugas akhir ini yang didalamnya terdapat tahapan yang telah disebutkan di subbab 2.2 dan subbab 2.4, kecuali untuk mengecek kebenaran dari suatu panjang kunci. Gambar mengenai fungsi SOLVE dapat dilihat pada gambar 3.2. Mengenai modulo 26 yang terdapat pada gambar digunakan untuk memastikan bahwa sesilih dari *plain text* dan *ciphertext* adalah 0 sampai dengan 25, dan ditambah 26 pada gambar dimaksudkan agar silisih antara *plain text* dan *ciphertext* selalu bernilai positif.

Algorithm 2 Gambar Fungsi SOLVE

```

1: function SOLVE(message,chiper,m)
2:   counter_diketahui  $\leftarrow$  0
3:   counter_yang_ingin_diketahui  $\leftarrow$  0
4:   diketahui[ ]
5:   Selisih_diketahui[ ]
6:   ingin_diketahui[ ]
7:   Key[ ]
8:   for i = 0 to message[i]  $\neq$  0 ; i + = 1 do
9:     if message[i]  $\neq$  '*' dan cipher[i]  $\neq$  '*' then
10:      diketahui[counter_diketahui] = i
11:      Selisih_diketahui[i] = (message[i] - cipher[i] + 26)%26
12:      counter_diketahui = counter_diketahui + 1
13:     else if message[i] = '*' dan cipher[i]  $\neq$  '*' then
14:      ingin_diketahui[counter_yang_ingin_diketahui] = i
15:      counter_yang_ingin_diketahui + 1
16:     end if
17:   end for
18:   m = min(m, panjang message)
19:   for n =  $\frac{m}{2} + 1$  to n  $\leq$  m; n + = 1 do
20:     if VALIDITY (Key, counter_diketahui, diketahui, Selisih_diketahui, n) = True
21:   then
22:     counter  $\leftarrow$  0
23:     while counter  $\neq$  sizeof(ingin_diketahui) do
24:       if Key[ingin_diketahui[counter]]%n] = null then
25:         message[ingin_diketahui[counter]] = '*'
26:         remove element index i in ingin_diketahui
27:       else if message[ingin_diketahui[counter]] = '*' then
28:         message[ingin_diketahui[counter]] = (ciphertext[ingin_diketahui[counter]] -
29:         Key[ingin_diketahui[counter] + 26)%26
30:         counter = counter + 1
31:       else if message[ingin_diketahui[counter]]  $\neq$ 
32:         (ciphertext[ingin_diketahui[counter]] - Key[ingin_diketahui[counter] + 26) %26) then
33:         message[ingin_diketahui[counter]] = '*'
34:         remove element index i in ingin_diketahui
35:       else
36:         counter = counter + 1
37:       end if
38:     end while
39:   end if
40: end for
41: end function

```

Gambar 3.2 Gambar Fungsi SOLVE

3.2.2 Desain Fungsi VALIDITY

Fungsi ini digunakan untuk memvalidasi suatu panjang kunci yang sekarang di cek kebenarannya. Gambar mengenai fungsi VALIDITY dapat dilihat pada gambar 3.3. Penjelasan mengenai fungsi ini terdapat pada subbab 2.4

Algorithm 3 Gambar Fungsi VALIDITY

```

1: function VALIDITY(Key, counter_diketahui, diketahui, Selisih_diketahui, n)
2:   Initialize(Key, -1)
3:   for i = 0 to i < counter_diketahui; i += 1 do
4:     temp = diketahui[i]
5:     if Key[temp%n] = -1 then
6:       Key[temp%n] = Selisih_diketahui[temp]
7:     else if Key[temp%n] ≠ Selisih_diketahui[temp] then return False
8:     end if
9:   end for
10:  return True
11: end function

```

Gambar 3.3 Gambar Fungsi VALIDITY

BAB IV

IMPLEMENTASI

Pada bab ini menjelaskan implementasi yang sesuai dengan desain algoritma yang telah ditentukan sebelumnya.

4.1 Lingkungan Implementasi

Lingkungan uji coba yang digunakan adalah sebagai berikut:

1. Perangkat Keras
 - *Processor* Intel(R) Core(TM)i7-5700 @ 2.7GHz.
 - Memori 8 GB
2. Perangkat Lunak
 - Sistem Operasi Windows 10 Home 64 bit
 - *Text editor* Bloodshed Dev-C++ 5.11.
 - *Compiler* g++ (TDM-GCC 4.9.2 32-bit).

4.2 Rancangan Data

Pada subbab ini dijelaskan mengenai desain data masukan yang diperlukan untuk melakukan proses algoritma, dan data keluaran yang dihasilkan oleh program.

4.2.1 Data Masukan

Data masukan adalah data yang akan diproses oleh program sebagai masukan menggunakan algoritma yang telah dirancang dalam tugas akhir ini.

Data masukan berupa berkas teks yang berisi data dengan format yang telah ditentukan pada deskripsi *The Bytelandian Cryptographer (Act IV)*. Pada masing-masing berkas data masukan, baris pertama berupa sebuah bilangan bulat yang merepresentasikan jumlah kasus uji yang ada pada berkas tersebut. Untuk setiap kasus uji, baris pertama berupa sebuah bilangan bulat yang merepresentasikan batas atas dari kunci.

baris kedua berupa *string* yang merepresentasikan *plain text* dan baris ketiga berupa *string* yang merepresentasikan *ciphertext*.

4.2.2 Data Keluaran

Data keluaran yang dihasilkan oleh program hanya berupa satu kalimat yang berisikan *plain text* yang bisa didapatkan dari *ciphertext* dan batas atas panjang kunci yang telah di berikan.

4.3 Implementasi Algoritma

Pada subbab ini akan dijelaskan tentang implementasi proses algoritma secara keseluruhan berdasarkan desain yang telah dijelaskan pada bab III. Pada bagian ini menggunakan optimasi kompiler yang bertujuan untuk mempersingkat waktu eksekusi, seperti inline dan noexcept. Inline berguna untuk membuat baris kode dalam kompiler menjadi berurutan, karena bisa saja baris kode yang terjadi pada kompiler tidak berurutan. Noexcept adalah membuang *exception* apabila terjadinya *exception*.

4.3.1 Header yang Diperlukan

Implementasi algoritma dengan teknik *Kasiski Examination* untuk menyelesaikan *The Bytelandian Cryptographer (Act IV)* untuk membutuhkan 4 *header* yaitu *cstdio*, *cstring*, *algorithm*, dan *unordered_map*. Seperti yang terdapat pada kode sumber

```
1 #include <cstdio>
2 #include <cstring>
3 #include <unordered_map>
4 #include <algorithm>
```

Kode Sumber IV.1 *Header* yang diperlukan

Header cstdio berisi modul untuk menerima masukan dan memberikan keluaran. *Header algorithm* berisi modul yang memiliki fungsi-fungsi yang sangat berguna dalam membantu mengimplementasi algoritma yang telah dibangun. Contohnya adalah fungsi *max* dan *sort*. *Header cstring* berisi modul yang memiliki fungsi-fungsi untuk melakukan pemrosesan *string*. Contoh fungsi yang membantu mengimplementasikan algoritma yang dibangun adalah fungsi *memset*. *Header unordered_map* berisi modul-modul untuk membuat suatu tempat penyimpanan data yang dapat diisi, dihapus untuk setiap elemennya, tetapi hanya dapat menyimpan data dalam bentuk seperti array 1 dimensi, akan tetapi media penyimpanannya seperti memetakan suatu elemen himpunan kedalam elemen lainnya. Pengindeksan yang ada menggunakan *hashing function*.

4.3.2 Preprocessor Directives

Preprocessor directives digunakan untuk memudahkan dalam menyingkat kode-kode yang akan dibuat dan biasanya berupa fungsi ataupun suatu konstanta yang akan digunakan dalam proses perhitungan, yang nantinya akan diterjemahkan terlebih dahulu sebelum mengeksekusi kode. Kode Sumber implementasi konstanta variabel dapat dilihat pada Kode Sumber IV.2.

```

1 #define mp make_pair
2 #define ins insert
3 #define MAX (int)(1e6)+1
4 #define MAXK (int)(1e5)+1

```

Kode Sumber IV.2 Preprocessor Directives

4.3.3 Variabel Global

Variabel global digunakan untuk memudahkan dalam mengakses data yang digunakan lintas fungsi. Kode sumber implementasi variabel global dapat dilihat pada Kode Sumber IV.3.

```

1 char plaintext[MAX], ciphertext[MAX];
2 int key[MAXK], both[MAX], known[MAX], knownall;
3 unordered_map<int, int> tf;

```

Kode Sumber IV.3 Variabel Global

4.3.4 Implementasi Fungsi Main

Fungsi Main adalah implementasi algoritma yang dirancang pada Gambar 3.1. Implementasi fungsi Main dapat dilihat pada Kode Sumber IV.4.

```

1 int main()noexcept{
2     int tc;
3     scanf("%d", &tc);
4     while(tc--){
5         int m;
6         scanf("%d", &m);
7         scanf("%s %s", plaintext, ciphertext);
8         tf.clear();
9         knownall=0;
10        SOLVE(m);
11    }

```

Kode Sumber IV.4 Fungsi main

4.3.5 Implementasi Fungsi SOLVE

Fungsi SOLVE adalah implementasi algoritma yang dirancang pada Gambar 3.2. Implementasi fungsi SOLVE dapat dilihat pada Kode Sumber IV.5.

```

1 inline void SOLVE(int m) noexcept
2 {
3     int ntofind = 0;
4     for(int i=0; plaintext[i]!=0; i++)
5         if(plaintext[i]!='*' && ciphertext[i]!='*'){
6             known[knownall++]=i;
7             both[i]=((ciphertext[i]-plaintext[i]
8                 +26)%26);
9         }
10        else if(plaintext[i]=='*' && ciphertext[i]!='*'){
11            tf.ins(mp(ntofind,i));
12            ntofind++;
13        }
14        unordered_map<int,int>::iterator it;
15        m = min(m, (int)strlen(plaintext));
16        for(int n=m/2+1;n<=m;n++)
17        {
18            if(VALIDITY(n))
19            {
20                it=tf.begin();
21                while(it!=tf.end())
22                    if(key[(it->second)%n]==-1){
23                        plaintext[it->second]='*';
24                        it=tf.erase(it);
25                    }
26                    else if(plaintext[it->second]=='*'){
27                        plaintext[it->second]=
28                            (ciphertext[it->second]- 'A'
29                                -key[(it->second)%n]+26)%26 + 'A';
30                        it++;
31                    }
32                    else if(plaintext[it->second] !=
33                        (ciphertext[it->second]- 'A'
34                            -key[(it->second)%n]+26)%26 + 'A'){
35                        plaintext[it->second]='*';
36                        it=tf.erase(it);
37                    }
38                    else it++;
39            }
40        }
41        printf("%s\n", plaintext);
42    }

```

4.3.6 Implementasi Fungsi VALIDITY

Fungsi VALIDITY adalah implementasi algoritma yang dirancang pada Gambar 3.3. Implementasi fungsi VALIDITY dapat dilihat pada Kode Sumber IV.6.

```
1 inline bool VALIDITY(int n) noexcept
2 {
3     memset(key, -1, sizeof(int)*n);
4     for(int x=0; x<knownall; x++){
5         int temp=known[x];
6         if(key[temp%n]==-1) {
7             key[temp%n]=both[temp];
8         }
9         else if(key[temp%n]!=both[temp])
10             return false;
11     }
12     return true;
13 }
```

Kode Sumber IV.6 Fungsi VALIDITY

(Halaman ini sengaja dikosongkan)

BAB V

UJI COBA DAN EVALUASI

Pada bab ini dijelaskan tentang uji coba dan evaluasi dari implementasi yang telah dilakukan pada tugas akhir ini.

5.1 Lingkungan Uji Coba

Lingkungan uji coba yang digunakan adalah salah satu sistem yang digunakan situs penilaian daring SPOJ, yaitu kluster *Cube* dengan spesifikasi sebagai berikut:

1. Perangkat Keras:
 - *Processor* Intel(R) Pentium G860 CPU @ 3GHz.
 - *Memory* 1536 MB.
2. Perangkat Lunak:
 - *Compiler* CPP14.

5.2 Uji Coba Kebenaran

Uji coba kebenaran dilakukan dengan mengirimkan kode sumber program ke dalam situs penilaian daring SPOJ dan melakukan hasil uji coba kasus sederhana dengan langkah-langkah sesuai dengan algoritma yang telah dirancang dengan keluaran sistem. Permasalahan yang diselesaikan adalah *The Bytelandian Cryptographer (Act IV)*. Hasil uji coba dengan waktu terbaik pada situs SPOJ ditunjukkan pada Gambar 1.1.

Selain itu, dilakukan pengujian sebanyak 30 kali pada situs penilaian daring SPOJ untuk melihat variasi waktu dan memori yang dibutuhkan program. Hasil uji coba sebanyak 30 kali dapat dilihat pada Gambar 1.3, 1.6 dan 1.2.

Dari hasil uji coba pada Gambar 1.3, 1.6 dan 1.2 dapat ditarik beberapa informasi seperti yang tertera pada Tabel 5.1.

Berdasarkan Tabel 5.1, dari percobaan yang dilakukan, didapatkan waktu eksekusi rata-rata 4.418 detik dan waktu maksimal 4,47 detik. Waktu eksekusi tersebut 3,8 kali lebih

Waktu Maksimal	4, 49 detik
Waktu Minimal	4, 38 detik
Waktu Rata-Rata	4.418 detik
Memori Maksimal	27 MB
Memori Minimal	26 MB
Memori Rata-Rata	26.5 MB

Tabel 5.1 Kecepatan Maksimal, Minimal, dan Rata-Rata dari Hasil Uji Coba Pengumpulan 30 Kali pada Situs Pengujian Daring Spoj

cepat dari batas waktu eksekusi yang tertera pada deskripsi permasalahan, yaitu 17 detik.

Uji Coba dengan menggunakan contoh kasus ujicoba yang tersedia didalam SPOJ *The Bytelandian Cryptographer (Act IV)*. Sebagai contoh akan digunakan kasus ujicoba yang menggunakan baik mencari panjang kunci maupun *intersection* yang terjadi dalam permasalahan ini.

Sesuai dengan algoritma yang telah dirancang pada pseudocode yang terdapat pada gambar 3.2 maupun pada gambar 3.3. Algoritma ini akan melakukan iterasi yang terdapat pada *plain text* dan *ciphertext* yang diperoleh dari inputan dan akan menyimpan posisi karakter dengan ketentuan apabila pada indeks tersebut diketahui baik *plain text* dan *ciphertext* beserta dengan selisih antara *ciphertext* dan *plain text* . Selanjutnya juga menyimpan posisi karakter yang diperoleh dari *ciphertext* dengan ketentuan apabila *ciphertext* pada indeks tersebut diketahui karakternya dan *plain text* diindeks tersebut tidak diketahui karakternya. Misalnya diambilkan contoh dari tabel 2.4. Maka yang disimpan untuk bagian yang diketahui keduanya adalah indeks ke 1 dengan selisih 0 dan indeks ke 2 dengan selisih 0, sedangkan untuk yang disimpan pada diketahui *ciphertext* saja maka jawabannya semua indeks kecuali indeks ke 1 dan 2. Selanjutnya, akan membandingkan antara panjang *plain*

text atau *ciphertext* dengan m untuk dicari yang lebih kecil yang mana. Selanjutnya, mulai mengiterasi panjang kunci yang akan muncul dari $\frac{m}{2} + 1$ sampai dengan m . Didalam iterasi tersebut akan dilakukan pengecekan apakah nilai m dengan fungsi $\text{VALIDITY}(m)$. Jika gagal program akan melanjutkan untuk mencari panjang kunci selanjutnya, sebaliknya jika hasil dari fungsi tersebut benar maka akan melanjutkan proses mengenerate hasil yang telah diperoleh dari panjang kunci secara satu persatu dan dibandingkan dengan hasil yang sudah ada sebelumnya. Perbandingan tersebut akan mengikuti aturan apabila suatu indeks ternyata ada yang konflik (baik yang nilainya berubah ataupun tidak memiliki suatu aturan kunci dari panjang kunci yang saat itu tersedia) (maka hasil dari indeks tersebut adalah '*') dan menghapus element dari tempat penyimpanan yang menampung indeks *plain text* yang '*' dan *ciphertext* yang tidak '*', apabila tidak ada konflik maka *plain text* pada indeks tersebut tidak menjadi '*'. Seperti contohnya terdapat pada table 2.3 dan tabel 2.4

Sehingga hasil keluaran yang diperoleh dari algoritma ini adalah seluruh *plain text* yang dapat dibentuk.

5.3 Analisa Kompleksitas Waktu

Pada *pseudocode* yang terdapat pada Gambar 3.1. Untuk setiap kasus ujicoba terdapat 2 fungsi utama. Dengan menggunakan *Kasiski Examination* fungsi SOLVE dan VALIDITY memiliki kompleksitas $\mathcal{O}((n + (\frac{M}{2} * (N + S))))$. n adalah panjang karakter *plain text* atau *ciphertext*, $M/2$ adalah batas atas kunci dibagi dengan 2, N adalah jumlah posisi karakter yang terdapat bisa jadi memiliki suatu nilai yang bisa didapat dari *ciphertext*, dan S adalah jumlah posisi karakter yang diketahui. Untuk kompleksitas fungsi VALIDITY $\mathcal{O}(S)$. Sehingga kompleksitas dapat disederhanakan menjadi

$\mathcal{O}(T * \frac{M}{2} * (N + S))$. Sehingga secara keseluruhan kompleksitas dari algoritma yang dirancang pada tugas akhir ini adalah $\mathcal{O}(T * \frac{M}{2} * (N + S))$.

Pada umumnya, eksekusi program pada situs penilaian daring SPOJ adalah 1 detik untuk setiap 1.000.000.000 proses. Eksekusi program dengan kompleksitas $\mathcal{O}(T * \frac{M}{2} * (N + S))$. Pada *worst case* $T * (N + S) = 1.000.000$, sedangkan $\frac{M}{2}$ adalah 50,000. Hasilnya melebihi dari 50 miliar perulangan, maka waktu yang dibutuhkan adalah 50 detik. Jika hal ini terjadi maka waktu eksekusi akan berjalan dengan sangat lama. Estimasi waktu kurang lebih 100 detik, tetapi kenyataan yang terjadi tidak demikian, alasannya karena jumlah S bisa berkurang seringin dengan perulangan yang ada. Karena dari pernyataan soal bahwa file masukkan tidak akan lebih besar daripada 2 MB[1].

BAB VI

PENUTUP

Bab ini membahas kesimpulan yang dapat diambil dari tujuan pembuatan sistem dan hubungannya dengan hasil uji coba yang telah dilakukan. Selain itu, terdapat beberapa saran yang bisa dijadikan acuan untuk melakukan pengembangan dan penelitian lebih lanjut.

6.1 Kesimpulan

Dari hasil uji coba yang telah dilakukan terhadap perancangan dan implementasi algoritma untuk menyelesaikan SPOJ *The Bytelandian Cryptographer (Act IV)* dapat diambil kesimpulan sebagai berikut:

1. Implementasi algoritma dengan menggunakan teknik *Kasiski Examination* dengan adanya optimasi dapat menyelesaikan permasalahan SPOJ *The Bytelandian Cryptographer (Act IV)* dengan benar.
2. Kompleksitas waktu $\mathcal{O}(T * \frac{M}{2} * (N + S))$ masih dapat menyelesaikan permasalahan SPOJ *The Bytelandian Cryptographer (Act IV)*
3. Waktu yang dibutuhkan oleh program untuk menyelesaikan SPOJ *The Bytelandian Cryptographer (Act IV)* minimum 4,38 detik, maksimum 4,49 detik dan rata-rata 4.418 detik. Memori yang dibutuhkan berkisar antara 26-27 MB.

6.2 Saran

Pada Tugas Akhir kali ini tentunya terdapat kekurangan serta nilai-nilai yang dapat penulis ambil. Berikut adalah saran-saran yang dapat diambil melalui Tugas Akhir ini:

1. Dengan teknik *Kasiski Examination* masih cenderung lambat, karena masih menggunakan teknik *brute force*

sehingga hasil yang diperoleh kurang optimal, perlu adanya optimisasi lanjutan yang dapat mencari suatu panjang kunci.

2. Perlu adanya Optimisasi dalam hal pencarian suatu indeks yang perlu dirubah atau tidak. Dengan teknik yang dipakai oleh penulis tidak dapat memenuhi ekspektasi jika berharap dengan hasil yang sangat cepat.

DAFTAR PUSTAKA

- [1] K. Piwakowski, “CRYPTO4 - The Bytelandian Cryptographer (Act IV),” 2004. [Online]. Available: <http://www.spoj.com/problems/CRYPTO4/>
- [2] W. Stallings and L. Brown, *Computer Security Principles and Practice*, 3rd ed. Pearson, 2015.
- [3] S. William, *Cryptography and Network Security*, 5th ed. Pearson, 2011.
- [4] “Kasiski Method.” [Online]. Available: <http://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Kasiski.html>
- [5] K. Devlin, *The Joy of Sets: Fundamentals of Contemporary Set Theory*, 2nd ed. New York: Springer, 1993.
- [6] john_jones, “SPOJ Discussion Board,” 2009. [Online]. Available: <http://discuss.spoj.com/t/problemset-3/242/13>

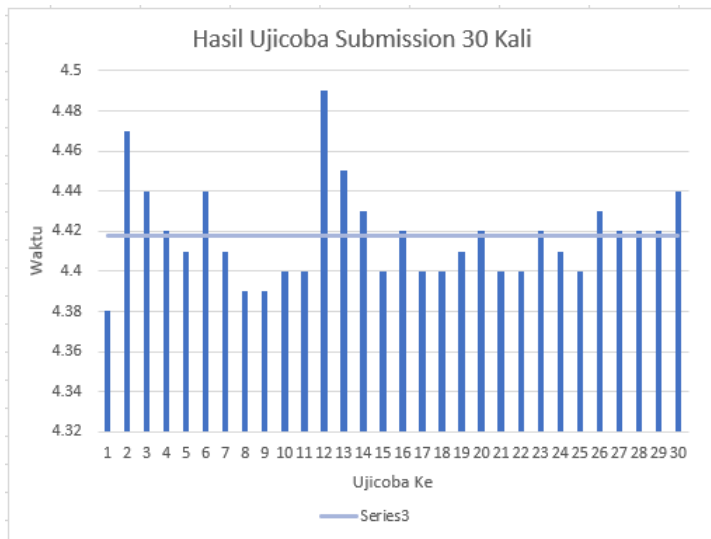
(Halaman ini sengaja dikosongkan)

BAB A

HASIL UJI COBA KEBENARAN PADA SITUS SPOJ

20809690		2017-11-16 06:24:28	The Bytelandian Cryptographer (Act IV)	accepted edit idone it	4.38	26M	CPP14
----------	---	------------------------	--	----------------------------------	------	-----	-------











Gambar 1.1 Hasil Uji Coba pada Situs Penilaian SPOJ



Gambar 1.2 Grafik Hasil Uji Coba pada Situs SPOJ Sebanyak 30 Kali

20609690	■	2017-11-09 06:24:26	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,38	26M	CPP14
20609689	■	2017-11-09 06:24:20	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,47	27M	CPP14
20609688	■	2017-11-09 06:24:10	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,44	26M	CPP14
20609686	■	2017-11-09 06:24:02	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,42	26M	CPP14
20609684	■	2017-11-09 06:23:52	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,41	26M	CPP14
20609682	■	2017-11-09 06:23:43	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,44	26M	CPP14
20609681	■	2017-11-09 06:23:36	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,41	26M	CPP14
20609680	■	2017-11-09 06:23:20	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,39	26M	CPP14
20609678	■	2017-11-09 06:23:20	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,39	26M	CPP14
20609675	■	2017-11-09 06:23:10	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,40	27M	CPP14
20609673	■	2017-11-09 06:23:05	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,40	26M	CPP14
20609672	■	2017-11-09 06:23:52	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,49	27M	CPP14
20609671	■	2017-11-09 06:23:43	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,43	27M	CPP14
20609669	■	2017-11-09 06:22:26	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,43	27M	CPP14
20609667	■	2017-11-09 06:22:19	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,40	27M	CPP14
20609664	■	2017-11-09 06:22:07	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,42	27M	CPP14
20609663	■	2017-11-09 06:21:56	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,40	26M	CPP14
20609663	■	2017-11-09 06:21:44	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,40	26M	CPP14
20609662	■	2017-11-09 06:21:36	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,41	26M	CPP14
20609661	■	2017-11-09 06:21:20	The Bytelandian Cryptographer (Act IV)	accepted edit delete 0	4,42	26M	CPP14

Gambar 1.3 Hasil Pengujian Sebanyak 30 Kali pada Situs Penilaian Daring SPOJ (1)

20609659		2017-11-16 06:21:21	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.40	26M	CPP14
20609657		2017-11-16 06:21:12	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.40	27M	CPP14
20609656		2017-11-16 06:21:02	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.42	26M	CPP14
20609655		2017-11-16 06:20:50	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.41	26M	CPP14
20609654		2017-11-16 06:20:32	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.40	27M	CPP14
20609652		2017-11-16 06:20:11	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.43	26M	CPP14
20609651		2017-11-16 06:20:00	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.42	27M	CPP14
20609650		2017-11-16 06:19:35	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.42	26M	CPP14
20603932		2017-11-15 12:19:55	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.42	27M	CPP14
20603856		2017-11-15 12:06:01	The Bytelandian Cryptographer (Act IV)	accepted edit ideone.it	4.44	27M	CPP14

Gambar 1.4 Hasil Pengujian Sebanyak 30 Kali pada Situs Penilaian Daring SPOJ (2)

RANK	DATE	USER	RESULT	TIME	MEM	LANG
1	2014-07-09 20:26:13	sidharth jain	accepted	0.21	18M	C++ 4.3.2
2	2011-02-04 10:11:14	Josef K.	accepted	0.32	9.0M	CPP
3	2010-02-25 22:16:52	Carlos Eduardo Rodrigues Alves [USJT]	accepted	0.33	31M	CPP
4	2011-06-04 01:25:06	NiHaobin	accepted	0.34	151M	CPP
5	2009-12-29 16:48:15	[Rampage] Blue.Mary	accepted	0.39	28M	C++ 4.3.2
6	2010-05-03 01:07:25	Carlos Eduardo Rodrigues Alves [USJT]	accepted	0.39	30M	C++ 4.3.2
7	2011-02-04 10:12:30	Josef K.	accepted	0.39	8.4M	C++ 4.3.2
8	2004-12-08 18:13:03	Jakub Łopuszański	accepted	0.42	14M	CPP
9	2009-03-07 01:11:57	Robert Gerbicz	accepted	0.42	33M	CPP
10	2010-04-23 11:23:55	Oleg	accepted	0.44	7.5M	C++ 4.3.2
11	2004-11-27 07:22:27	Tomek Czajka	accepted	0.53	4.3M	CPP
12	2007-05-31 03:54:03	Huacheng Yu	accepted	0.60	17M	C
13	2010-07-02 12:47:04	刘启鹏	accepted	0.61	17M	C
14	2010-12-18 14:59:02	sevenkplus	accepted	0.70	21M	C++ 4.3.2
15	2010-12-18 14:55:16	sevenkplus	accepted	0.77	21M	CPP
16	2011-03-05 23:42:24	Alexander Pivovarov	accepted	0.77	118M	CPP
17	2013-08-02 09:56:37	Tomasz Stanislawski	accepted	0.77	14M	C99
18	2011-06-06 13:20:16	blashyrkh	accepted	0.80	23M	C
19	2007-05-31 01:58:27	FG	accepted	0.95	2.7M	PAS- FPC
20	2008-03-19 03:57:13	zhengxi	accepted	0.98	52M	CPP

Gambar 1.5 Peringkat yang lebih tinggi dari program ini (1)

RANK	DATE	USER	RESULT	TIME	MEM	LANG
21	2009-06-22 16:57:33	QIZiChao	accepted	0.98	13M	CPP
22	2007-09-08 22:37:16	Sandeep Kumar	accepted	1.24	17M	CPP
23	2006-08-31 22:54:06	Tijs van Bakel	accepted	1.32	59M	CPP
24	2007-02-04 18:33:29	James Cook	accepted	1.52	10M	C
25	2010-09-14 13:48:55	Laxminarayana	accepted	1.57	12M	C++ 4.3.2
26	2013-02-05 03:27:04	roginn	accepted	1.60	3.9M	C++ 4.3.2
27	2009-11-01 21:00:00	anonymous	accepted	1.64	3.1M	C++ 4.3.2
28	2011-08-06 21:38:41	Peutri	accepted	1.91	2.8M	C++ 4.3.2
29	2004-11-18 17:26:14	Pascal Zimmer	accepted	1.94	7.2M	C
30	2005-02-03 10:06:50	Tim Green @ Ark	accepted	1.94	13M	CPP
31	2015-09-03 20:00:03	vijaygbvv	accepted	2.36	5.6M	C++ 4.3.2
32	2011-08-23 16:06:32	Darren Izzard	accepted	2.48	3.1M	C++ 4.3.2

Gambar 1.6 Peringkat yang lebih tinggi dari program ini (2)

(Halaman ini sengaja dikosongkan)

BIODATA PENULIS



Freddy Hermawan Yuwono, kelahiran & besar di Bondowoso-Jawa Timur, sangat suka membaca. Penulis menempuh jenjang pendidikan S1 Teknik Informatika ITS dari tahun 2013 sampai dengan dibuatnya buku ini.

Motto penulis yaitu "Segala sesuatu pasti akan terjadi dan pasti akan dilewati", membawa penulis mencoba belajar yang baru topik tugas akhir ini, dimana penulis dapat menerapkan sesuatu yang belum pernah penulis untuk melakukannya. Algoritma, optimasi dan pelajaran yang penulis petik dari yang pernah dilakukan oleh penulis sebelumnya, dengan bimbingan dosen-dosen pembimbing. Dalam pendalaman topik tugas akhir ini juga, penulis banyak belajar dan menjadi sangat tertarik mendalami *cryptography*, dan *data scientist*.

Dengan segala kerendahan hati, ilmu penulis masihlah setitik dibandingkan susu sebelanga. Penulis sangat mengharapkan diskusi, ajaran dan bantuan dalam memperbaiki diri. Apabila pembaca berkenan, penulis dapat dihubungi melalui *email* ke freddy.yuwono@gmail.com.