MODIFIKASI *CAESAR CIPHER* UNTUK MENGHASILKAN *READABLE CIPHERTXT*

SKRIPSI

OLEH
ALFIATUS SHOLEHAH
NIM. 17610082

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

MODIFIKASI *CAESAR CIPHER* UNTUK MENGHASILKAN *READABLE CIPHERTXT*

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
ALFIATUS SHOLEHAH
NIM. 17610082

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2022

MODIFIKASI *CAESAR CIPHER* UNTUK MENGHASILKAN *READABLE CIPHERTXT*

SKRIPSI

Oleh
Alfiatus Sholehah
NIM. 17610082

Telah Diperiksa dan Disetujui untuk Diuji

Malang, 15 Juni 2022

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Dr. H. Imam Sujarwo, M.Pd
NIDT 19900511 20160801 1 057	NIP. 19630502 198703 1 005

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

MODIFIKASI *CAESAR CIPHER* MENGGUNAKAN *READABLE CIPHERTEXT*

SKRIPSI

Oleh
Alfiatus Sholehah
NIM. 17610082

Telah Dipertahankan di Depan Penguji Seminar Hasil Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 22 Juni 2022

Ketua Penguji : Hisyam Fahmi, M. Kom .....

Anggota Penguji 1 : Mohammad Nafie Jauhari, M.Si .....

Anggota Penguji 2 : Muhammad Khudzaifah, M.Si .....

Anggota Penguji 3 : Dr. H. Imam Sujarwo, M.Pd .....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

PERNYATAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Alfiatus Sholehah

NIM : 17610082

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Modifikasi *Caesar Cipher* Menggunakan *Readable Ciphertext*

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila di kemudian hari terbukti atau dapat dibuktikan hasil skripsi saya ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 20 Juni 2022

Yang membuat pernyataan,

Alfiatus Sholehah

NIM. 17610082

MOTO

“Menjadi cerdas tidaklah cukup, pun menjadi kuat juga tidaklah cukup. Maka dari itu, cerdaslah untuk menjadi kuat, dan kuatlah untuk menjadi cerdas”.

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Kedua orang tua, ayahanda Sucipto, S.Pd.I dan ibunda Rosyidah yang senantiasa membimbing dan mencurahkan seluruh kasih sayangnya serta seluruh keluarga, sahabat, dan teman yang selalu mendukung.

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh

Puji syukur penulis panjatkan ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan sksipsi ini sebagai syarat memperoleh gelar sarjana matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna, maka dari itu penulis mengharapkan saran dan kritik yang membangun dari semua pihak demi kesempurnaan skripsi ini dan penulis juga mengharapkan skripsi ini dapat menjadi sumber informasi serta pengetahuan baru bagi penelitian – penelitian selanjutnya.

Ucapan terimakasih yang sebesar – besarnya penulis sampaikan kepada setiap pihak yang telah memberikan bimbingan, dukungan serta bantuan di berbagai hal terutama kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Dr. H. Imam Sujarwo, M.Pd, selaku dosen pembimbing I.
5. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing II.
6. Hisyam Fahmi, M.Kom, selaku penguji utama dalam seminar proposal.
7. Ach. Nashichuddin, M.A selaku dosen wali.
8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
9. Orang tua saya, yakni yayah (Sucipto, S.Pd.I) dan mama (Rosyidah) yang senantiasa ikhlas memberikan do'a, bimbingan serta dukungan yang tiada henti bagi penulis.

10. Seluruh keluarga khususnya kakak perempuan saya (Arini Hidayati) serta almarhum kakek (Muja'in) dan nenek (Maryama) yang juga memberikan dukungan serta do'a.
11. Kedua ponakan saya (Idad dan Kayla) yang menjadi penghibur ketika penulis merasa jenuh dalam proses pengerjaan skripsi.
12. Seluruh mahasiswa angkatan 2017 khususnya Program studi matematika (MAGΣNTA).
13. Sahabat – sahabat PMII Rayon *Pencerahan* Galileo (khususnya Dirgantara) dan Komisariat Sunan Ampel Malang yang telah memberikan ruang bagi penulis untuk berproses menimba ilmu dan pengalaman.
14. Teman-teman HMJ "Integral" Matematika, DEMA-FST Kabinet Metamorfosa Cita dan DEMA-U Kabinet Sakti yang telah memberikan wadah bagi penulis untuk berproses.
15. Bagus Setio Nugroho yang senantiasa setia menemani dan memberikan dukungan serta do'a dalam proses penyelesaian skripsi.
16. Keluarga besar Komunitas Averroes yang telah memberikan tempat berproses bagi penulis dalam memperoleh ilmu dan pengalaman.

Malang, 30 Mei 2022

Penulis

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PENGAJUAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PENGESAHAN ..... **iv**
PERNYATAAN KEASLIAN TULISAN ..... **v**
MOTO ..... **vi**
PERSEMBAHAN ..... **vii**
KATA PENGANTAR ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR TABEL ..... **xii**
DAFTAR GAMBAR ..... **xiii**
ABSTRAK ..... **xiv**
ABSTRACT ..... **xv**
ملخص ..... **xvi**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Manfaat Penelitian 4
1.5 Batasan Masalah 4
1.6 Definisi Istilah 5
BAB II KAJIAN TEORI **7**
2.1 Teori Pendukung 7
2.1.1 Keterbagian 7
2.1.2 Aritmatika Modulo 12
2.1.3 Kongruensi 13
2.1.4 Kriptografi 14
2.1.5 Tujuan Kriptografi 16
2.1.6 Jenis-jenis Kriptografi 17
2.1.7 Kriptografi Klasik 18
2.1.8 Algoritma Kriptografi 20
2.1.9 Karakteristik Sistem Kriptografi 21
2.1.9.1 Tipe Operasi yang Dipakai dalam Enkripsi dan Dekripsi 21
2.1.9.2 Tipe Kunci yang Dipakai 21
2.1.9.3 Tipe Pengolahan Pesan 22
2.1.10 *Monoalphabetic Caesar Cipher* 22
2.1.11 Keamanan Data 24
2.1.12 Modifikasi *Caesar Cipher* 26
2.1.13 *Readable Ciphertext* 29
2.2 Kajian Kriptografi Dalam Perspektif Islam 29
2.3 Kajian Topik Dengan Teori Pendukung 31

BAB III METODE PENELITIAN 32
3.1 Jenis Penelitian 32
3.2 Pra Penelitian 32
3.3 Tahapan Penelitian 33
3.3.1 Modifikasi Caesar Cipher untuk Menghasilkan Readable Ciphertext 33
BAB IV HASIL DAN PEMBAHASAN 36
4.1 Menyusun Enkripsi Algoritma *Caesar Cipher* Modifikasi untuk Menghasilkan *Readable Ciphertext* 36
4.1.1 Frekuensi Alfabet Pada Teks Bahasa Indonesia 36
4.1.2 Membuat Sandi Monoalfabetik 40
4.1.3 Melakukan Pengujian *Caesar Cipher* Modifikasi 40
4.2 Menyusun Dekripsi Algoritma *Caesar Cipher* Modifikasi untuk Menghasilkan *Readable Ciphertext* 42
4.3 Hasil Pengujian Lain 43
BAB V PENUTUP 46
5.1 Kesimpulan 46
5.2 Saran 47
DAFTAR PUSTAKA 48
LAMPIRAN 49

DAFTAR TABEL

Tabel 2.1 Skema Pergeseran Caesar Cipher 22
Tabel 2.2 Enkripsi Awas Ada Bahaya 23
Tabel 2.3 Frekuensi Kemunculan Alfabet dalam Bahasa Indonesia 24
Tabel 4.1 Substitusi Huruf Vokal pada Caesar Cipher Modifikasi.....38
Tabel 4.2 Substitusi Huruf Konsonan pada Caesar Cipher Modifikasi 39
Tabel 4.3 Jumlah Substitusi pada Setiap Alfabet.....40
Tabel 4.4 Hasil Pengujian Ada Musuh Caesar Cipher Modifikasi 41
Tabel 4.5 Hasil Pengujian Lain.....44

DAFTAR GAMBAR

Gambar 2.1 Proses Kriptografi 21
Gambar 3.1 Diagram Alir Proses Enkripsi 34
Gambar 3.2 Diagram Alir Proses Dekripsi 35

ABSTRAK

Sholehah, Alfiatus. 2022. **Modifikasi *Caesar Cipher* untuk menghasilkan *Readable Ciphertext*.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Dr. H. Imam Sujarwo, M.Pd.

Kata kunci : Modifikasi, Caesar, *Cipher*, *Ciphertext*, Frekuensi, Algoritma.

Kriptografi merupakan salah satu metode pengamanan pesan dari serangan pihak luar, dengan adanya serangan ini maka diperlukan pengamanan agar pesan yang ingin disampaikan tidak mudah terbaca. Pengamanan pesan dapat dilakukan dengan cara memodifikasi metode yang sudah ada, salah satunya metode *Caesar cipher*. Pada semua percobaan modifikasi yang dilakukan, *ciphertext* yang dihasilkan masih berupa karakter yang acak sehingga hal ini akan menimbulkan kecurigaan dan upaya pemecahan pesan oleh pihak lain. Dalam penelitian in dilakukan modifkasi *Caesar cipher* untuk menghasilkan *ciphertext* yang dapat dibaca dan memiliki makna dalam Bahasa Indonesia.

Tujuan dari penelitian ini adalah untuk mengamankan pesan dengan menghasilkan *ciphertext* yang masih dapat dibaca dan memiliki makna dalam Bahasa Indonesia, sehingga dengan hasil ini tidak menimbulkan kecurigaan orang lain. Modifikasi ini dilakukan dengan mengelompokkan huruf dalam Bahasa Indonesia sesuai dengan frekuensi kemunculan dalam penggunaannya, kemudian huruf – huruf tersebut disubstitusi dengan huruf lain sesuai dengan algoritma yang sudah dibuat. Pada penelitian ini dilakukan proses enkripsi dan dekripsi untuk menguji keberhasilan algoritma yang dihasilkan.

ABSTRACT

Sholehah, Alfiatus. 2022. **Caesar Cipher Modification to Generate Readable Ciphertext.** Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Dr. H. Imam Sujarwo, M.Pd.

Cryptography is one method of securing messages from external attacks, by this attack, security is needed so that the message to be conveyed is not easily readable. Message security can be done by modifying existing methods, one of which is the Caesar cipher method. In all modification experiments carried out, the resulting ciphertext is still a random character, so it will raise suspicion and attempt to solve the message by other people. In this study, Caesar cipher modification was carried out to produce a ciphertext that can be read and has meaning in Indonesian.

The purpose of this research is to secure the message by producing a ciphertext that can still be read and has meaning in Indonesian so that this result does not arouse the suspicion of others. This modification is done by grouping the letters in Indonesian according to the frequency of occurrence in their use, then the letters are substituted with other letters according to the algorithm that has been made. In this study, encryption and decryption processes were carried out to test the success of the resulting algorithm.

ملخص

الصا لحة، الفية. 2022. **قم بتعديل *Caesar Cipher* لإنتاج *Readable Ciphertex*t**. البحث الجامعي. برنامج دراسة الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك ابراهيم الاسلامية الحكومية مالانج. المشرف: (1) محمد جظيفة الماجستير. (2) الدكتور الحاج إمام سوجاروى الماجستير

الكلمات الاساسية: التعديل، *Caesar*، *Cipher*، *Ciphertext*، تردد، الخوارزمية.

التشفير هو إحدى طرق تأمين الرسائل من الهجمات الخارجية، مع هذا الهجوم، يكون الأمان مطلوبًا بحيث لا يمكن قراءة الرسالة المراد نقلها بسهولة. يمكن عمل أمان الرسائل عن طريق تعديل الطرق الحالية، إحدى هذه الطرق هي طريقة *Caesar Cipher*. في جميع تجارب التعديل التي تم إجراؤها، لا يزال *Ciphertext* الناتج حرفًا عشوائيًا بحيث يثير هذا الشك ويحاول الطرف الآخر حل الرسالة. في هذا البحث، تم إجراء تعديل *Caesar Cipher* لإنتاج *Ciphertext* يمكن قراءته وله معنى باللغة الإندونيسية.

الغرض من هذا البحث هو تأمين الرسالة من خلال إنتاج *Ciphertext* ليزال من الممكن قراءته وله معنى باللغة الإندونيسية، بحيث لا تثير هذه النتيجة شكوك الآخرين. يتم هذا التعديل من خلال تجميع الأحرف في اللغة الإندونيسية وفقًا لتكرار حدوثها في استخدامها، ثم يتم استبدال الأحرف بأحرف أخرى وفقًا للخوارزمية التي تم إجراؤها. أجريت في هذه الدراسة عمليات التشفير و الوصف لاختبار نجاح الخوارزمية الناتجة.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Manusia sebagai makhluk sosial dalam kehidupannya sehari-hari pastilah membutuhkan manusia yang lain. Dalam proses hubungannya dengan manusia lain, manusia membutuhkan bahasa sebagai pengantar komunikasi satu dengan yang lain. Dalam suatu keadaan tertentu, pesan yang ingin disampaikan antar dua manusia atau lebih terkadang tidak ingin diketahui oleh manusia yang lain atau bersifat rahasia. Untuk menjaga kerahasiaan pesan ini maka dibutuhkan suatu perilaku khusus agar pesan ini tidak dapat diketahui orang lain dan biasanya dibutuhkan kunci untuk membuka kembali pesan tersebut, dengan demikian pesan yang dimaksudkan hanya dapat dibaca oleh orang tertentu saja, yakni si pengirim dan penerima pesan. Berkaitan dengan penyampaian pesan terhadap pihak yag disinggung, terdapat penjelasan dalam al-quran yang berbunyi:

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum diantara manusia, supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberikan pengajaran yang sebaik-baiknya. Sesungguhnya Allah maha mendengar lagi maha melihat"

Seiring berkembangnya teknologi dan kebutuhan manusia yang semakin meningkat dapat dimanfaatkan untuk menciptakan suatu keamanan. Salah satu contohnya adalah keamanan pesan dalam berkomunikasi, keamaan merupakan hal yang diinginkan semua orang untuk menjaga privasi. Agar pesan yang dikirim

aman dari orang yang tidak bertanggung jawab, maka pesan tersebut disembunyikan menggunakan algoritma kriptografi (Ariyus, 2008). Kriptografi dibagi menjadi dua yaitu kriptografi klasik dan kriptografi *modern.* Di dalam kriptografi ada beberapa teknik dalam menyandikan pesan yaitu: teknik substitusi, teknik permutasi, teknik *blocking*, teknik ekspansi, dan teknik perampatan. Dengan beberapa teknik ini dapat dilakukan beberapa proses penyandian untuk merahasiakan sebuah pesan.

Dalam pesan rahasia, kriptografi lebih mengarah ke pesan yang dienkripsi sementara steganografi lebih mengarah pada pesan tersembunyi. Namun, kedua metode tersebut memiliki tujuan yang sama, yaitu upaya untuk menyembunyikan pesan. Di sisi lain, ternyata penggunaan kriptografi seringkali dapat diselesaikan atau diterjemahkan oleh orang lain atau kriptoanalis. Hal ini dimungkinkan karena biasanya pesan teks yang tidak dapat dibaca memberikan kecurigaan seseorang bahwa pesan teks tersebut mengandung arti tertentu bagi pemilik pesan.

Seiring berkembangnya teknologi dan ilmu pengetahuan, maka ancaman penyerangan atau pemecahan terhadap sandi kriptografi juga semakin berkembang. Caesar cipher sebagai salah satu jenis kriptografi klasik tentunya mengalami ancaman yang sama. Dengan teknik penyandian yang digunakan dalam Caesar cipher masih bersifat sederhana yakni menggunakan teknik substitusi dan transposisi, maka hasil penyandian tersebut akan mudah mengalami ancaman pemecahan atau penyerangan. Sehingga atas dasar tersebut maka diperlukan modifikasi terhadap teknik penyandian Caesar cipher agar tidak mudah terpecahkan oleh kriptanalis. Proses modifikasi yang dapat digunakan dalam penyandian ini sangat beragam sebagaimana telah disebutkan sebelumnya, yakni

dapat menggunakan teknik substitusi, permutasi, *blocking,* ekspansi, dan teknik perampatan.

Berdasarkan penelitian yang dilakukan (Pooja Singh, Pintu Sen, 2017) dalam penelitian yang berjudul "*Enhancing Security of Caesar Cipher Using Divide and Conquer Approach"* algoritma *caesar cipher* mudah dipecahkan karena pada umumnya hanya dilakukan dengan teknik substitusi dengan pergeseran tiga kali. Pada penelitian yang dilakukan (Pooja Singh, Pintu Sen, 2017) dibahas bagaimana memodifikasi *caesar cipher* dengan menggunakan teknik substitusi dan membalikkan posisi masing-masing huruf lalu mengelompokkannya menjadi masing-masing dua huruf, kemudian tiga huruf dan kemudian mengacaknya lagi. Dikarenakan hasil enkripsi dalam modifikasi ini masih terlihat acak dan memungkinkan timbulnya kecurigaan dari orang lain bahwa sandi tersebut merupakan sandi kriptografi sehingga akan timbul peluang untuk diterjemahkan kembali, maka peneliti ingin memodifikasi *caesar cipher* menggunakan *readable ciphertext* sehingga *ciphertext* yang dihasilkan masih berupa kata yang dapat dibaca dan memiliki makna. Dengan ciphertext yang bisa terbaca, maka kriptanalis tidak mencurigai *ciphertext* tersebut.

Merujuk pada beberapa penelitian sebelumnya yang membuat modifikasi Caesar cipher dengan berbagai cara namun pada hasil enkripsinya masih berupa teks dengan karakter yang acak, sehingga dapat menimbulkan kecurigaan bagi orang lain terhadap hal tersebut dan akan menimbulkan kemungkinan pemecahan atau penyerangan terhadap sandi kriptografi yang telah dibuat, maka dalam penelitian ini Caesar cipher dimodifikasi menjadi kata atau kalimat yang bukan berupa karakter acak, akan tetapi masih berupa kata atau kalimat yang masih

memiliki arti atau makna dalam Bahasa Indonesia. Proses modifikasi ini dilakukan dengan tujuan agar sandi kriptografi yang telah dibuat sebelumnya tidak menimbulkan kecurigaan orang lain sehingga dapat meminimalisir proses penyerangan atau pemecahan.

1.2 Rumusan Masalah

1. Bagaimana proses enkripsi modifikasi *caesar cipher* untuk menghasilkan *readable ciphertext*?
2. Bagaimana proses dekripsi modfikasi *caesar cipher* untuk menghasilkan *readable ciphertext*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk memodifikasi *caesar cipher* untuk menghasilkan *readable ciphertext* sehingga menghasilkan ciphertext yang dapat dibaca dan memiliki makna.

1.4 Manfaat Penelitian

Beberapa manfaat yang terdapat dalam penelitian ini, di antaranya sebagai berikut:

1. Sebagai bahan pembelajaran dan pengetahuan mengenai proses modifikasi *Caesar cipher* menggunakan *readable ciphertext*
2. Mencegah adanya pesan rahasia yang mudah terbaca

1.5 Batasan Masalah

Peneliti membatasi masalah dalam penelitian yang akan dibahas yaitu:

1. Hanya mengenkripsi alfabet.
2. Mengenkripsi Bahasa Indonesia.
3. Mengenkripsi 2 sampai 3 kata yang berhubungan.

4. Untuk karakter atau simbol dienkripsi dengan karakter atau simbol yang sama.

1.6 Definisi Istilah

Untuk menghindiri terjadinya kesalahpahaman dalam proses memahami istilah dalam penelitian ini, maka perlu adanya batasan-batasan pengertian sebagai berikut:

1. Kriptografi adalah teknik menyampaikan pesan rahasia secara tersembunyi dengan menggunakan fitur enkripsi data.
2. Kriptanalis adalah orang yang melakukan proses pemecahan kode atau sandi tertentu sehingga dapat merubah ciphertext menjadi plaintext tanpa mengetahui algoritma yang dipakai.
3. *Cipher* atau sandi adalah kode, kata atau pesan rahasia.
4. Enkripsi adalah proses penyandian atau pengubahan suatu informasi dan pesan yang ingin dikirim menjadi bentuk yang hampir tidak dikenali dengan menggunakan algoritma tertentu.
5. Dekripsi adalah proses pengembalian bentuk pesan tersembunyi menjadi pesan awal yang disampaikan atau sebelum pesan tersebut mengalami proses enkripsi.
6. *Plaintext* adalah sebuah pesan atau data yang masih berupa bentuk asli dan belum mengalami proses penyandian.
7. *Ciphertext* adalah bentuk pesan atau data yang telah mengalami proses penyandian atau proses enkripsi.
8. Modifikasi adalah proses pengubahan bentuk sesuatu menjadi bentuk yang lain tanpa menghilangkan fungsi aslinya.

9. *Key line* adalah baris kunci atau letak posisi hasil kata yang dienkripsi.
10. Substitusi adalah penggantian setiap karakter asli menjadi karakter atau bentuk yang lain.
11. Algoritma yaitu metode atau ketentuan-ketentuan yang digunakan untuk melakukan proses enkripsi atau dekripsi.
12. Frekuensi adalah ukuran jumlah terjadinya suatu peristiwa dalam satuan waktu, dalam konteks penelitian ini adalah jumlah munculnya masing-masing alfabet dalam teks Bahasa Indonesia.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

Beberapa teori yang mendukung penelitian ini diambil atau dikutip dari beberapa buku dan jurnal yang relevan. Teori yang akan dibahas dalam penelitian ini meliputi, keterbagian, aritmatika modulo, kongruensi, kriptografi, tujuan, jenis–jenis, algoritma dan karakteristik kriptografi, serta *Caesar cipher monoalphabetic*. Berikut penjelasan tentang teori-teori yang dibahas dalam penelitian ini.

2.1.1 Keterbagian

Definisi 2.1 *Misalkan* $a, b \in Z$*, dengan* $a \neq 0$*, maka* a *disebut membagi* b *ditulis sebagai* $a|b$ *apabila* $b = ak$ *untuk suatu* $k \in Z$

Dari definisi tersebut, suatu bilangan bulat a dengan $a \neq 0$, dikatakan membagi bilangan bulat b jika ada suatu bilangan bulat k sedemikian hingga $b = ak$. Notasi $a|b$ dibaca dengan "a membagi b" atau "b habis dibagi a" atau "a pembagi b" atau "a faktor dari b", atau "b kelipatan dari a". Jika a tidak membagi b, maka ditulis sebagai $a \nmid b$. Jika $a|b$ dan $0 < a < b$, maka a disebut pembagi sejati dari b. (Henky, Hijriyah, Riza, 2014)

Teorema 2.1 *Untuk sebarang bilangan bulat a, b, c berlaku*

1. *Jika* $a|b$*, maka* $a|bc$ *untuk setiap bilangan bulat* $c; a \neq 0$.
2. *Jika* $a|b$ *dan* $b|c$*, maka* $a|c; a \neq 0, b \neq 0$.

3. *Jika* $a|b$ *dan* $a|c$, *maka* $a|b \pm c; a \neq 0$.
4. *Jika* $a|b$ *dan* $a|c$, *maka* $a|(bx \pm cy)$ *untuk setiap bilangan bulat x dan y; dengan* $a \neq 0$.
5. *Jika* $a|b$ *dan* $b|a$, *maka* $a = \pm b; a \neq 0, b \neq 0$.
6. *Untuk suatu bilangan bulat* $k \neq 0, a|b$ *jika dan hanya jika* $ka|kb$ *dan* $a \neq 0$.

Bukti:

1. $a|b$ berarti $b = ak$ untuk suatu $k \in Z$ (menurut definisi)

   $bc = (ak)c$ untuk setiap $c \in Z$ (dikalikan dengan *c*)

   $bc = a(kc)$ dengan $kc \in Z$ (asosiatif perkalian)

   Berarti, $a|bc$ (terbukti)

2. $a|b \rightarrow b = ak$ untuk suatu $k \in Z$

   $b|c \rightarrow c = bt$ dengan $t \in Z$

   Substitusikan b pada persamaan kedua diperoleh

   $$c = (ak)t$$

   $c = a(kt)$ untuk suatu $kt \in Z$ (asosiatif perkalian)

   Jadi $a|c$ (terbukti)

3. $a|b \rightarrow b = ak_1$; untuk suatu $k_1 \in Z$ (i (menurut definisi))

   $a|c \rightarrow c = ak_2$; untuk suatu $k_2 \in Z$ (ii (menurut definisi))

   Keduanya dijumlahkan sehingga diperoleh

   $b + c = a(k_1 + k_2)$ dengan $(k_1 + k_2) \in Z$

   Maka sesuai definisi berlaku $a|b + c$

   Begitu pula dengan mengurangkan (i) dan (ii) maka diperoleh

$b + c = a(k_1 - k_2)$ dengan $(k_1 - k_2) \in Z$

Maka sesuai definisi berlaku $a|b - c$

Jadi, $a|b \pm c$ (terbukti)

4. $a|b \rightarrow b = ak_1$; untuk suatu $k_1 \in Z$ (menurut definisi)

   $a|c \rightarrow c = ak_2$; untuk suatu $k_2 \in Z$ (menurut definisi)

   Dari $b = ak_1$

   Maka $bx = (ak_1).x$, dengan $x \in Z$ (i (dikalikan *x*))

   Begitu pula $c = ak_2$ maka $cy = (ak_2)y$,

   dengan $y \in Z$ (ii (dikalikan *y*))

   dengan menjumlahkan (i) dan (ii) diperoleh

   $$bx + cy = (ak_1)x + (ak_2)y$$

   $bx + cy = a(k_1x + k_2y)$ untuk suatu $(k_1x + k_2y) \in Z$

   Maka sesuai definisi berlaku $a|(bx \pm cy)$

   Begitu pula bila mengurangkan (i) oleh (ii) maka diperoleh

   $$bx - cy = (ak_1)x - (ak_2)y$$

   $bx - cy = a(k_1x - k_2y)$ untuk suatu $(k_1x - k_2y) \in Z$

   Maka sesuai definisi berlaku $a|(bx \pm cy)$

5. $a|b \rightarrow b = ak$; untuk suatu $k \in Z$ (i(menurut definisi))

   $b|a \rightarrow a = bt$; untuk suatu $t \in Z$ (ii(menurut definisi))

   Substitusi *a* pada (i) diperoleh

   $$b = (bt)k = b(tk) = b(1 - tk) = 0$$

   Karena $b \neq 0$, maka $1 - tk = 0$ atau $k = t = -1$

   Selanjutnya substitusikan ke (i) dan (ii) sehingga diperoleh $= \pm b$.

Demikian pula dengan mensubstitusi b pada (ii) diperoleh

$a(1-kt)=0$. Karena $a \neq 0$, maka $1-tk=0$ atau $kt=1$ sehingga $a=\pm b$.

6. Jika $a|b$, maka $b=ak$ untuk suatu $k \in Z$ (menurut definisi)

   Karena $a>0, b>0$ dan $b=ak$, maka $k>0$

   Untuk $k=1$ maka diperoleh $a=b$, sedangkan untuk $k>1$ maka $b>a$.

   Karena $a>b$ dan $a=b$, jadi $a \leq b$ (terbukti)

7. (←) jika $a|b$, maka $b=ak$ untuk suatu $k \in Z$ (menurut definisi)

   $mb=m(ak)$ untuk suatu $m \in Z$ dan $m \neq 0$ (kalikan m)

   $=(ma)k$ untuk suatu $k \in Z$ (asosiatif perkalian)

   Jadi $ma|mb$

   (←) jika $ma|mb$ dan $m \neq 0$, maka $mb=(ma)k$ untuk suatu $k \in Z$

   Sehingga $mb=(ma)k$

$$mb-(ma)k=0$$

$$m(b-ak)=0$$

   Karena $m \neq 0$, maka $b-ak=0$ atau $b=ak$ untuk suatu $k \in Z$

   Jadi $a|b$

Teorema 2.2 (Algoritma Pembagian) *untuk sebarang bilangan bulat a dan b dengan* $a>0$, *maka terdapatlah dengan tunggal bilangan bulat q dan r sedemikian hingga hubungan bilangan a dan b dapat dinyatakan sebagai*

$b=qa+r, 0 \leq r<a$

Jika $a|b$ *maka* r *memenuhi ketaksamaan* $0<r<a$.

Bukti:

Perhatikan barisan aritmatika

$$\dots, b-3a, b-2a, b-a, b, b+a, b+2a, b+3a, \dots$$

Jika diketahui bilangan bulat a dan b, maka barisan ini dapat dinyatakan dalam bentuk umum sebagai $b-qa$ dengan $q \in Z$.

Barisan bilangan ini ditulis sebagai himpunan $S = \{(b-qa|qc\}$

Selanjutnya ambil himpunan T yang semua elemen-elemennya adalah elemen-elemen himpunan T yang tidak negatif, yaitu:

$$T = \{(b-qa)|q \in Z, b-qa \geq 0\}$$

Maka diperoleh

(1) $T \neq 0$

(2) Bila $b \geq 0$ dan $q = 0$ maka $b \in T$

(3) Bila $b < 0$ dan $q = b$, maka $b - ba = b(1-a) \in S$

Di pihak lain $b - ba = b(1-a) \geq 0$

Oleh karena $b < 0$ dan $a > 0$ atau $a \geq 1$ atau $1 - a \leq 0$

Sehingga $b - ba \in T$

Menurut prinsip urutan, maka T mempunyai elemen terkecil, misalnya r, maka r ini dapat dinyatakan sebagai $r = b - qa$ atau $b = qa + r$ dan berlaku bahwa $r \geq 0$

Selanjutnya akan dibuktikan bahwa $r < a$

Misalkan $r \geq a$ atau $0 \leq r - a$

Karena $r = b - qa$ maka $0 \leq r - a = b - qa - a = b - a(q+1) \in T$

Tetapi $b - a(q+1) = b - qa - a = r - a < r$ (karena $a > 0$)

Sehingga terlihat disini ada elemen $r - a \in T$ yang lebih kecil dari r. Hal ini kontradiksi bahwa r adalah elemen terkecil dari T.

Jadi pengandaian salah sehingga diperoleh bahwa $r < a$.

Dari $r \geq 0$ dan $r < 0$, maka $0 \leq r < a$ sehingga $b = qa + r$ untuk $0 \leq r < a$

Kemudian akan ditunjukkan bukti ketunggalan untuk q dan r. Andaikan terdapatlah q_1 dan q_2 dengan $q_1 \neq q_2$ maka terdapatlah r_1 dan r_2 dengan $r_1 \neq r_2$.

Sehingga:

$b = q_1 a + r_1$ untuk $0 \leq r_1 < a$

dan $b = q_2 a + r_2$ untuk $0 \leq r_2 < a$

dengan substitusi b diperoleh $q_1 a + r_1 = q_2 a + r_2$

$a(q_1 - q_2) = r_2 - r_1$ yang berarti $a|(r_1 - r_2)$ ……(1)

Di pihak lain $0 \leq r_1 < a$ dan $0 \leq r_2 < a$ sehingga

$-a < (r_2 - r_1) < a$ …… (2)

Satu-satunya kelipatan a yang terletak diantara $-a$ dan a adalah 0 sehingga

$r_2 - r_1 = 0$ berakibat $r_2 = r_1$ sehingga $a(q_1 - q_2) = 0$

Karena $a > 0$ maka $q_1 - q_2 = 0$ atau $q_2 = q_1$

Jadi q dan r masing-masing adalah tunggal.

2.1.2 Aritmatika Modulo

Penggunaan aritnatika modulo (*modular arithmetic*) dengan operator mod memiliki peranan penting dalam perhitungan bilangan bulat, salah satunya dalam kriptografi. Penggunaan operator mod dalam pembagian

bilangan bulat akan menghasilkan sisa pembagian. (Sansani, 2008).

Berikut definisi operator mod:

Definisi 2.2 *misalkan* p *dan* n *merupakan bilangan bulat dengan* $n > 0$. *Operasi* $p \bmod n$ *(dibaca "p modulo n") menghasilkan sisa jika* p *dibagi dengan* n. *Dapat dinyatakan pula sebagai* $p \bmod n = r$ *sedemikian sehingga* $p = nq + r$, *dengan* $0 \leq r < n$ (Sansani, 2008)

Jika p merupakan kelipatan dari n, maka diperoleh $p \bmod n = 0$, yaitu n membagi habis p.

Contoh 2.1

(i) $32 \bmod 5 = 2, (32 = 5.6 + 2)$

(ii) $0 \bmod 10 = 0, (0 = 10.0 + 0)$

(iii) $-26 \bmod 3 = 1, (-26 = 3.-9 + 1)$

2.1.3 Kongruensi

Konsep kongruensi digunakan dalam keterbagian bilangan bulat beserta sifat-sifatnya (Henky, Hijriyah, Riza, 2014).

Definisi 2.3 *jika sebuah bilangan bulat* M *tak nol, membagi selisih* $a - b$, *maka dikatakan* a *kongruen dengan* b *modulo* M, *ditulis:*

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

Jika $a - b$ *tidak membagi* M, *maka dikatakan* a *tidak kongruen dengan* $b \bmod M$ *dan dituliskan* (Henky, Hijriyah, Riza, 2014)*:*

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

Kekongruenan $a \equiv b \pmod{M}$ *dapat dituliskan pula dalam bentuk:*

$$a = b + km$$

Dengan k merupakan bilangan bulat (Munir, Teori Bilangan, 2004).

Teorema 2.3 *diberikan sebarang bilangan asli* $n > 1$. Untuk setiap $a, b, c, d \in \mathbb{Z}$. Berlaku:

1. $a \equiv a \bmod n$.
2. Jika $a \equiv b \bmod n$ maka $b \equiv a \bmod n$.
3. Jika $a \equiv b \bmod n$ maka $a + c \equiv b + c \bmod n,\ a - c \equiv b - c \bmod n$, dan $ac \equiv bc \bmod n$.
4. Jika $a \equiv b \bmod n$ dan $c \equiv d \bmod n$ maka $ac \equiv bd \bmod n$

Contoh 2.2

(i) $29 \equiv 2(mod\ 9)$ dapat dituliskan sebagai $29 = 2 + 3.9$

(ii) $-13 \equiv 14(mod\ 9)$ dapat dituliskan sebagai $-13 = 14 + (-3).9$

2.1.4 Kriptografi

Kriptografi adalah ilmu yang merancang metode yang memungkinkan informasi untuk dikirim dalam form yang aman sehingga satu-satunya orang yang dapat mengambil informasi ini adalah penerima yang dimaksud. Pada masa-masa awal, kriptografi dilakukan dengan menggunakan teknik manual. Kerangka dasar untuk melakukan kriptografi kurang lebih sama, tentu saja dengan banyak perbaikan dalam implementasinya.

Kriptologi bukanlah hal baru; kriptografi telah ada selama lebih dari 2000 tahun dan dikenalkan oleh orang-orang Mesir Kuno lewat *hieroglyph* dan jenis tulisan ini bukan bentuk standar dalam penulisan pesan. Dikisahkan pada Zaman Romawi Kuno, suatu hari Julius Caesar ingin mengirimkan pesan rahasia kepada Jendral di Medan Perang yang mana pesan tersebut

harus disampaikan melalui seorang kurir. Karena pesan tersebut bersifat rahasia, Julius Caesar tidak ingin pesan itu terbuka di jalan, kemudian ia memikirkan bagaimana cara mengatasi hal tersebut. Lalu dia mengacak pesan itu hingga menjadi pesan yang tidak bisa dipahami oleh siapapun kecuali Sang Jendral. Sebelumnya, tentu sang Jendral telah diberitahu mengenai bagaimana cara membaca pesan tersebut. Julius Caesar melakukan penggantian susunan huruf alphabet dari a, b, c dan seterusnya. Huruf a diganti dengan d, b menjadi e, c menjadi f begitu seterusnya.

Pada awalnya kriptografi hanya digunakan oleh pihak militer dan intelijen untuk menyandikan pesan, namun seiring berkembangnya teknologi kebutuhan sistem keamanan semakin besar dan pesat, sehingga semakin kompleks data yang harus diamankan. Maka kriptografi yang pada awalnya hanya digunakan oleh militer saat ini menjadi sangat populer seiring berjalannya waktu. Karena kriptografi dinggap sebagai metode keamanan yang baik, maka banyak organisasi atau pribadi yang menggunakannya karea teruji kemanannya.

Kriptografi adalah suatu area dalam bidang kriptologi. Nama kriptologi adalah kombinasi dari bahasa Yunani cryptos (tersembunyi) dan logos (ilmu, sains). Oleh karena itu, kata kriptologi secara harfiah menyiratkan ilmu penyembunyian. Sedangkan kata kriptografi sendiri juga berasal dari Bahasa Yunani, *crypto* yang berarti *secret* atau rahasia dan *graphia* yang berarti *writing* atau tulisan. Secara istilah kriptografi diartikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan berupa data atau informasi yang mempunyai arti atau nilai dengan cara mengacak atau

menyamarkan menjadi bentuk yang tidak dapat dimengerti dan haya dapat diubah kode-kode tersebut oleh penerima menjadi pesan asli yang dapat dimengerti.

Menurut Meneze dkk (2014), kriptografi adalah ilmu yang memperlajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data dan otentikasi. Sehingga dapat diambil kesimpulan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika untuk menjaga keamaan informasi.

2.1.5 Tujuan Kriptografi

Kriptografi adalah dasar keamanan komputer dalam jaringan yang menjadi pokok data atau informasi dengan sarana distribusinya adalah komputer. Kriptografi digunakan untuk menjaga data atau informasi yang dikirim bebas dari ancaman diketahui oleh pihak luar. Menurut Janner Simarmat dkk (2020), kriptografi sering digunakan untuk melakukan pekerjaan sebagai berikut:

1. *Confidentiality* (kerahasiaan) yakni layanan yang bertujuan agar pesan tidak mudah dibaca oleh pihak yang tidak berkepentingan. Dalam kriptografi layanan ini direalisasakan dalam bentuk penyandian pesan menjadi pesan yang tidak mudah terbaca.
2. *Authentication* (autentikasi) adalah layanan yang memiliki hubungan dengan identifikasi, baik mengidentifikasi kebenaran dari pihak-pihak yang berkomunikasi (*user authentication*) atau mengidentifikasi kebenaran dari sumber pesan (*data origin authentication*). Kedua pihak

yang saling berkomunikasi harus dapat mengidentifikasi satu dan yang lainnya sehingga dapat memastikan sumber pesan. Pesan yang dikirim lewat saluran komunikasi harus diautentikasi sumbernya.

3. *Data integrity* (integritas data) merupakan layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman. Agar integritas data terjaga, sistem yang digunakan harus memiliki kemampuan untuk mendeteksi pesan yang dimanipulasi oleh pihak-pihak lain seperti perubahan, penghapusan, dan penyisipan data lain ke dalam pesan yang sesungguhnya. Kriptografi layanan ini direalisasikan dengan menggunakan tanda tangan digital (*digital signature*).
4. *Non-repudiation* (tidak ada penyangkalan) adalah layanan yang digunakan dalam upaya mencegah entitas berkomunikasi menggunakan penyangkalan, yakni pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.1.6 Jenis-jenis Kriptografi

1. *Hash Function*

Hash function digunakan untuk meringkas data dan mengirimkan penjelasan yang telah dirangkum. Kriptografi jenis ini menggunakan algoritma matematika dengan cara mengambil nilai numerik sebagai sistem dan diringkas oleh *hash system*. Metode ini juga tidak memerlukan kunci karena telah disesuaikan dengan tahapan scenario pengiriman data berbasis satu arah (*direct*).

2. *Public Key Cryptography*

Public key cryptography adalah pengamanan data yang bersifat revolusioner dalam kurun waktu 300 sampai 400 taun terakhir. Istilah ini sering disebut sebagai kunci publik. Kriptografi ini memanfaatkan dua kunci yang saling berhubungan, yakni kunci publik dan kunci privat. Metode ini dianggap lebih aman jika dibandingkan dengan *symetric key.* Pada jenis ini sering digunakan metode RSA dan beberapa contoh lain yang terdapat DSA, PKC serta teknik kurva elips.

3. *Symetric Key Cryptohraphy*

Symetric Key Cryptohraphy disebut juga kunci rahasia yang berarti penerima dan pengirim informasi hanya memakai satu kunci dalam melakukan proses enkripsi. Jenis kriptografi yang digunakan pada metode ini adalah AES (*Advanced Encryption System*). Pendekatan yang dilakukan AES dianggap lebih efisien dibandingkan menggunakan metode lainnya.

Secara umum, berdasarkan sejarah kriptografi memiliki dua macam jenis, yakni kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah kriptografi yang menggunakan satu kunci dalam proses pengamanan data dan telah ada sejak berabad tahun yang lalu, sedangkan kriptografi modern tercipta karena berbagai perubahan yang terjadi disesuaikan dengan prioritas teknik yang digunakan untuk melindungi data privasi secara kontinu.

2.1.7 Kriptografi Klasik

Sebelum computer ada, kriptografi dilakukan dengan hanya menggunakan pensil dan kertas. Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik

ini sudah digunakan beberapa abad yang lalu. Menurut Rinaldi Munir (2006), terdapat tiga alasan mempelajari algoritma kriptografi klasik, yaitu:

1. Memberikan pemahaman konsep dasar kriptografi
2. Sebagai dasar dari algortima kriptografi modern, dan
3. Agar mudah memahami potensi-potensi kelemahan sistem cipher.

Umumya kriptografi klasik merupakan teknik penyandian dengan kunci simetrik dan menyembunyikan pesan yang memiliki arti ke sebuah pesan yang nampaknya tidak memiliki arti. Dua teknik dasar yang biasa digunakan pada algoritma jenis ini adalah sebagai berikut:

1. Teknik substitusi, penggantian setiap karakter teks-asli dengan karakter lain, ada empat istilah dari substitusi cipher diantaranya: monoalfabet, polyalfabet, monograph, dan polygraph. Sistem kriptografi berbasis substitusi diantaranya adalah *Caesar cipher, shift cipher,affine cipher, vignere cipher* dan *hill cipher*.
2. Teknik transposisi (permutasi), dilakukan dengan menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula atau disebut dengan dekripsi (Ariyus, 2008).

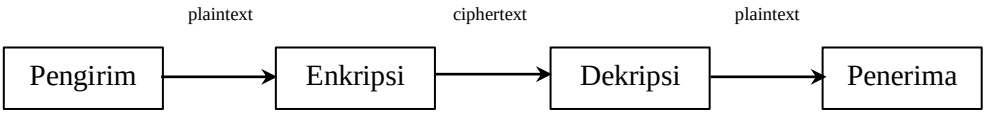
Salah satu teknik enkripsi menggunakan kunci simetri adalah teknik substitusi, yaitu mengganti setiap karakter *plaintext* dengan karakter lain. Terdapat empat cara dalam menggunakan teknik substitusi, yaitu:

1. *Monoalfabet*, dimana setiap karakter *ciphertext* mengganti satu macam karakter *plaintext* tertentu.

2. *Polialfabet*, dimana setiap karakter *ciphertext* mengganti lebih dari satu macam karakter *plaintext*.
3. *Monograf/unilateral*, dimana satu enkripsi dilakukan terhadap satu karakter *plaintext*.
4. *Poligraf/multilateral*, dimana satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext (Menezes, 1996).

2.1.8 Algoritma Kriptografi

Di bidang kriptografi, ada dua konsep terpenting yang disebut juga enkripsi dan dekripsi. Enkripsi merupakan proses suatu informasi atau pesan yang ingin dikirim akan diubah ke dalam bentuk yang hampir tidak dapat dikenali dengan menggunakan metode algoritma tertentu. Algoritma enkripsi memiliki dua masukan teks asli dan kunci rahasia. Sedangkan dekripsi merupakan lawan dari enkripsi, yaitu mengembalikan bentuk pesan tersembunyi tersebut menjadi pesan awal yang ingin disampaikan. Algoritma dekripsi memiliki dua masukan yaitu teks sandi dan kunci rahasia. Sebuah pesan atau data yang masih asli dan belum mengalami proses penyamaran disebut dengan kata plaintext. Kemudian setelah dilakukannya penyamaran dengan beberapa cara penyandian, maka plaintext itu disebut sebagai ciphertext. Dengan kata lain, proses penyamaran dari plaintext menjadi ciphertext disebut dengan istilah enkripsi (encryption), sedangkan proses mengubah kembali dari ciphertext ke plaintext disebut juga dengan istilah dekripsi (decryption).



Gambar 2.1 Proses Kriptografi

Secara fundamental, kriptografi dipakai untuk menawarkan sejumlah layanan keamanan digital:

- Enkripsi
- Fungsi hash
- MAC (*Message Authentication Codes*)
- Sidik (tanda tangan digital)

2.1.9 Karakteristik Sistem Kriptografi

2.1.9.1 Tipe Operasi yang Dipakai dalam Enkripsi dan Dekripsi

Tipe operasi yang dipakai dalam enkripsi dan dekripsi ada dua tipe, yakni substitusi dengan cara menukar atau mensubstitusi elemen pada pesan (karakter, byte atau bit) dengan elemen lain dari ruang pesan. Misalnya A ditukar dengan B, B dengan D dan C ditukar dengan Z, pesan "BACA" menjadi "DBZB". Tipe operasi yang kedua adalah transposisi, yakni dengan cara memindah posisi elemen pada pesan , misalnya posisi 1 menjadi posisi 4, posisi 2 menjadi pesan 3, posisi 3 menjadi posisi 1 dan posisi 4 menjadi posisi 2, pesan "AWAS" menjadi "AWSA"

2.1.9.2 Tipe Kunci yang Dipakai

Pada umumnya sistem kriptografi klasik dan beberapa sistem kriptografi modern menggunakan kunci yang sama pada sisi penyandi dan pengganti sandi. Sistem kriptografi ini disebut kriptografi dengan kunci simetri. Pada tahun 1976 sistem kriptografi yang memperbolehkan kunci

yang tidak sama diusulkan oleh Whitfield Deffie dan Martin Hellman.

2.1.9.3 Tipe Pengolahan Pesan

Ketika melakukan penyandian pesan yang akan dienkripsi atau didekripsi diolah menjadi blok elemen yang disebut dengan *block cipher.* Cara lain adalah dengan menganggap masukan untuk enkripsi dan dekripsi sebagai aliran elemen secara terus menerus disebut dengan *stream cipher*.

2.1.10 *Monoalfabetic Caesar Cipher*

Julius Caesar menggunakan sandi aditif untuk berkomunikasi dengan petugasnya. Karena alasan ini, sandi aditif terkadang disebut sebagai Caesar cipher. Caesar menggunakan kunci dalam 3 untuk komunikasinya. Dalam Kriptografi, sandi Caesar adalah salah satu algoritma dekripsi-enkripsi yang paling dikenal luas. Caesar cipher adalah sandi jenis substitusi. Dalam sandi jenis ini, setiap huruf dalam teks biasa diganti dengan huruf yang menduduki posisi dengan beberapa pergeseran. Enkripsi direpresentasikan menggunakan modular aritmatika. Misalnya dengan pergeseran 2, A akan diganti dengan D, B akan diganti dengan E, C akan diganti dengan F, dan seterusnya. Jadi, skema pergeseran dapat dilihat pada tabel 2.1. Baris pertama menunjukkan alfabet asli dan baris kedua menunjukkan alfabet pengganti.

Tabel 2.1 Skema Pergeseran Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C

Kemudian dapat dibuat algoritma sebagai berikut.

Untuk setiap huruf plaintext p, gantikan huruf ciphertext

$$C = E(3, p) = (p + 3)\ mod\ 26 \quad (1)$$

Pergeseran dapat berapapun jumlahnya, sehingga algoritma Caesar umumnya adalah:

$$C = E(k, p) = (p + k)\ mod\ 26 \quad (2)$$

Dimana k mengambil nilai dalam rentang 1 hingga 26. Sehingga menghasilkan algoritma dekripsi:

$$p = D(k, C) = (C - k)\ mod\ 26 \quad (3)$$

Bukti:

$C \equiv (p + k)\ mod\ 26$	definisi kongruensi
$26 \mid C - (p + k)$	definisi keterbagian
$C - (p + k) = 26.k, k \in Z$	sifat distributif
$C - p - k = 26.k$	sifat distributif
$-p + C - k = 26.k$	sifat komutatif
$(-p + C - k = 26.k)\ x - 1$	kedua ruas dikali -1
$p - C + k = 26.k$	sifat distributif
$p - (C - k) = 26.k$	sifat distributif
$26 \mid (p - (C - k))$	definisi keterbagian
$p \equiv (C + k)\ mod\ 26$	definisi kongruensi

Misalnya, pesan yang akan dienkripsi adalah Awas ada bahaya. Jadi ciphertext dalam contoh ini adalah Dzdvdgdedkdbd

Tabel 2.2 Enkripsi Awas Ada Bahaya

A	W	A	S		A	D	A		B	A	H	A	Y	A
D	Z	D	V		D	G	D		E	D	K	D	B	D

Caesar cipher dapat dipecahkan dengan cara *brute force* atau suatu bentuk dari sebuah serangan yang dimana mencoba kemungkinan –

kemungkinan untuk menemukan kunci sampai kunci itu dapat ditemukan sehingga membuat pesan dapat diterjemahkan.

Ada beberapa kelemahan Caesar cipher yang memungkinkan terkena serangan *brute force*, yaitu:

1. Algoritma enkripsi dan dekripsi diketahui.
2. Hanya 25 kunci yang dicoba.
3. Bahasa teks biasa dikenal dan mudah dikenali.

Banyaknya kunci dari suatu cipher cukup menarik perhatian para kriptanalis, namun walaupun dicoba dengan *Brute Force Attack* akan membutuhkan waktu untuk menemukan kunci ciphertext. Walaupun memerlukan waktu yang lama, cara ini cukup berhasil. Namun ada beberapa cara yang dapat dilakukan oleh kriptanalis dengan melihat frekuensi kemunculan huruf seperti pada tabel di bawah ini:

Tabel 2.3 Frekuensi Kemunculan Alfabet dalam Bahasa Indonesia

Huruf	Frekuensi Kemunculan (%)
A	17.50
N	10.30
I	8.70
E	7.50
K	5.65
T	5.10
R	4.60
D	4.50
S	4.50
M	4.50

Sumber: Buku Kriptografi Keamanan Data dan Komunikasi (Dony Ariyus, 2006)

2.1.11 Keamanan Data

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Informasi menentukan hampir setiap elemen dari

kehidupan manusia. Keberadaan informasi juga sangat penting bagi kehidupan manusia karena tanpa adanya informasi hampir semuanya tidak dapat dilakukan dengan baik.

Secara definisi keamanan data merupakan usaha untuk menjamin dan melindungi tiga aspek terpenting dalam dunia *cyber*, yakni:

1. Kerahasiaan data,
2. Keutuhan data, dan
3. Ketersediaan data

(Garfinkel & Lipford, 2014)

Kerahasiaan data menjamin pengguna terlindungi privasinya. Baik privasi yang berada pada computer pribadi, gadget, atau saat melakukan aktivitas jelajah internet. Sementara keutuhan data menjamin pengguna mendapatkan data yang utuh dan valid tanpa dimodifikasi dan dirubah oleh pihak lain. Sedangkan ketersediaan data menjamin pengguna mendapatkan data pada saat yang diinginkan tanpa ditutupi atau dicegah oleh pihak lain. Berdasarkan masalah yang berkaitan dengan keamanan data pada suatu sistem, tinjauan keamanan menurut Whitman dan Mattord (2011) dibagi menjadi 5, yaitu:

1. *Physical Security*, memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

2. *Personal Security*, overlap dengan ‘phisycal security’ dalam melindungi orang-orang dalam organisasi.
3. *Operation Security*, memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan agar dapat bekerja tanpa gangguan.
4. *Communications Security*, bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
5. *Network Security*, fokus pada pengamanan peralatan jaringan data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

2.1.12 Modifikasi Caesar Cipher

Ada beberapa metode untuk meningkatkan keamanan metode Caesar cipher yang telah dikemukakan oleh peneliti sebelumnya. Namun dari semua metode yang telah dimodifikasi sebelumnya, mengakibatkan ciphertext tidak terbaca.

Begitu juga dengan modifikasi yang telah dilakukan sebelumnya oleh ilmuwan Arab, Abu Alkindi dalam bukunya *A Manuscript on Deciphering Cryptographic Messages* terbitan abad ke-9 sebagai berikut:

- *Mixed monoalfabetic*, Dalam metode ini setiap kunci diganti dengan beberapa kunci acak dalam range tersebut. dari 26 huruf dalam alfabet. Algoritma ini menggantikan huruf yang digunakan untuk mengirim pesan dengan huruf lain ke korespondensi satu satu.

Aturan:

Jika *plaintext* : ABCDE FGHIJ KLMNO PQRST UVWXYZ

Maka *ciphertext*: KLMNO UVWXY JIHGF CDEAB ZPQRST

Kelemahan dari hasil modifikasi ini adalah masih adanya proses pertukaran monoalfabetic yang masih memungkinkan kriptoanalis untuk dapat mengatasinya.

- *Easier Monoalfabetic*, pada kata kunci Easier ini hanya menggunakan satu kata atau sekumpulan kata, kemudian dihilangkan / dihapus huruf yang sama pada kata kunci tersebut kemudian diteruskan ke huruf berikutnya dengan huruf terakhir pada kata kunci tersebut dan seterusnya secara berurutan pada 26 huruf tersebut.

  Contoh:

  Diberikan Kunci: SAMPAI AKHIR NANTI

  Aturan (+kunci)

  Plaintext: ABCDE FGHIJ KLMNO PQRST UVWXYZ

  Ciphertext: SAMPI KHRNT BCDEF GJLOQ UVWXYZ

  Kelemahan pada teknik modifikasi ini adalah adanya beberapa karakter yang tidak tergantikan. Umumnya karakter yang tidak diganti merupakan karakter yang jarang digunakan dalam penggunaan bahasa Indonesia (x, q, v, z).

- G*eneral monoalfabetic*, spesifikasi umum enkripsi ditentukan oleh perulangan posisi kolom sesuai dengan jumlah huruf yang berbeda dalam kata kunci. Teknik modifikasi Monoalfabetic umum

sebenarnya merupakan pengembangan dan pengurangan kelemahan dari modifikasi sebelumnya. *Easier Monoalfabetic* dimana terdapat beberapa karakter yang tidak dapat diganti dan karakter umum, tidak tersubstitusi dalam urutan alfabet paling belakang. Untuk menghindari hal tersebut, beban umum monoalfabetic berupa tabel yang juga diberi perlakuan yang sama dengan tuts pada *Easier Monoalfabetic*.

Contoh:

Diberikan kunci: LOOK FOR MISTAKE

Jadi, Kuncinya: LOKFRMISTAE

Buat kolom:

- LOKFR
- MISTA
- EBCDG
- HJNPQ
- UVWXY
- Z

Kemudian kolom dibaca dari atas ke bawah lalu bergeser dari kiri ke kanan, sehingga menjadi:

Planitext: ABCDE FGHIJ KLMNO PQRST UVWXYZ

Ciphertext: LMEHU ZOIBJ VKSCN WFTDP XRAGQY

Dengan melihat ketiga tipe enkripsi monoalfabetik di atas, akan didapatkan kesimpulan sebagai berikut:

1. Masih terdapat hasil cipher yang memiliki huruf yang sama, maka hal ini dapat dijadikan celah ketika isi informasi bocor.
2. Ketika melakukan dekripsi maka proses pembuatan aturan tidak berpengaruh dengan hasil dekripsi.
3. Untuk melakukan dekripsi maka hanya memerlukan pengetahuan tentang perubahan/penggantian huruf saja dari *plaintext > ciphertext*

2.1.13 *Readable Ciphertext*

Readable Ciphertext adalah algoritma baru yang dibuat dalam memodifikasi *Caesar cipher* dengan menggunakan metode substitusi. Hasil dari penggunaan slgoritma ini adalah enkripsi yang berupa kata tidak acak atau kata yang masih tetap memiliki makna dalam Bahasa Indonesia. Kata "*readable*" dibuat karena hasil yang diperoleh dari proses enkripsi berupa kata yang dapat dibaca atau memiliki makna sebagaimana telah dijelaskan sebelumnya. Algoritma dari metode ini dibuat dengan beberapa ketentuan yang diperoleh dari menghitung jumlah frekuensi alfabet dalam teks Bahasa Indonesia serta kajian beberapa penelitian sebelumnya.

2.2 Kajian Kriptografi dalam Perspektif Islam

Al-Quran menjelaskan bahwasanya Allah SWT memerintahkan hambanya untuk menyampaikan amanat atau pesan hanya kepada hambaNya yang berhak dan menetapkan hukum dengan adil, sebagaimana terdapat dalam surat an-Nisa ayat 58 yang berbunyi:

بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا ۞ اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ
٥٨ ـبِالْعَدْلِ ۗاِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖ ۗاِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

Artinya: *"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum diantara manusia, supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberikan pengajaran yang sebaik-baiknya. Sesungguhnya Allah maha mendengar lagi maha melihat"*

(Sesungguhnya Allah menyuruh kamu untuk menyampaikan amanat) artinya kewajiban-kewajiban yang dipercayakan dari seseorang (kepada yang berhak menerimanya) ayat ini turun ketika Sayyidina Ali RA hendak mengambil kunci Ka'bah secara paksa dari Usman bin Thalhah al-Hajabi sang penjaganya, yakni ketika Nabi SAW datang ke Mekah pada tahun pembebasan. Usman ketika itu tidak mau memberikannya lalu katanya, Seandainya saya tahu bahwa ia Rasulullah tentulah saya tidak akan menghalanginya." Maka Rasulullah Saw pun menyuruh mengembalikan kunci itu padanya seraya bersabda, "Terimalah ini untuk selama- lamanya tiada putus-putusnya!" Usman merasa heran atas hal itu lalu dibacakannya ayat tersebut sehingga Usman pun masuk Islam. Ketika akan meninggal kunci itu diserahkan kepada saudaranya Syaibah lalu tinggal pada anaknya. Ayat ini walaupun datang dengan sebab khusus, tetapi berlaku secara umum disebabkan persamaan di antaranya (dan apabila kamu mengadili di antara manusia) maka Allah memerintahkanmu (agar menetapkan hukum dengan adil Sesungguhnya Allah amat baik sekali) pada ni'immaa diidghamkan mim kepada ma, yaitu nakirah maushufah artinya ni`ma syaian atau sesuatu yang amat baik (nasihat yang diberikan-Nya kepadamu) yaitu menyampaikan amanat dan menjatuhkan putusan secara adil. (Sesungguhnya Allah Maha Mendengar) akan semua perkataan (lagi Maha Melihat) segala perbuatan (Asy-Syuyuthi, 2008).

Dalam tafsir Ibnu Katsir Allah SWT memerintahkan agar amanat-amanat itu disampaikan hanya kepada yang berhak menerimanya. Dari Abu Hurairah Rasulullah SAW bersabda: "*sampaikanlah amanat itu kepada orang yang mempercayaimu, dan janganlah kamu berkhianat terhadap orang yang berkhianat kepadamu*". Makna hadits ini mencakup semua jenis amanat yang diharuskan bagi manusia menyampaikannya. ar-Rabi' bin Anas juga berkata bahwasanya "*Diantara amanat yang dituntut adalah amanat-amanat yang menyangkut antara kamu dan orang lain*" dan Ibnu 'Abbas berkata, "*Amanah di sini umum mencakup orang yang berbakti maupun yang durhaka. Maksudnya, amanat harus dikembalikan kepada pemiliknya, meski pemiliknya itu orang durhaka*". (Ibnu Katsir, 2017:335)

2.3 Kajian Topik Dengan Teori Pendukung

Teori yang digunakan pada penelitian ini sebagian besar adalah teori kriptografi yang mana dalam prosesnya juga menggunakan teori keterbagian, aritmatika modulo dan kongruensi karena pada penelitian ini jenis kriptografi yang digunakan adalah kriptografi klasik yang pada prosesnya menggunakan teknik substitusi.

Pada tahapan awal penelitian ini akan dihitung jumlah frekuensi alfabet dalam teks Bahasa Indonesia yang kemudian dengan hasil ini akan dibuat algoritma proses enkripsi dan dekripsi dengan modifikasi menggunakan *readable ciphertext*. Dari algoritma yang sudah dibuat maka akan dilakukan beberapa kali percobaan untuk menguji hasil dari algoritma tersebut.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian Modifikasi Caesar Cipher menggunakan Readable Ciphertext menggunakan metode studi pustaka, yakni penelitian yang dilakukan dengan cara mengumpulkan data dan informasi dengan bantuan berbagai macam referensi meliputi buku, catatan dan hasil penelitian lain, dokumen, serta artikel yang berkaitan dengan objek permasalahan. Kemudian berbagai data dan informasi tersebut digunakan sebagai bahan untuk menggabungkan beberapa metode atau cara sehingga dapat terbentuk hasil penelitian yang dapat menjawab rumusan masalah yang telah dibuat.

3.2 Pra Penelitian

Pada tahap pra penelitian ini dipersiapkan segala macam hal yang diperlukan sebelum peneliti melakukan kegiatan penelitian. Serta beberapa tahapan yang perlu diperhatikan seperti rancangan penelitian, hal-hal yang perlu diteliti serta pengumpulan data yang didaptakan dari beberapa literatur atau hasil penelitian sebelumnya.

Dalam tahapan ini yang pertama dilakukan ada merumuskan masalah. Rumusan masalah yang dibuat adalah berdasarkan pada proses kejadian yang ditemukan di lapangan serta proses telaah literatur yang sudah dilakukan oleh peneliti sebelumnya. Setelah didapatkan rumusan masalah, maka dilakukan penentuan judul yang sesuai sehingga kemudian judul tersebut akan menjadi gambaran utama dalam proses penelitian berlangsung. Selanjutnya judul ini

diajukan untuk disetujui dan kemudian dilanjutkan pada tahapan penelitian berikutnya. Setelah judul dibuat dan disetujui serta telah terbentuk rumusan masalah, maka dilakukan pembatasan masalah yang akan diteliti agar hasil dari penelitian sesuai dengan rancangan yang telah dibuat. Kemudian tahapan berikutnya adalah pengumpulan data atau informasi yang didapatkan melalui proses studi literatur terhadap beberapa penelitian atau sumber pustaka yang lain. Selanjutnya data atau informasi ini menjadi bahan proses pengolahan untuk menjawab rumusan masalah yang telah ditentukan.

3.3 Tahapan Penelitian

Hal pertama yang dilakukan pada penelitian ini adalah mengetahui frekuensi kemunculan alfabet dalam Bahasa Indonesia yang didapatkan pada literartur. Selanjutnya dengan hasil perhitungan tersebut dibuat sandi monoalfabetik yang kemudian menjadi algoritma modifikasi *Caesar Cipher* menggunakan *Readable Ciphertext*. Algoritma yang dibuat adalah untuk proses enkripsi dan dekripsi.

3.3.1 Modifikasi *Caesar Cipher* untuk Menghasilkan Readable Ciphertext

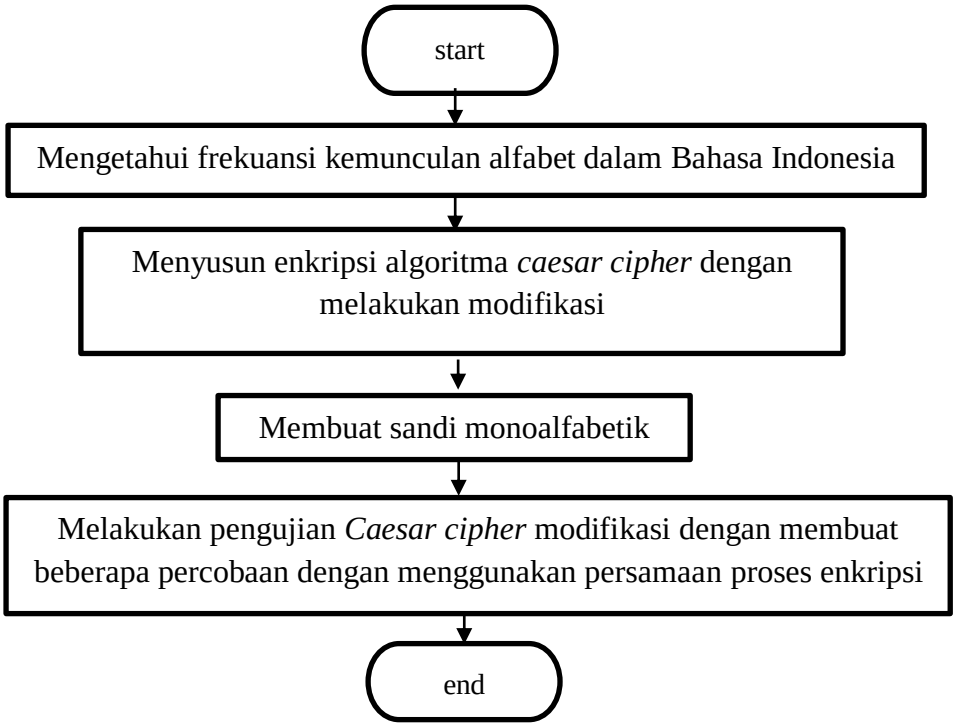
Pada penelitian ini langkah – langkah yang digunakan dalam proses enkripsi dan dekripsi modifikasi Caesar Cipher untuk menghasilkan Readable Ciphertext adalah:

1. Mengetahui frekuensi kemunculan alfabet dalam teks Bahasa Indonesia
2. Menyusun enkripsi algoritma *caesar cipher* dengan melakukan proses modifikasi.
   a. Membuat sandi monoalfabetik dengan ketentuan:
      1. Untuk alfabet vokal, (A, I, U, E, O) diganti alfabet vokal juga.

2. Untuk alfabet konsonan, (BCDFGHJKLMNPQRSTVWXYZ) juga menggantikan alfabet konsonan. Dari alfabet yang ada, ada beberapa sebagai berikut:
3. alfabet QVXYZ tidak tersubstitusi karena penggunaan alfabet dalam bahasa Indonesia sudah jarang digunakan dan untuk menghindari terbentuknya hasil enkripsi yang kurang lazim dalam hal penggunaan bahasa Indonesia.
4. Alfabet N dan G tidak mengalami pergantian, dimaksudkan dengan penggunaan alfabet terutama dalam penggunaan bahasa Indonesia, alfabet tersebut selalu berpasangan.

b. Melakukan pengujian *Caesar cipher* modifikasi dengan membuat beberapa percobaan dengan menggunakan persamaan proses enkripsi:

$$C_{vc} = \{(p_v + b_{k\times1}) + (p_c + b_{k\times1})\} mod 70 + \{(p_v + b_{k\times2}) + (p_c + b_{k\times2})\} mod 70 + (p_v + b_{k\times n}) + (p_c + b_{k\times n})\} \ mod\ 70)\}$$



Gambar 3.1 Diagram Alir Proses Enkripsi

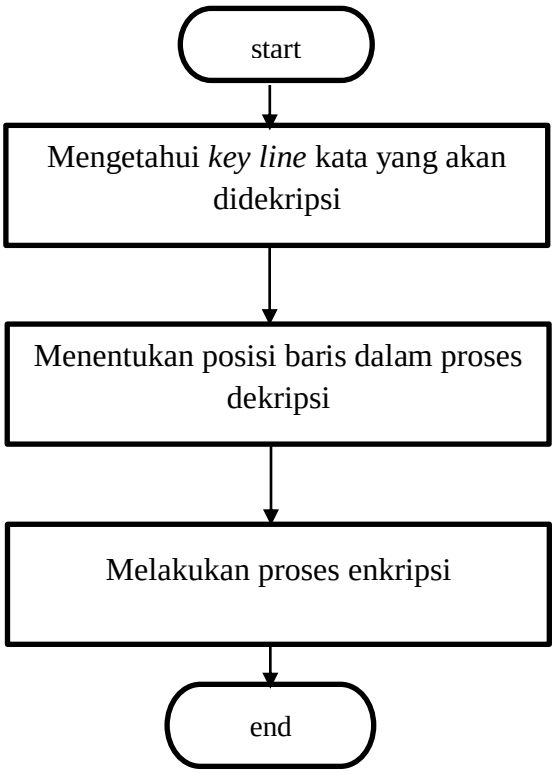
3. Menyusun dekripsi algoritma *caesar cipher* dengan melakukan proses modifikasi

   a. Mengetahui *key line* kata yang akan didekripsi.

   b. Menentukan posisi baris dalam proses dekripsi dengan cara 70 dikurangi baris kata dalam proses enkripsi.

   c. Melakukan proses enkripsi dengan menggunakan persamaan:

$$C_{vc} = \{(p_v + b_{k\times1}) + (p_c + b_{k\times1})\}mod70 + \{(p_v + b_{k\times2}) + (p_c + b_{k\times2})\}mod70 + (p_v + b_{k\times n}) + (p_c + b_{k\times n})\} \ mod\ 70)\}$$



Gambar 3.2 Diagram Alir Proses Dekripsi

BAB IV

HASIL DAN PEMBAHASAN

4.1 Proses Enkripsi Algoritma *Caesar Cipher* Modifikasi untuk Menghasilkan *Readable Ciphertext*

4.1.1 Frekuensi Alfabet Pada Teks Bahasa Indonesia

Sebagaimana dijelaskan pada Bab II terkait ancaman penyerangan atau pemecahan terhadap sandi Caesar cipher, maka hal penting yang harus kita ketahui adalah jumlah frekuensi alfabet dalam Bahasa Indonesia karena pada penelitian ini peneliti membatasi pesan yang akan dienkripsi menggunakan modifikasi Caesar cipher adalah pesan dalam Bahasa Indonesia.

Berdasarkan telaah dari sumber yang didapatkan pada buku "Kriptografi Keamanan Data dan Jaringan" yang ditulis oleh Dony Ariyus pada tahun 2006, didapatkan hasil dalam teks Bahasa Indonesia, penggunaan alfabet sangat berbeda dengan penggunaan alfabet dalam bahasa Inggris. Di mana dalam abjad Bahasa Inggris frekuensi kemunculan tertinggi adalah huruf E. Sedangkan dalam Bahasa Indonesia frekuensi kemunculan tertinggi alfabet adalah huruf A. Untuk memperoleh persamaan proses enkripsi menggunkan modifikasi *Caesar cipher* dengan *readable ciphertext* maka perlu diketahui frekuensi alfabet yang muncul dalam teks Bahasa Indonesia karena hasil ini akan mempengaruhi pembuatan persamaan atau algoritma yang dibuat yang mana hal ini didasarkan pada jumlah masing-masing frekuensi huruf. Huruf apa saja yang paling banyak muncul sampai huruf apa saja yang jarang muncul atau jarang digunakan dalam kalimat Bahasa Indonesia. Karena alasan hasil perhitungan yang berbeda antara teks

Bahasa Indonesia dan Bahasa Inggris inilah juga yang menjadi alasan pembatasan penelitian ini hanya dikhususkan pada pesan berbahasa Indonesia.

Dari hasil yang didapatkan pada beberapa sumber mengenai frekuensi kemunculan alfabet dalam Bahasa Indonesia, maka huruf yang sering muncul yakni huruf A, N, I, E, K, T, R, D, S, M, sedangkan huruf yang jarang muncul atau penggunaannya jarang dalam Bahasa Indonesia yaitu huruf Q, V, X, Y, Z serta huruf yang penggunaannya cenderung berpasangan adalah huruf N dan G. Melihat hasil tersebut penulis mencoba untuk memodifikasi metode *Caesar Cipher* sehingga menghasilkan *ciphertext* yang dapat dibaca dan memiliki makna dalam Bahasa Indonesia. Sehingga dengan ciphertext yang dapat dibaca dan memiliki ini akan meminimalisir kemungkinan kecurigaan kriptanalis terhadap pesan tersebut sehingga akan memperkecil upaya untuk percobaan penyerangan atau pemecahan terhadap pesan yang telah dibuat.

4.1.2 Membuat Sandi Monoalfabetik

Pada modifikasi *Caesar Cipher*, penulis membandingkan beberapa metode modifikasi yang telah dijelaskan sebelumnya modifikasi ini juga didasarkan pada perhitungan frekuensi alfabet dalam teks Bahasa Indonesia yang telah didapatkan sebelumnya. Dari ketiga metode yang telah dijelaskan sebelumnya, penulis mencoba memodifikasi Caesar cipher agar dapat terbaca, yaitu Sandi *Monoalfabetic Readable* dengan syarat atau aturan sebagai berikut:

- Untuk alfabet vocal (A, I, U, E, O) disubstitusi dengan alfabet vokal juga.
- Untuk alfabet konsonan, (BCDFGHJKLMNPQRSTVWXYZ) juga disubstitusi dengan alfabet konsonan. Dari alfabet yang ada, ada beberapa temuan dan ketentuan sebagai berikut:

- Alfabet QVXYZ tidak tersubstitusi karena penggunaan alfabet dalam bahasa Indonesia sudah jarang digunakan dan untuk menghindari terbentuknya hasil enkripsi yang kurang lazim dalam penggunaan bahasa Indonesia.
- Alfabet N dan G tidak mengalami pergantian, karena dalam penggunaannya terutama dalam penggunaan bahasa Indonesia, alfabet tersebut selalu berpasangan.

Berdasarkan uraian di atas maka dapat dikemukakan bahwa pada proses pembacaan sandi *Monoalphabetic Cipher* metode enkripsi hanya melakukan substitusi pada dua jenis alfabet yang sama yaitu vokal dan konsonan dengan alfabet vokal sebanyak 5 dan alfabet konsonan sebanyak 14. Sedangkan sebanyak 7 alfabet tidak mengalami pergantian huruf konsonan.

Pernyataan ini dapat dinotasikan dalam bentuk persamaan sebagai berikut:

Untuk vokal : $C_v = f(p_v + p)\ mod\ 5$, (4)

Konsonan: $C_c = g(p_c + p)\ mod\ 14$ (5)

Ketentuan diatas merupakan hasil modifikasi baru dari Caesar cipher yang diberi nama Readable Ciphertext dan dapat dilihat pada tabel berikut ini :

Tabel 4.1 Substitusi Huruf Vokal Pada Caesar Cipher Modifikasi

		0	1	2	3	4
Plaintext	0	A	O	E	I	U
Ciphertext	1	O	E	I	U	A

Tabel 4.2 Substitusi Huruf Konsonan Pada Caesar Cipher Modifikasi

		0	1	2	3	4	5	6	7	8	9	10	11	12	13
Plaintext	0	B	D	J	M	P	R	L	S	C	F	H	K	T	W
Ciphertext	1	D	J	M	P	R	L	S	C	F	H	K	T	W	B

Dari tabel 4.2 di atas dapat dilihat bahwa setiap huruf vokal disubstitusikan dengan vokal (A = O, E = I, I = U, O = E, U = A), sedangkan huruf konsonan disubstitusikan dengan huruf konsonan kecuali ada tujuh huruf yang tidak disubstitusikan yakni huruf Q, V, X, Y, Z karena jarang digunakan dalam Bahasa Indonesia dan huruf N dan G karena dua huruf ini dalam penggunaannya sering berpasangan.

Dari persamaan sebelumnya

$C_v = f(p_v + p)\ mod\ 5$, (4) dan

$C_c = g(p_c + p)\ mod\ 14$ (5)

Setelah didapatkan persamaan di atas, maka dilakukan proses substitusi

Catatan:

C_v = Ciphertext vocal

C_c = Ciphertext konsonan

p_v= plaintext vokal

bk= key line (baris kunci)

p_c= plaintext konsonan

Berdasarkan persamaan di atas diketahui bahwa proses substitusi dalam alfabet terjadi sebanyak 70 kali dengan rincian sebagai berikut:

- Proses substitusi huruf vokal = 5 x 14 = 70

- Proses substitusi huruf konsonan = 14 x 5 = 70 substitusi
- Karena konstanta konsonan tidak mengalami substitusi, maka mengikuti bilangan yang ada atau proses substitusi dapat dinyatakan 70 x 1 = 70 substitusi.

Berdasarkan uraian di atas, proses substitusi *readable ciphertext* secara keseluruhan dapat dilihat pada tabel 1 di halaman lampiran.

Pada proses substitusi, setiap huruf mengalami substitusi atau pergantian sebanyak 70 kali sesuai dengan algoritma atau persamaan yang telah dibuat. Proses tersebut menghasilkan jumlah atau frekuensi masing-masing huruf muncul. Jumlah frekuensi pada setiap alfabet dapat dilihat pada tabel berikut:

Tabel 4.3 Jumlah Substitusi Pada Setiap Alfabet

A	B	C	D	E	F	G	H	I	J	K	L	M
14	5	5	5	14	5	70	5	14	5	5	5	5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
70	14	5	70	5	5	5	14	70	5	70	70	70

4.1.3 Melakukan Pengujian *Caesar Cipher* Modifikasi

Setelah proses modifikasi pada Readable Ciphertext ini, maka langkah selanjutnya adalah pengujian modifikasi. Pengujian dilakukan dengan membuat plaintext menggunakan kalimat “ADA MUSUH”. Maka hasil enkripsi atau substitusi pertama pada metode ini dapat dilihat pada tabel berikut ini.

Tabel 4.4 Hasil Pengujian Ada Musuh Caesar Cipher Modifikasi

A	D	A		M	U	S	U	H
O	J	O		P	A	C	A	K

Dari tabel di atas dapat dilihat bahwa hasil enkripsi “ADA MUSUH” adalah “OJO PACAK”, maka terbukti bahwa hasil ciphertext dari *Raedable Monoalfabetic* ini adalah ciphertext yang dapat dibaca. Walaupun hasil ciphertext ini dapat dibaca, namun belum menghasilkan kalimat atau pesan yang mengandung makna atau arti istilah dalam kamus Bahasa Indonesia, jadi pesan tersebut masih dapat menimbulkan kecurigaan bagi pihak yang membacanya sehingga menimbulkan kemungkinan untuk dipecahkan.

Agar dapat menghasilkan ciphertext yang dapat dibaca dan memiliki arti atau makna istilah serta dapat diimplikasikan, maka kita harus melihat semua hasil proses enkripsi sebanyak 70 kali dari proses substitusi. Dalam keseluruhan proses inilah kita dapat menentukan dan mengambil hasil dari proses enkripsi atau urutan dari proses enkripsi yang akan kita ambil sehingga pada akhirnya akan ditemukan dan dipilih hasil dari proses substitusi berupa kata yang juga dapat dibaca dan memiliki makna dalam Bahasa Indonesia.

Berdasarkan pembahasan plaintext tersebut, dapat diperoleh hasil enkripsi yang dapat dilihat pada tabel 2 di halaman lampiran.

Berdasarkan tabel 2 tersebut terlihat ada beberapa kata atau istilah yang mengisyaratkan adanya kata “ADA” menjadi kata “ISI” pada baris ke-48 dan kata “MUSUH” menjadi kata “PUCUK” pada baris ke-15. Untuk lebih jelasnya dapat dilihat pada tabel 3 di halaman lampiran.

Dari tabel 3 tersebut, ciphertext yang dipilih adalah yang memiliki makna atau arti dalam Bahasa Indonesia dari 70 substitusi yang telah dilakukan, yakni kata “ISI” pada baris ke-48 dan kata “PUCUK” pada baris ke-15. Dikarenakan metode *readable ciphertext* ini tidak memiliki key atau kunci, sehingga kita dapat menyatakan bahwa urutan baris yang terbaca dapat digunakan sebagai kunci dan selanjutnya kita sebut sebagai *key line*.

Persamaan proses enkripsi tersebut dapat dinyatakan dalam bentuk persamaan berikut:

$$C_{vc} = \{(p_v + b_{k\times1}) + (p_c + b_{k\times1})\} mod 70 + \{(p_v + b_{k\times2}) + (p_c + b_{k\times2})\} mod 70 + (p_v + b_{k\times n}) + (p_c + b_{k\times n})\} \ mod\ 70)\} \quad (8)$$

Lalu pada kasus enkripsi teks “ADA MUSUH” maka persamaannya sebagai berikut:

$$C_{vc} = \{(p_v + 48) + (p_c + 48)\}\, mod\ 70 + \{(p_v + 15) + (p_c + 15)\}\, mod\ 70\} \quad (9)$$

4.2 Menyusun Dekripsi Algoritma *Caesar Cipher* Modifikasi untuk Menghasilkan *Readable Ciphertext.*

Proses dekripsi sama halnya dengan proses enkripsi. Namun pada hasil enkripsi yang kita gunakan adalah baris tertentu. Maka saat melakukan proses dekripsi, kita harus mengetahui baris kunci (*key line*) dari kata yang dienkripsikan. Adapun algoritma dekripsi *Caesar cipher* yang dimodifikasi menggunakan *readable ciphertext* sebagai berikut:

a. Mengetahui *key line* kata yang akan didekripsi.

   contoh:

   Pada contoh dekripsi “ADA MUSUH” menghasilkan ciphertext “ISI PUCUK”, dimana kata “ISI” berada pada baris ke-48 dan kata “PUCUK” pada

baris ke-15. Urutan ini didasarkan pada proses substitusi sebanyak 70 kali yang telah dilakukan berdasarkan pada algoritma atau ketentuan yang telah dibuat sebelumnya.

b. Menentukan posisi baris dalam proses dekripsi dengan cara 70 dikurangi nilai *key line* pada proses enkripsi

Dalam melakukan proses enkripsi, dilakukan substitusi sebanyak 70 kali. Sehingga dalam proses enkripsi dapat dinyatakan bahwa kata "ISI" berada pada baris ke-48 dan karena hasil inilah sehingga pada proses dekripsi kata "ISI" berada pada posisi baris ke-22 (didapatkan dari 70 – 48 = 22) serta kata "PUCUK" di baris ke-15 sehingga pada proses dekripsi kata "PUCUK" berada pada posisi ke-55 (didapatkan dari 70 – 15 = 55).

Proses dekripsi dapat ditulis dalam bentuk persamaan sebagai berikut:

$$P_{vc} = \{(C_v - b_{k\times1}) + (C_c - b_{k\times1})\} \, mod \, 70 + \{(C_v - b_{k\times2}) + (C_c - b_{k\times2})\} \, mod \, 70 + \{(C_v - b_{k\times n}) + (C_c - b_{k\times2})\} \; mod \, 70)\} \quad (10)$$

Sehingga pada kasus dekripsi "ADA MUSUH" maka persamaannya sebagai berikut:

$$P_{vc} = \{(C_v - 48) + (C_c - 48)\} \, mod \, 70 + \{(C_v - 15) + (C_c - 15)\} \, mod \, 70\} \quad (11)$$

Berdasarkan persamaan di atas, hasil dekripsi "ADA MUSUH" tersebut dapat dilihat pada tabel 4 di halaman lampiran.

4.3 Hasil pengujian lain

Untuk membuktikan keberhasilan persamaan yang dibuat pada proses modifikasi *Caesar cipher* menggunakan *readable ciphertext*, maka dilakukan beberapa percobaan dengan menggunakan contoh yang terdiri dari dua dan tiga kata. Beberapa percobaan yang dilakukan adalah sebanyak 40 kali dan

menghasilkan hasil enkripsi yang juga berupa kata yang dapat dibaca dan memiliki makna dalam Bahasa Indonesia. Pada percobaan juga dilakukan proses dekripsi dari masing – masing kata yang telah ditentukan.

Berikut beberapa contoh hasil pengujian lain yang telah dilakukan:

Tabel 4.5 Hasil Pengujian Lain

No	Plaintext	Ciphertext	Keys	Dekripsi
1	JALAN RUSAK	LAHAN RESIK	60, 28	10, 42
2	CEPAT LARI	SEMAK RAPI	55, 55	15, 15
3	AMAN SUDAH	IPIN SEDIH	43, 28	27, 42
4	AWAS BOM	UKUR POS	54, 60	16, 10
5	JALAN BUNTU	SUKUN MUNDU	19, 45	51. 25
6	LARI JAM DUA	MEJA LAS TUA	67, 60, 25	3, 10, 45
7	MAJU TERUS	JUDI HUMOR	69, 14	1, 56
8	LIMA DUA	JIWA TUA	10,25	60, 45
9	JANGAN LARI	TANGAN WATI	10, 35	60, 35
10	MUSUH DATANG	PUCUK CARANG	15, 35	55, 35
11	MAJU DUA KALI	JUDI TUA MATI	69, 27, 22	1, 43, 48
12	JALAN MUNDUR	LAHAN MANDAR	60, 56	10, 14
13	JALAN MAJU	LAHAN JUDI	60, 69	10, 1
14	RUANG LAWAN	TUANG PAKAN	35, 40	35, 30
15	LAWAN LARI	MOHON RAPI	11, 55	59, 15
16	MUSUH TIBA	PUCUK TEBU	15, 14	55, 56
17	KIJANG SATU	TAMENG BARU	57, 35	13, 35
18	SERANG MUSUH	SARING PUCUK	28, 17	42, 53
19	KAKI TANGAN	PAPI DINGIN	35, 3	35, 67
20	BATAS AMAN	POJOK AWAN	46, 10	24, 60

21	SERANG MUSUH KITA	SARING PUCUK PARE	28, 15, 7	42, 55, 63
22	TANAM BOM	RANAH PAS	35, 4	35, 66
23	JALAN CEPAT - CEPAT	LAHAN SEMAK - SEMAK	60, 55	10, 15
24	MATA-MATA MUSUH	RABA-RABA PUCUK	30, 15	40, 55
25	JALAN SEPI	LAHAN CERI	60, 15	10, 55
26	POS AMAN	BOM AWAN	10, 10	60, 60
27	JAGA BATAS KOTA	LOGO POJOK JAMU	46, 46, 19	24, 24, 51
28	MUSUH MENANG	PUCUK BENANG	15, 25	55, 45
29	SERANG KOTA	SARING JAMU	28, 19	42, 51
30	MISI GAGAL	SUKU GAGAH	46, 60	24, 10

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Proses enkripsi *caesar cipher* dengan modifikasi untuk menghasilkan *readable ciphertext* dilakukan dengan cara substitusi, yakni mengganti alfabet vokal dengan alfabet vokal dengan persamaan: $C_v = (p_v + bk)\ mod\ 5$,

   alfabet konsonan dengan alfabet konsonan dengan persamaan:

   $C_c = (p_c + bk)\ mod\ 14$ dan untuk simbol tetap disubstitusi dengan simbol yang sama. Dengan ketentuan huruf QVXYZ tidak disubstitusi karena penggunaannya jarang dalam bahasa Indonesia dan alfabet N dan G juga tidak disubstitusi karena dalam Bahasa Indonesia, penggunaannya cenderung selalu berpasangan. Dari persamaan substitusi huruf vokal dan konsonan tersebut maka didapatkan substitusi sebanyak 70 kali untuk mendapatkan enkripsi kata yang nantinya kata yang dihasilkan adalah kata yang dapat dibaca dan memiliki makna dalam Bahasa Indonesia.
2. Proses dekripsi *caesar cipher* dengan modifikasi untuk menghasilkan *readable ciphertext* dilakukan dengan cara mengetahui *key line* atau baris kunci kata yang akan didekripsikan untuk selanjutnya dapat diketahui posisi baris dalam proses dekripsi dengan cara 70 dikurangi baris kata dalam proses enkripsi sehingga didapatkan persamaan: $P_{vc} = \{(C_v - b_{k\times 1}) +$

$(C_c - b_{k\times1})\} \, mod \, 70 + \{(C_v - b_{k\times2}) + (C_c - b_{k\times2})\} \, mod \, 70 + \{(C_v - b_{k\times n}) + (C_c - b_{k\times2})\} \; mod \, 70)\}$.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran untuk penelitian berikutnya:

1. Menggunakan algoritma yang lain tetapi enkripsi yang dilakukan tetap menghasilkan *ciphertext* yang dapat dibaca dan memiliki makna dalam Bahasa Indonesia.
2. Menggunakan algoritma program untuk mempermudah proses substitusi dan mendapatkan hasil yang lebih akurat.

DAFTAR PUSTAKA

Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Penerbit Graha Ilmu.

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis dan implementasi*. Yogyakarta: C.V Andi Offset.

Atul Kahate, 2008, *Cryptography and Network Security, Tata McGraw Hill Education Private Limited*, New Delhi.

Fattah, A.S. 2017. *Mudah Tafsir Ibnu Katsir Jilid 2*. Jakarta: Maghfirah Pustaka.

F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "*Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard,* Inform. Mulawarman J. Ilm. Ilmu Komput., vol. 10, no. 1, p. 20, 2016.

Gunawan, Indra, 2021. *Keamanan Data: Teori dan Implementasi*. Sukabumi: CV. Jejak.

Irawan, W. H., dkk. *Pengantar Teori Bilangan*. Malang: UIN-MALIKI PRESS.

Jamaluddin. Romindo. 2020. *Kriptografi: Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vignere Cipher dan RSA*. Yayasan Kita Menulis.

Ravindra, B. Kallam, *A Survey on Cryptography and Steganography Methods for Information Security*, International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyarkarta: Penerbit Andi.

Sansani, S. (2008). *Penggunaan Aritmetika Modulo dan Balikan Modulo pada Modifikasi Algoritma Knapsack*. 3-4.

Siahaan, V. 2020. *Three Books in One: SQLite dengan Java*. Jakarta: Balige Publishing. 2020.

Singh, Pooja and Sen, Pintu. *Enhancing Security of Caesar Cipher Using Divide and Conquer Approach,* International Journal of Advance Research in Science and Engineering Volume No. 06 Special Issue, September 2017.

LAMPIRAN

Plaintext	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	1	O	D	F	J	I	H	G	K	U	M	T	S	P	N	E	R	Q	L	C	W	A	V	B	X	Y	Z
	2	E	J	H	M	U	K	G	T	A	P	W	C	R	N	I	L	Q	S	F	B	O	V	D	X	Y	Z
	3	I	M	K	P	A	T	G	W	O	R	B	F	L	N	U	S	Q	C	H	D	E	V	J	X	Y	Z
	4	U	P	T	R	O	W	G	B	E	L	D	H	S	N	A	C	Q	F	K	J	I	V	M	X	Y	Z
	5	A	R	W	L	E	B	G	D	I	S	J	K	C	N	O	F	Q	H	T	M	U	V	P	X	Y	Z
	6	O	L	B	S	I	D	G	J	U	C	M	T	F	N	E	H	Q	K	W	P	A	V	R	X	Y	Z
	7	E	S	D	C	U	J	G	M	A	F	P	W	H	N	I	K	Q	T	B	R	O	V	L	X	Y	Z
	8	I	C	J	F	A	M	G	P	O	H	R	B	K	N	U	T	Q	W	D	L	E	V	S	X	Y	Z
	9	U	F	M	H	O	P	G	R	E	K	L	D	T	N	A	W	Q	B	J	S	I	V	C	X	Y	Z
	10	A	H	P	K	E	R	G	L	I	T	S	J	W	N	O	B	Q	D	M	C	U	V	F	X	Y	Z
	11	O	K	R	T	I	L	G	S	U	W	C	M	B	N	E	D	Q	J	P	F	A	V	H	X	Y	Z
	12	E	T	L	W	U	S	G	C	A	B	F	P	D	N	I	J	Q	M	R	H	O	V	K	X	Y	Z
	13	I	W	S	B	A	C	G	F	O	D	H	R	J	N	U	M	Q	P	L	K	E	V	T	X	Y	Z
	14	U	B	C	D	O	F	G	H	E	J	K	L	M	N	A	P	Q	R	S	T	I	V	W	X	Y	Z
	15	A	D	F	J	E	H	G	K	I	M	T	S	P	N	O	R	Q	L	C	W	U	V	B	X	Y	Z
	16	O	J	H	M	I	K	G	T	U	P	W	C	R	N	E	L	Q	S	F	B	A	V	D	X	Y	Z
	17	E	M	K	P	U	T	G	W	A	R	B	F	L	N	I	S	Q	C	H	D	O	V	J	X	Y	Z
	18	I	P	T	R	A	W	G	B	O	L	D	H	S	N	U	C	Q	F	K	J	E	V	M	X	Y	Z
	19	U	R	W	L	O	B	G	D	E	S	J	K	C	N	A	F	Q	H	T	M	I	V	P	X	Y	Z
	20	A	L	B	S	E	D	G	J	I	C	M	T	F	N	O	H	Q	K	W	P	U	V	R	X	Y	Z
	21	O	S	D	C	I	J	G	M	U	F	P	W	H	N	E	K	Q	T	B	R	A	V	L	X	Y	Z
	22	E	C	J	F	U	M	G	P	A	H	R	B	K	N	I	T	Q	W	D	L	O	V	S	X	Y	Z
	23	I	F	M	H	A	P	G	R	O	K	L	D	T	N	U	W	Q	B	J	S	E	V	C	X	Y	Z
	24	U	H	P	K	O	R	G	L	E	T	S	J	W	N	A	B	Q	D	M	C	I	V	F	X	Y	
	25	A	K	R	T	E	L	G	S	I	W	C	M	B	N	O	D	Q	J	P	F	U	V	H	X	Y	Z
	26	O	T	L	W	I	S	G	C	U	B	F	P	D	N	E	J	Q	M	R	H	A	V	K	X	Y	Z
	27	E	W	S	B	U	C	G	F	A	D	H	R	J	N	I	M	Q	P	L	K	O	V	T	X	Y	Z
	28	I	B	C	D	A	F	G	H	O	J	K	L	M	N	U	P	Q	R	S	T	E	V	W	X	Y	Z
	29	U	D	F	J	O	H	G	K	E	M	T	S	P	N	A	R	Q	L	C	W	I	V	B	X	Y	Z
	30	A	J	H	M	E	K	G	T	I	P	W	C	R	N	O	L	Q	S	F	B	U	V	D	X	Y	Z
	31	O	M	K	P	I	T	G	W	U	R	B	F	L	N	E	S	Q	C	H	D	A	V	J	X	Y	Z
	32	E	P	T	R	U	W	G	B	A	L	D	H	S	N	I	C	Q	F	K	J	O	V	M	X	Y	Z
	33	I	R	W	L	A	B	G	D	O	S	J	K	C	N	U	F	Q	H	T	M	E	V	P	X	Y	Z
	34	U	L	B	S	O	D	G	J	E	C	M	T	F	N	A	H	Q	K	W	P	I	V	R	X	Y	Z
	35	A	S	D	C	E	J	G	M	I	F	P	W	H	N	O	K	Q	T	B	R	U	V	L	X	Y	Z
	36	O	C	J	F	I	M	G	P	U	H	R	B	K	N	E	T	Q	W	D	L	A	V	S	X	Y	Z
	37	E	F	M	H	U	P	G	R	A	K	L	D	T	N	I	W	Q	B	J	S	O	V	C	X	Y	Z
	38	I	H	P	K	A	R	G	L	O	T	S	J	W	N	U	B	Q	D	M	C	E	V	F	X	Y	Z
	39	U	K	R	T	O	L	G	S	E	W	C	M	B	N	A	D	Q	J	P	F	I	V	H	X	Y	Z
	40	A	T	L	W	E	S	G	C	I	B	F	P	D	N	O	J	Q	M	R	H	U	V	K	X	Y	Z
	41	O	W	S	B	I	C	G	F	U	D	H	R	J	N	E	M	Q	P	L	K	A	V	T	X	Y	Z
	42	E	B	C	D	U	F	G	H	A	J	K	L	M	N	I	P	Q	R	S	T	O	V	W	X	Y	Z
	43	I	D	F	J	A	H	G	K	O	M	T	S	P	N	U	R	Q	L	C	W	E	V	B	X	Y	Z
	44	U	J	H	M	O	K	G	T	E	P	W	C	R	N	A	L	Q	S	F	B	I	V	D	X	Y	Z
	45	A	M	K	P	E	T	G	W	I	R	B	F	L	N	O	S	Q	C	H	D	U	V	J	X	Y	Z
	46	O	P	T	R	I	W	G	B	U	L	D	H	S	N	E	C	Q	F	K	J	A	V	M	X	Y	Z
	47	E	R	W	L	U	B	G	D	A	S	J	K	C	N	I	F	Q	H	T	M	O	V	P	X	Y	Z
	48	I	L	B	S	A	D	G	J	O	C	M	T	F	N	U	H	Q	K	W	P	E	V	R	X	Y	Z
	49	U	S	D	C	O	J	G	M	E	F	P	W	H	N	A	K	Q	T	B	R	I	V	L	X	Y	Z
	50	A	C	J	F	E	M	G	P	I	H	R	B	K	N	O	T	Q	W	D	L	U	V	S	X	Y	Z

	51	O	F	M	H	I	P	G	R	U	K	L	D	T	N	E	W	Q	B	J	S	A	V	C	X	Y	Z
	52	E	H	P	K	U	R	G	L	A	T	S	J	W	N	I	B	Q	D	M	C	O	V	F	X	Y	Z
	53	I	K	R	T	A	L	G	S	O	W	C	M	B	N	U	D	Q	J	P	F	E	V	H	X	Y	Z
	54	U	T	L	W	O	S	G	C	E	B	F	P	D	N	A	J	Q	M	R	H	I	V	K	X	Y	Z
	55	A	W	S	B	E	C	G	F	I	D	H	R	J	N	O	M	Q	P	L	K	U	V	T	X	Y	Z
	56	O	B	C	D	I	F	G	H	U	J	K	L	M	N	E	P	Q	R	S	T	A	V	W	X	Y	Z
	57	E	D	F	J	U	H	G	K	A	M	T	S	P	N	I	R	Q	L	C	W	O	V	B	X	Y	Z
	58	I	J	H	M	A	K	G	T	O	P	W	C	R	N	U	L	Q	S	F	B	E	V	D	X	Y	Z
	59	U	M	K	P	O	T	G	W	E	R	B	F	L	N	A	S	Q	C	H	D	I	V	J	X	Y	Z
	60	A	P	T	R	E	W	G	B	I	L	D	H	S	N	O	C	Q	F	K	J	U	V	M	X	Y	Z
	61	O	R	W	L	I	B	G	D	U	S	J	K	C	N	E	F	Q	H	T	M	A	V	P	X	Y	Z
	62	E	L	B	S	U	D	G	J	A	C	M	T	F	N	I	H	Q	K	W	P	O	V	R	X	Y	Z
	63	I	S	D	C	A	J	G	M	O	F	P	W	H	N	U	K	Q	T	B	R	E	V	L	X	Y	Z
	64	U	C	J	F	O	M	G	P	E	H	R	B	K	N	A	T	Q	W	D	L	I	V	S	X	Y	Z
	65	A	F	M	H	E	P	G	R	I	K	L	D	T	N	O	W	Q	B	J	S	U	V	C	X	Y	Z
	66	O	H	P	K	I	R	G	L	U	T	S	J	W	N	E	B	Q	D	M	C	A	V	F	X	Y	Z
	67	E	K	R	T	U	L	G	S	A	W	C	M	B	N	I	D	Q	J	P	F	O	V	H	X	Y	Z
	68	I	T	L	W	A	S	G	C	O	B	F	P	D	N	U	J	Q	M	R	H	E	V	K	X	Y	Z
	69	U	W	S	B	O	C	G	F	E	D	H	R	J	N	A	M	Q	P	L	K	I	V	T	X	Y	Z
	70	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabel 1 Proses Substitusi Readable Ciphertext

0	1	2	3	4	5	6	7	8	9		0	1	2	3	4	5	6	7	8	9
0	A	D	A		M	U	S	U	H		25	A	T	A		B	U	P	U	S
1	O	J	O		P	A	C	A	K		26	O	W	O		D	A	R	A	C
2	E	M	E		R	O	F	O	T		27	E	B	E		J	O	L	O	F
3	I	P	I		L	E	H	E	W		28	I	D	I		M	E	S	E	H
4	U	R	U		S	I	K	I	B		29	U	J	U		P	I	C	I	K
5	A	L	A		C	U	T	U	D		30	A	M	A		R	U	F	U	T
6	O	S	O		F	A	W	A	J		31	O	P	O		L	A	H	A	W
7	E	C	E		H	O	B	O	M		32	E	R	E		S	O	K	O	B
8	I	F	I		K	E	D	E	P		33	I	L	I		C	E	T	E	D
9	U	H	U		T	I	J	I	R		34	U	S	U		F	I	W	I	J
10	A	K	A		W	U	M	U	L		35	A	C	A		H	U	B	U	M
11	O	T	O		B	A	P	A	S		36	O	F	O		K	A	D	A	P
12	E	W	E		D	O	R	O	C		37	E	H	E		T	O	J	O	R
13	I	B	I		J	E	L	E	F		38	I	K	I		W	E	M	E	L
14	U	D	U		M	I	S	I	H		39	U	T	U		B	I	P	I	S
15	A	J	A		P	U	C	U	K		40	A	W	A		D	U	R	U	C
16	O	M	O		R	A	F	A	T		41	O	B	O		J	A	L	A	F
17	E	P	E		L	O	H	O	W		42	E	D	E		M	O	S	O	H
18	I	R	I		S	E	K	E	B		43	I	J	I		P	E	C	E	K
19	U	L	U		C	I	T	I	D		44	U	M	U		R	I	F	I	T
20	A	S	A		F	U	W	U	J		45	A	P	A		L	U	H	U	W
21	O	C	O		H	A	B	A	M		46	O	R	O		S	A	K	A	B
22	E	F	E		K	O	D	O	P		47	E	L	E		C	O	T	O	D
23	I	H	I		T	E	J	E	R		48	I	S	I		F	E	W	E	J
24	U	K	U		W	I	M	I	L											

Tabel 2 Hasil Pengujian Caesar Cipher Modifikasi “Ada Musuh” sebanyak 70 substitusi

0	1	2	3	4	5	6	7	8	9		0	1	2	3	4	5	6	7	8	9
0	A	D	A		M	U	S	U	H		36	O	F	O		K	A	D	A	P
1	O	J	O		P	A	C	A	K		37	E	H	E		T	O	J	O	R
2	E	M	E		R	O	F	O	T		38	I	K	I		W	E	M	E	L
3	I	P	I		L	E	H	E	W		39	U	T	U		B	I	P	I	S
4	U	R	U		S	I	K	I	B		40	A	W	A		D	U	R	U	C
5	A	L	A		C	U	T	U	D		41	O	B	O		J	A	L	A	F
6	O	S	O		F	A	W	A	J		42	E	D	E		M	O	S	O	H
7	E	C	E		H	O	B	O	M		43	I	J	I		P	E	C	E	K
8	I	F	I		K	E	D	E	P		44	U	M	U		R	I	F	I	T
9	U	H	U		T	I	J	I	R		45	A	P	A		L	U	H	U	W
10	A	K	A		W	U	M	U	L		46	O	R	O		S	A	K	A	B
11	O	T	O		B	A	P	A	S		47	E	L	E		C	O	T	O	D
12	E	W	E		D	O	R	O	C		48	I	S	I		F	E	W	E	J
13	I	B	I		J	E	L	E	F		49	U	C	U		H	I	B	I	M
14	U	D	U		M	I	S	I	H		50	A	F	A		K	U	D	U	P
15	A	J	A		P	U	C	U	K		51	O	H	O		T	A	J	A	R
16	O	M	O		R	A	F	A	T		52	E	K	E		W	O	M	O	L
17	E	P	E		L	O	H	O	W		53	I	T	I		B	E	P	E	S
18	I	R	I		S	E	K	E	B		54	U	W	U		D	I	R	I	C
19	U	L	U		C	I	T	I	D		55	A	B	A		J	U	L	U	F
20	A	S	A		F	U	W	U	J		56	O	D	O		M	A	S	A	H
21	O	C	O		H	A	B	A	M		57	E	J	E		P	O	C	O	K
22	E	F	E		K	O	D	O	P		58	I	M	I		R	E	F	E	T
23	I	H	I		T	E	J	E	R		59	U	P	U		L	I	H	I	W
24	U	K	U		W	I	M	I	L		60	A	R	A		S	U	K	U	B
25	A	T	A		B	U	P	U	S		61	O	L	O		C	A	T	A	D
26	O	W	O		D	A	R	A	C		62	E	S	E		F	O	W	O	J
27	E	B	E		J	O	L	O	F		63	I	C	I		H	E	B	E	M
28	I	D	I		M	E	S	E	H		64	U	F	U		K	I	D	I	P
29	U	J	U		P	I	C	I	K		65	A	H	A		T	U	J	U	R
30	A	M	A		R	U	F	U	T		66	O	K	O		W	A	M	A	L
31	O	P	O		L	A	H	A	W		67	E	T	E		B	O	P	O	S
32	E	R	E		S	O	K	O	B		68	I	W	I		D	E	R	E	C
33	I	L	I		C	E	T	E	D		69	U	B	U		J	I	L	I	F
34	U	S	U		F	I	W	I	J		70	A	D	A		M	U	S	U	H
35	A	C	A		H	U	B	U	M											

Tabel 3 Ciphertext yang Dipilih

0	1	2	3	4	5	6	7	8	9		0	1	2	3	4	5	6	7	8	9

0	I	S	I		P	U	C	U	K		36	U	D	U		T	A	J	A	R
1	U	C	U		R	A	F	A	T		37	A	J	A		W	O	M	O	L
2	A	F	A		L	O	H	O	W		38	O	M	O		B	E	P	E	S
3	O	H	O		S	E	K	E	B		39	E	P	E		D	I	R	I	C
4	E	K	E		C	I	T	I	D		40	I	R	I		J	U	L	U	F
5	I	T	I		F	U	W	U	J		41	U	L	U		M	A	S	A	H
6	U	W	U		H	A	B	A	M		42	A	S	A		P	O	C	O	K
7	A	B	A		K	O	D	O	P		43	O	C	O		R	E	F	E	T
8	O	D	O		T	E	J	E	R		44	E	F	E		L	I	H	I	W
9	E	J	E		W	I	M	I	L		45	I	H	I		S	U	K	U	B
10	I	M	I		B	U	P	U	S		46	U	K	U		C	A	T	A	D
11	U	P	U		D	A	R	A	C		47	A	T	A		F	O	W	O	J
12	A	R	A		J	O	L	O	F		48	O	W	O		H	E	B	E	M
13	O	L	O		M	E	S	E	H		49	E	B	E		K	I	D	I	P
14	E	S	E		P	I	C	I	K		50	I	D	I		T	U	J	U	R
15	I	C	I		R	U	F	U	T		51	U	J	U		W	A	M	A	L
16	U	F	U		L	A	H	A	W		52	A	M	A		B	O	P	O	S
17	A	H	A		S	O	K	O	B		53	O	P	O		D	E	R	E	C
18	O	K	O		C	E	T	E	D		54	E	R	E		J	I	L	I	F
19	E	T	E		F	I	W	I	J		55	I	L	I		M	U	S	U	H
20	I	W	I		H	U	B	U	M		56	U	S	U		P	A	C	A	K
21	U	B	U		K	A	D	A	P		57	A	C	A		R	O	F	O	T
22	A	D	A		T	O	J	O	R		58	O	F	O		L	E	H	E	W
23	O	J	O		W	E	M	E	L		59	E	H	E		S	I	K	I	B
24	E	M	E		B	I	P	I	S		60	I	K	I		C	U	T	U	D
25	I	P	I		D	U	R	U	C		61	U	T	U		F	A	W	A	J
26	U	R	U		J	A	L	A	F		62	A	W	A		H	O	B	O	M
27	A	L	A		M	O	S	O	H		63	O	B	O		K	E	D	E	P
28	O	S	O		P	E	C	E	K		64	E	D	E		T	I	J	I	R
29	E	C	E		R	I	F	I	T		65	I	J	I		W	U	M	U	L
30	I	F	I		L	U	H	U	W		66	U	M	U		B	A	P	A	S
31	U	H	U		S	A	K	A	B		67	A	P	A		D	O	R	O	C
32	A	K	A		C	O	T	O	D		68	O	R	O		J	E	L	E	F
33	O	T	O		F	E	W	E	J		69	E	L	E		M	I	S	I	H
34	E	W	E		H	I	B	I	M		70	I	S	I		P	U	C	U	K
35	I	B	I		K	U	D	U	P											

Tabel 4 Plaintext pada proses dekripsi berdasarkan kata kunci yang telah ditentukan

0	1	2	3	4	5	6	7	8	7	9		0	1	2	3	4	5	6	7	8	9	1
0	C	E	P	A	T		L	A	R	I		3	J	I	T	O	L		B	O	W	U
1	F	I	R	O	W		S	O	L	U		3	M	U	W	E	S		D	E	B	A
2	H	U	L	E	B		C	E	S	A		3	P	A	B	I	C		J	I	D	O
3	K	A	S	I	D		F	I	C	O		3	R	O	D	U	F		M	U	J	E
4	T	O	C	U	J		H	U	F	E		4	L	E	J	A	H		P	A	M	I
5	W	E	F	A	M		K	A	H	I		4	S	I	M	O	K		R	O	P	U
6	B	I	H	O	P		T	O	K	U		4	C	U	P	E	T		L	E	R	A
7	D	U	K	E	R		W	E	T	A		4	F	A	R	I	W		S	I	L	O
8	J	A	T	I	L		B	I	W	O		4	H	O	L	U	B		C	U	S	E
9	M	O	W	U	S		D	U	B	E		4	K	E	S	A	D		F	A	C	I
1	P	E	B	A	C		J	A	D	I		4	T	I	C	O	J		H	O	F	U
1	R	I	D	O	F		M	O	J	U		4	W	U	F	E	M		K	E	H	A
1	L	U	J	E	H		P	E	M	A		4	B	A	H	I	P		T	I	K	O
1	S	A	M	I	K		R	I	P	O		4	D	O	K	U	R		W	U	T	E
1	C	O	P	U	T		L	U	R	E		5	J	E	T	A	L		B	A	W	I
1	F	E	R	A	W		S	A	L	I		5	M	I	W	O	S		D	O	B	U
1	H	I	L	O	B		C	O	S	U		5	P	U	B	E	C		J	E	D	A
1	K	U	S	E	D		F	E	C	A		5	R	A	D	I	F		M	I	J	O
1	T	A	C	I	J		H	I	F	O		5	L	O	J	U	H		P	U	M	E
1	W	O	F	U	M		K	U	H	E		5	S	E	M	A	K		R	A	P	I
2	B	E	H	A	P		T	A	K	I		5	C	I	P	O	T		L	O	R	U
2	D	I	K	O	R		W	O	T	U		5	F	U	R	E	W		S	E	L	A
2	J	U	T	E	L		B	E	W	A		5	H	A	L	I	B		C	I	S	O
2	M	A	W	I	S		D	I	B	O		5	K	O	S	U	D		F	U	C	E
2	P	O	B	U	C		J	U	D	E		6	T	E	C	A	J		H	A	F	I
2	R	E	D	A	F		M	A	J	I		6	W	I	F	O	M		K	O	H	U
2	L	I	J	O	H		P	O	M	U		6	B	U	H	E	P		T	E	K	A
2	S	U	M	E	K		R	E	P	A		6	D	A	K	I	R		W	I	T	O
2	C	A	P	I	T		L	I	R	O		6	J	O	T	U	L		B	U	W	E
2	F	O	R	U	W		S	U	L	E		6	M	E	W	A	S		D	A	B	I
3	H	E	L	A	B		C	A	S	I		6	P	I	B	O	C		J	O	D	U
3	K	I	S	O	D		F	O	C	U		6	R	U	D	E	F		M	E	J	A
3	T	U	C	E	J		H	E	F	A		6	L	A	J	I	H		P	I	M	O
3	W	A	F	I	M		K	I	H	O		6	S	O	M	U	K		R	U	P	E
3	B	O	H	U	P		T	U	K	E		7	C	E	P	A	T		L	A	R	I
3	D	E	K	A	R		W	A	T	I			F	I	R							

0	1	2	3	4	5	6	7	8		0	1	2	3	4	5	6	7	8
0	A	W	A	S		B	O	M		36	O	S	O	D		C	E	K
1	O	B	O	C		D	E	P		37	E	C	E	J		F	I	T
2	E	D	E	F		J	I	R		38	I	F	I	M		H	U	W
3	I	J	I	H		M	U	L		39	U	H	U	P		K	A	B
4	U	M	U	K		P	A	S		40	A	K	A	R		T	O	D
5	A	P	A	T		R	O	C		41	O	T	O	L		W	E	J
6	O	R	O	W		L	E	F		42	E	W	E	S		B	I	M
7	E	L	E	B		S	I	H		43	I	B	I	C		D	U	P
8	I	S	I	D		C	U	K		44	U	D	U	F		J	A	R
9	U	C	U	J		F	A	T		45	A	J	A	H		M	O	L
10	A	F	A	M		H	O	W		46	O	M	O	K		P	E	S
11	O	H	O	P		K	E	B		47	E	P	E	T		R	I	C
12	E	K	E	R		T	I	D		48	I	R	I	W		L	U	F
13	I	T	I	L		W	U	J		49	U	L	U	B		S	A	H
14	U	W	U	S		B	A	M		50	A	S	A	D		C	O	K
15	A	B	A	C		D	O	P		51	O	C	O	J		F	E	T
16	O	D	O	F		J	E	R		52	E	F	E	M		H	I	W
17	E	J	E	H		M	I	L		53	I	H	I	P		K	U	B
18	I	M	I	K		P	U	S		54	U	K	U	R		T	A	D
19	U	P	U	T		R	A	C		55	A	T	A	L		W	O	J
20	A	R	A	W		L	O	F		56	O	W	O	S		B	E	M
21	O	L	O	B		S	E	H		57	E	B	E	C		D	I	P
22	E	S	E	D		C	I	K		58	I	D	I	F		J	U	R
23	I	C	I	J		F	U	T		59	U	J	U	H		M	A	L
24	U	F	U	M		H	A	W		60	A	M	A	K		P	O	S
25	A	H	A	P		K	O	B		61	O	P	O	T		R	E	C
26	O	K	O	R		T	E	D		62	E	R	E	W		L	I	F
27	E	T	E	L		W	I	J		63	I	L	I	B		S	U	H
28	I	W	I	S		B	U	M		64	U	S	U	D		C	A	K
29	U	B	U	C		D	A	P		65	A	C	A	J		F	O	T
30	A	D	A	F		J	O	R		66	O	F	O	M		H	E	W
31	O	J	O	H		M	E	L		67	E	H	E	P		K	I	B
32	E	M	E	K		P	I	S		68	I	K	I	R		T	U	D
33	I	P	I	T		R	U	C		69	U	T	U	L		W	A	J
34	U	R	U	W		L	A	F		70	A	W	A	S		B	O	M
35	A	L	A	B		S	O	H										

0	1	2	3	4	5	6	7	8	9	10	11		0	1	2	3	4	5	6	7	8	9	10	11
0	J	A	L	A	N		B	U	N	T	U		36	H	O	B	O	N		C	A	N	L	A
1	M	O	S	O	N		D	A	N	W	A		37	K	E	D	E	N		F	O	N	S	O
2	P	E	C	E	N		J	O	N	B	O		38	T	I	J	I	N		H	E	N	C	E
3	R	I	F	I	N		M	E	N	D	E		39	W	U	M	U	N		K	I	N	F	I
4	L	U	H	U	N		P	I	N	J	I		40	B	A	P	A	N		T	U	N	H	U
5	S	A	K	A	N		R	U	N	M	U		41	D	O	R	O	N		W	A	N	K	A
6	C	O	T	O	N		L	A	N	P	A		42	J	E	L	E	N		B	O	N	T	O
7	F	E	W	E	N		S	O	N	R	O		43	M	I	S	I	N		D	E	N	W	E
8	H	I	B	I	N		C	E	N	L	E		44	P	U	C	U	N		J	I	N	B	I
9	K	U	D	U	N		F	I	N	S	I		45	R	A	F	A	N		M	U	N	D	U
10	T	A	J	A	N		H	U	N	C	U		46	L	O	H	O	N		P	A	N	J	A
11	W	O	M	O	N		K	A	N	F	A		47	S	E	K	E	N		R	O	N	M	O
12	B	E	P	E	N		T	O	N	H	O		48	C	I	T	I	N		L	E	N	P	E
13	D	I	R	I	N		W	E	N	K	E		49	F	U	W	U	N		S	I	N	R	I
14	J	U	L	U	N		B	I	N	T	I		50	H	A	B	A	N		C	U	N	L	U
15	M	A	S	A	N		D	U	N	W	U		51	K	O	D	O	N		F	A	N	S	A
16	P	O	C	O	N		J	A	N	B	A		52	T	E	J	E	N		H	O	N	C	O
17	R	E	F	E	N		M	O	N	D	O		53	W	I	M	I	N		K	E	N	F	E
18	L	I	H	I	N		P	E	N	J	E		54	B	U	P	U	N		T	I	N	H	I
19	S	U	K	U	N		R	I	N	M	I		55	D	A	R	A	N		W	U	N	K	U
20	C	A	T	A	N		L	U	N	P	U		56	J	O	L	O	N		B	A	N	T	A
21	F	O	W	O	N		S	A	N	R	A		57	M	E	S	E	N		D	O	N	W	O
22	H	E	B	E	N		C	O	N	L	O		58	P	I	C	I	N		J	E	N	B	E
23	K	I	D	I	N		F	E	N	S	E		59	R	U	F	U	N		M	I	N	D	I
24	T	U	J	U	N		H	I	N	C	I		60	L	A	H	A	N		P	U	N	J	U
25	W	A	M	A	N		K	U	N	F	U		61	S	O	K	O	N		R	A	N	M	A
26	B	O	P	O	N		T	A	N	H	A		62	C	E	T	E	N		L	O	N	P	O
27	D	E	R	E	N		W	O	N	K	O		63	F	I	W	I	N		S	E	N	R	E
28	J	I	L	I	N		B	E	N	T	E		64	H	U	B	U	N		C	I	N	L	I
29	M	U	S	U	N		D	I	N	W	I		65	K	A	D	A	N		F	U	N	S	U
30	P	A	C	A	N		J	U	N	B	U		66	T	O	J	O	N		H	A	N	C	A
31	R	O	F	O	N		M	A	N	D	A		67	W	E	M	E	N		K	O	N	F	O
32	L	E	H	E	N		P	O	N	J	O		68	B	I	P	I	N		T	E	N	H	E
33	S	I	K	I	N		R	E	N	M	E		69	D	U	R	U	N		W	I	N	K	I
34	C	U	T	U	N		L	I	N	P	I		70	J	A	L	A	N		B	U	N	T	U
35	F	A	W	A	N		S	U	N	R	U		69	M										

0	1	2	3	4	5	6	7	8	9	10	11	12		0	1	2	3	4	5	6	7	8	9	10	11	12
0	L	A	R	I		J	A	M		D	U	A		36	B	O	W	U		H	O	K		F	A	O
1	S	O	L	U		M	O	P		J	A	O		37	D	E	B	A		K	E	T		H	O	E
2	C	E	S	A		P	E	R		M	O	E		38	J	I	D	O		T	I	W		K	E	I
3	F	I	C	O		R	I	L		P	E	I		39	M	U	J	E		W	U	B		T	I	U
4	H	U	F	E		L	U	S		R	I	U		40	P	A	M	I		B	A	D		W	U	A
5	K	A	H	I		S	A	C		L	U	A		41	R	O	P	U		D	O	J		B	A	O
6	T	O	K	U		C	O	F		S	A	O		42	L	E	R	A		J	E	M		D	O	E
7	W	E	T	A		F	E	H		C	O	E		43	S	I	L	O		M	I	P		J	E	I
8	B	I	W	O		H	I	K		F	E	I		44	C	U	S	E		P	U	R		M	I	U
9	D	U	B	E		K	U	T		H	I	U		45	F	A	C	I		R	A	L		P	U	A
10	J	A	D	I		T	A	W		K	U	A		46	H	O	F	U		L	O	S		R	A	O
11	M	O	J	U		W	O	B		T	A	O		47	K	E	H	A		S	E	C		L	O	E
12	P	E	M	A		B	E	D		W	O	E		48	T	I	K	O		C	I	F		S	E	I
13	R	I	P	O		D	I	J		B	E	I		49	W	U	T	E		F	U	H		C	I	U
14	L	U	R	E		J	U	M		D	I	U		50	B	A	W	I		H	A	K		F	U	A
15	S	A	L	I		M	A	P		J	U	A		51	D	O	B	U		K	O	T		H	A	O
16	C	O	S	U		P	O	R		M	A	O		52	J	E	D	A		T	E	W		K	O	E
17	F	E	C	A		R	E	L		P	O	E		53	M	I	J	O		W	I	B		T	E	I
18	H	I	F	O		L	I	S		R	E	I		54	P	U	M	E		B	U	D		W	I	U
19	K	U	H	E		S	U	C		L	I	U		55	R	A	P	I		D	A	J		B	U	A
20	T	A	K	I		C	A	F		S	U	A		56	L	O	R	U		J	O	M		D	A	O
21	W	O	T	U		F	O	H		C	A	O		57	S	E	L	A		M	E	P		J	O	E
22	B	E	W	A		H	E	K		F	O	E		58	C	I	S	O		P	I	R		M	E	I
23	D	I	B	O		K	I	T		H	E	I		59	F	U	C	E		R	U	L		P	I	U
24	J	U	D	E		T	U	W		K	I	U		60	H	A	F	I		L	A	S		R	U	A
25	M	A	J	I		W	A	B		T	U	A		61	K	O	H	U		S	O	C		L	A	O
26	P	O	M	U		B	O	D		W	A	O		62	T	E	K	A		C	E	F		S	O	E
27	R	E	P	A		D	E	J		B	O	E		63	W	I	T	O		F	I	H		C	E	I
28	L	I	R	O		J	I	M		D	E	I		64	B	U	W	E		H	U	K		F	I	U
29	S	U	L	E		M	U	P		J	I	U		65	D	A	B	I		K	A	T		H	U	A
30	C	A	S	I		P	A	R		M	U	A		66	J	O	D	U		T	O	W		K	A	O
31	F	O	C	U		R	O	L		P	A	O		67	M	E	J	A		W	E	B		T	O	E
32	H	E	F	A		L	E	S		R	O	E		68	P	I	M	O		B	I	D		W	E	I
33	K	I	H	O		S	I	C		L	E	I		69	R	U	P	E		D	U	J		B	I	U
34	T	U	K	E		C	U	F		S	I	U		70	L	A	R	I		J	A	M		D	U	A
35	W	A	T	I		F	A	H		C	U	A														

0	1	2	3	4	5	6	7	8	9	10
0	M	A	J	U		T	E	R	U	S
1	P	O	M	A		W	I	L	A	C
2	R	E	P	O		B	U	S	O	F
3	L	I	R	E		D	A	C	E	H
4	S	U	L	I		J	O	F	I	K
5	C	A	S	U		M	E	H	U	T
6	F	O	C	A		P	I	K	A	W
7	H	E	F	O		R	U	T	O	B
8	K	I	H	E		L	A	W	E	D
9	T	U	K	I		S	O	B	I	J
10	W	A	T	U		C	E	D	U	M
11	B	O	W	A		F	I	J	A	P
12	D	E	B	O		H	U	M	O	R
13	J	I	D	E		K	A	P	E	L
14	M	U	J	I		T	O	R	I	S
15	P	A	M	U		W	E	L	U	C
16	R	O	P	A		B	I	S	A	F
17	L	E	R	O		D	U	C	O	H
18	S	I	L	E		J	A	F	E	K
19	C	U	S	I		M	O	H	I	T
20	F	A	C	U		P	E	K	U	W
21	H	O	F	A		R	I	T	A	B
22	K	E	H	O		L	U	W	O	D
23	T	I	K	E		S	A	B	E	J
24	W	U	T	I		C	O	D	I	M
25	B	A	W	U		F	E	J	U	P
26	D	O	B	A		H	I	M	A	R
27	J	E	D	O		K	U	P	O	L
28	M	I	J	E		T	A	R	E	S
29	P	U	M	I		W	O	L	I	C
30	R	A	P	U		B	E	S	U	F
31	L	O	R	A		D	I	C	A	H
32	S	E	L	O		J	U	F	O	K
33	C	I	S	E		M	A	H	E	T
34	F	U	C	I		P	O	K	I	W
35	H	A	F	U		R	E	T	U	B

0	1	2	3	4	5	6	7	8	9	10
36	K	O	H	A		L	I	W	A	D
37	T	E	K	O		S	U	B	O	J
38	W	I	T	E		C	A	D	E	M
39	B	U	W	I		F	O	J	I	P
40	D	A	B	U		H	E	M	U	R
41	J	O	D	A		K	I	P	A	L
42	M	E	J	O		T	U	R	O	S
43	P	I	M	E		W	A	L	E	C
44	R	U	P	I		B	O	S	I	F
45	L	A	R	U		D	E	C	U	H
46	S	O	L	A		J	I	F	A	K
47	C	E	S	O		M	U	H	O	T
48	F	I	C	E		P	A	K	E	W
49	H	U	F	I		R	O	T	I	B
50	K	A	H	U		L	E	W	U	D
51	T	O	K	A		S	I	B	A	J
52	W	E	T	O		C	U	D	O	M
53	B	I	W	E		F	A	J	E	P
54	D	U	B	I		H	O	M	I	R
55	J	A	D	U		K	E	P	U	L
56	M	O	J	A		T	I	R	A	S
57	P	E	M	O		W	U	L	O	C
58	R	I	P	E		B	A	S	E	F
59	L	U	R	I		D	O	C	I	H
60	S	A	L	U		J	E	F	U	K
61	C	O	S	A		M	I	H	A	T
62	F	E	C	O		P	U	K	O	W
63	H	I	F	E		R	A	T	E	B
64	K	U	H	I		L	O	W	I	D
65	T	A	K	U		S	E	B	U	J
66	W	O	T	A		C	I	D	A	M
67	B	E	W	O		F	U	J	O	P
68	D	I	B	E		H	A	M	E	R
69	J	U	D	I		K	O	P	I	L
70	M	A	J	U		T	E	R	U	S

0	1	2	3	4	5	6	7	8	9	10	11	12		0	1	2	3	4	5	6	7	8	9	10	11	12
0	M	U	S	U	H		D	A	T	A	N	G		36	K	A	D	A	P		F	O	L	O	N	G
1	P	A	C	A	K		J	O	W	O	N	G		37	T	O	J	O	R		H	E	S	E	N	G
2	R	O	F	O	T		M	E	B	E	N	G		38	W	E	M	E	L		K	I	C	I	N	G
3	L	E	H	E	W		P	I	D	I	N	G		39	B	I	P	I	S		T	U	F	U	N	G
4	S	I	K	I	B		R	U	J	U	N	G		40	D	U	R	U	C		W	A	H	A	N	G
5	C	U	T	U	D		L	A	M	A	N	G		41	J	A	L	A	F		B	O	K	O	N	G
6	F	A	W	A	J		S	O	P	O	N	G		42	M	O	S	O	H		D	E	T	E	N	G
7	H	O	B	O	M		C	E	R	E	N	G		43	P	E	C	E	K		J	I	W	I	N	G
8	K	E	D	E	P		F	I	L	I	N	G		44	R	I	F	I	T		M	U	B	U	N	G
9	T	I	J	I	R		H	U	S	U	N	G		45	L	U	H	U	W		P	A	D	A	N	G
10	W	U	M	U	L		K	A	C	A	N	G		46	S	A	K	A	B		R	O	J	O	N	G
11	B	A	P	A	S		T	O	F	O	N	G		47	C	O	T	O	D		L	E	M	E	N	G
12	D	O	R	O	C		W	E	H	E	N	G		48	F	E	W	E	J		S	I	P	I	N	G
13	J	E	L	E	F		B	I	K	I	N	G		49	H	I	B	I	M		C	U	R	U	N	G
14	M	I	S	I	H		D	U	T	U	N	G		50	K	U	D	U	P		F	A	L	A	N	G
15	P	U	C	U	K		J	A	W	A	N	G		51	T	A	J	A	R		H	O	S	O	N	G
16	R	A	F	A	T		M	O	B	O	N	G		52	W	O	M	O	L		K	E	C	E	N	G
17	L	O	H	O	W		P	E	D	E	N	G		53	B	E	P	E	S		T	I	F	I	N	G
18	S	E	K	E	B		R	I	J	I	N	G		54	D	I	R	I	C		W	U	H	U	N	G
19	C	I	T	I	D		L	U	M	U	N	G		55	J	U	L	U	F		B	A	K	A	N	G
20	F	U	W	U	J		S	A	P	A	N	G		56	M	A	S	A	H		D	O	T	O	N	G
21	H	A	B	A	M		C	O	R	O	N	G		57	P	O	C	O	K		J	E	W	E	N	G
22	K	O	D	O	P		F	E	L	E	N	G		58	R	E	F	E	T		M	I	B	I	N	G
23	T	E	J	E	R		H	I	S	I	N	G		59	L	I	H	I	W		P	U	D	U	N	G
24	W	I	M	I	L		K	U	C	U	N	G		60	S	U	K	U	B		R	A	J	A	N	G
25	B	U	P	U	S		T	A	F	A	N	G		61	C	A	T	A	D		L	O	M	O	N	G
26	D	A	R	A	C		W	O	H	O	N	G		62	F	O	W	O	J		S	E	P	E	N	G
27	J	O	L	O	F		B	E	K	E	N	G		63	H	E	B	E	M		C	I	R	I	N	G
28	M	E	S	E	H		D	I	T	I	N	G		64	K	I	D	I	P		F	U	L	U	N	G
29	P	I	C	I	K		J	U	W	U	N	G		65	T	U	J	U	R		H	A	S	A	N	G
30	R	U	F	U	T		M	A	B	A	N	G		66	W	A	M	A	L		K	O	C	O	N	G
31	L	A	H	A	W		P	O	D	O	N	G		67	B	O	P	O	S		T	E	F	E	N	G
32	S	O	K	O	B		R	E	J	E	N	G		68	D	E	R	E	C		W	I	H	I	N	G
33	C	E	T	E	D		L	I	M	I	N	G		69	J	I	L	I	F		B	U	K	U	N	G
34	F	I	W	I	J		S	U	P	U	N	G		70	M	U	S	U	H		D	A	T	A	N	G
35	H	U	B	U	M		C	A	R	A	N	G														

0	1	2	3	4	5	6	7	8	9	10	11	12
0	J	A	L	A	N		M	U	N	D	U	R
1	M	O	S	O	N		P	A	N	J	A	L
2	P	E	C	E	N		R	O	N	M	O	S
3	R	I	F	I	N		L	E	N	P	E	C
4	L	U	H	U	N		S	I	N	R	I	F
5	S	A	K	A	N		C	U	N	L	U	H
6	C	O	T	O	N		F	A	N	S	A	K
7	F	E	W	E	N		H	O	N	C	O	T
8	H	I	B	I	N		K	E	N	F	E	W
9	K	U	D	U	N		T	I	N	H	I	B
10	T	A	J	A	N		W	U	N	K	U	D
11	W	O	M	O	N		B	A	N	T	A	J
12	B	E	P	E	N		D	O	N	W	O	M
13	D	I	R	I	N		J	E	N	B	E	P
14	J	U	L	U	N		M	I	N	D	I	R
15	M	A	S	A	N		P	U	N	J	U	L
16	P	O	C	O	N		R	A	N	M	A	S
17	R	E	F	E	N		L	O	N	P	O	C
18	L	I	H	I	N		S	E	N	R	E	F
19	S	U	K	U	N		C	I	N	L	I	H
20	C	A	T	A	N		F	U	N	S	U	K
21	F	O	W	O	N		H	A	N	C	A	T
22	H	E	B	E	N		K	O	N	F	O	W
23	K	I	D	I	N		T	E	N	H	E	B
24	T	U	J	U	N		W	I	N	K	I	D
25	W	A	M	A	N		B	U	N	T	U	J
26	B	O	P	O	N		D	A	N	W	A	M
27	D	E	R	E	N		J	O	N	B	O	P
28	J	I	L	I	N		M	E	N	D	E	R
29	M	U	S	U	N		P	I	N	J	I	L
30	P	A	C	A	N		R	U	N	M	U	S
31	R	O	F	O	N		L	A	N	P	A	C
32	L	E	H	E	N		S	O	N	R	O	F
33	S	I	K	I	N		C	E	N	L	E	H
34	C	U	T	U	N		F	I	N	S	I	K
35	F	A	W	A	N		H	U	N	C	U	T

0	1	2	3	4	5	6	7	8	9	10	11	12
36	H	O	B	O	N		K	A	N	F	A	W
37	K	E	D	E	N		T	O	N	H	O	B
38	T	I	J	I	N		W	E	N	K	E	D
39	W	U	M	U	N		B	I	N	T	I	J
40	B	A	P	A	N		D	U	N	W	U	M
41	D	O	R	O	N		J	A	N	B	A	P
42	J	E	L	E	N		M	O	N	D	O	R
43	M	I	S	I	N		P	E	N	J	E	L
44	P	U	C	U	N		R	I	N	M	I	S
45	R	A	F	A	N		L	U	N	P	U	C
46	L	O	H	O	N		S	A	N	R	A	F
47	S	E	K	E	N		C	O	N	L	O	H
48	C	I	T	I	N		F	E	N	S	E	K
49	F	U	W	U	N		H	I	N	C	I	T
50	H	A	B	A	N		K	U	N	F	U	W
51	K	O	D	O	N		T	A	N	H	A	B
52	T	E	J	E	N		W	O	N	K	O	D
53	W	I	M	I	N		B	E	N	T	E	J
54	B	U	P	U	N		D	I	N	W	I	M
55	D	A	R	A	N		J	U	N	B	U	P
56	J	O	L	O	N		M	A	N	D	A	R
57	M	E	S	E	N		P	O	N	J	O	L
58	P	I	C	I	N		R	E	N	M	E	S
59	R	U	F	U	N		L	I	N	P	I	C
60	L	A	H	A	N		S	U	N	R	U	F
61	S	O	K	O	N		C	A	N	L	A	H
62	C	E	T	E	N		F	O	N	S	O	K
63	F	I	W	I	N		H	E	N	C	E	T
64	H	U	B	U	N		K	I	N	F	I	W
65	K	A	D	A	N		T	U	N	H	U	B
66	T	O	J	O	N		W	A	N	K	A	D
67	W	E	M	E	N		B	O	N	T	O	J
68	B	I	P	I	N		D	E	N	W	E	M
69	D	U	R	U	N		J	I	N	B	I	P
70	J	A	L	A	N		M	U	N	D	U	R

0.	1	2	3	4	5	6	7	8	9	10		0	1	2	3	4	5	6	7	8	9	10	
0	J	A	L	A	N		M	A	J	U		36	H	O	B	O	N		K	O	H	A	
1	M	O	S	O	N		P	O	M	A		37	K	E	D	E	N		T	E	K	O	
2	P	E	C	E	N		R	E	P	O		38	T	I	J	I	N		W	I	T	E	
3	R	I	F	I	N		L	I	R	E		39	W	U	M	U	N		B	U	W	I	
4	L	U	H	U	N		S	U	L	I		40	B	A	P	A	N		D	A	B	U	
5	S	A	K	A	N		C	A	S	U		41	D	O	R	O	N		J	O	D	A	
6	C	O	T	O	N		F	O	C	A		42	J	E	L	E	N		M	E	J	O	
7	F	E	W	E	N		H	E	F	O		43	M	I	S	I	N		P	I	M	E	
8	H	I	B	I	N		K	I	H	E		44	P	U	C	U	N		R	U	P	I	
9	K	U	D	U	N		T	U	K	I		45	R	A	F	A	N		L	A	R	U	
10	T	A	J	A	N		W	A	T	U		46	L	O	H	O	N		S	O	L	A	
11	W	O	M	O	N		B	O	W	A		47	S	E	K	E	N		C	E	S	O	
12	B	E	P	E	N		D	E	B	O		48	C	I	T	I	N		F	I	C	E	
13	D	I	R	I	N		J	I	D	E		49	F	U	W	U	N		H	U	F	I	
14	J	U	L	U	N		M	U	J	I		50	H	A	B	A	N		K	A	H	U	
15	M	A	S	A	N		P	A	M	U		51	K	O	D	O	N		T	O	K	A	
16	P	O	C	O	N		R	O	P	A		52	T	E	J	E	N		W	E	T	O	
17	R	E	F	E	N		L	E	R	O		53	W	I	M	I	N		B	I	W	E	
18	L	I	H	I	N		S	I	L	E		54	B	U	P	U	N		D	U	B	I	
19	S	U	K	U	N		C	U	S	I		55	D	A	R	A	N		J	A	D	U	
20	C	A	T	A	N		F	A	C	U		56	J	O	L	O	N		M	O	J	A	
21	F	O	W	O	N		H	O	F	A		57	M	E	S	E	N		P	E	M	O	
22	H	E	B	E	N		K	E	H	O		58	P	I	C	I	N		R	I	P	E	
23	K	I	D	I	N		T	I	K	E		59	R	U	F	U	N		L	U	R	I	
24	T	U	J	U	N		W	U	T	I		60	L	A	H	A	N		S	A	L	U	
25	W	A	M	A	N		B	A	W	U		61	S	O	K	O	N		C	O	S	A	
26	B	O	P	O	N		D	O	B	A		62	C	E	T	E	N		F	E	C	O	
27	D	E	R	E	N		J	E	D	O		63	F	I	W	I	N		H	I	F	E	
28	J	I	L	I	N		M	I	J	E		64	H	U	B	U	N		K	U	H	I	
29	M	U	S	U	N		P	U	M	I		65	K	A	D	A	N		T	A	K	U	
30	P	A	C	A	N		R	A	P	U		66	T	O	J	O	N		W	O	T	A	
31	R	O	F	O	N		L	O	R	A		67	W	E	M	E	N		B	E	W	O	
32	L	E	H	E	N		S	E	L	O		68	B	I	P	I	N		D	I	B	E	
33	S	I	K	I	N		C	I	S	E		69	D	U	R	U	N		J	U	D	I	
34	C	U	T	U	N		F	U	C	I		70	J	A	L	A	N		M	A	J	U	
35	F	A	W	A	N		H	A	F	U													

0	1	2	3	4	5	6	7	8	9	10	11
0	R	U	A	N	G		L	A	W	A	N
1	L	A	O	N	G		S	O	B	O	N
2	S	O	E	N	G		C	E	D	E	N
3	C	E	I	N	G		F	I	J	I	N
4	F	I	U	N	G		H	U	M	U	N
5	H	U	A	N	G		K	A	P	A	N
6	K	A	O	N	G		T	O	R	O	N
7	T	O	E	N	G		W	E	L	E	N
8	W	E	I	N	G		B	I	S	I	N
9	B	I	U	N	G		D	U	C	U	N
10	D	U	A	N	G		J	A	F	A	N
11	J	A	O	N	G		M	O	H	O	N
12	M	O	E	N	G		P	E	K	E	N
13	P	E	I	N	G		R	I	T	I	N
14	R	I	U	N	G		L	U	W	U	N
15	L	U	A	N	G		S	A	B	A	N
16	S	A	O	N	G		C	O	D	O	N
17	C	O	E	N	G		F	E	J	E	N
18	F	E	I	N	G		H	I	M	I	N
19	H	I	U	N	G		K	U	P	U	N
20	K	U	A	N	G		T	A	R	A	N
21	T	A	O	N	G		W	O	L	O	N
22	W	O	E	N	G		B	E	S	E	N
23	B	E	I	N	G		D	I	C	I	N
24	D	I	U	N	G		J	U	F	U	N
25	J	U	A	N	G		M	A	H	A	N
26	M	A	O	N	G		P	O	K	O	N
27	P	O	E	N	G		R	E	T	E	N
28	R	E	I	N	G		L	I	W	I	N
29	L	I	U	N	G		S	U	B	U	N
30	S	U	A	N	G		C	A	D	A	N
31	C	A	O	N	G		F	O	J	O	N
32	F	O	E	N	G		H	E	M	E	N
33	H	E	I	N	G		K	I	P	I	N
34	K	I	U	N	G		T	U	R	U	N
35	T	U	A	N	G		W	A	L	A	N

0	1	2	3	4	5	6	7	8	9	10	11
36	W	A	O	N	G		B	O	S	O	N
37	B	O	E	N	G		D	E	C	E	N
38	D	E	I	N	G		J	I	F	I	N
39	J	I	U	N	G		M	U	H	U	N
40	M	U	A	N	G		P	A	K	A	N
41	P	A	O	N	G		R	O	T	O	N
42	R	O	E	N	G		L	E	W	E	N
43	L	E	I	N	G		S	I	B	I	N
44	S	I	U	N	G		C	U	D	U	N
45	C	U	A	N	G		F	A	J	A	N
46	F	A	O	N	G		H	O	M	O	N
47	H	O	E	N	G		K	E	P	E	N
48	K	E	I	N	G		T	I	R	I	N
49	T	I	U	N	G		W	U	L	U	N
50	W	U	A	N	G		B	A	S	A	N
51	B	A	O	N	G		D	O	C	O	N
52	D	O	E	N	G		J	E	F	E	N
53	J	E	I	N	G		M	I	H	I	N
54	M	I	U	N	G		P	U	K	U	N
55	P	U	A	N	G		R	A	T	A	N
56	R	A	O	N	G		L	O	W	O	N
57	L	O	E	N	G		S	E	B	E	N
58	S	E	I	N	G		C	I	D	I	N
59	C	I	U	N	G		F	U	J	U	N
60	F	U	A	N	G		H	A	M	A	N
61	H	A	O	N	G		K	O	P	O	N
62	K	O	E	N	G		T	E	R	E	N
63	T	E	I	N	G		W	I	L	I	N
64	W	I	U	N	G		B	U	S	U	N
65	B	U	A	N	G		D	A	C	A	N
66	D	A	O	N	G		J	O	F	O	N
67	J	O	E	N	G		M	E	H	E	N
68	M	E	I	N	G		P	I	K	I	N
69	P	I	U	N	G		R	U	T	U	N
70	R	U	A	N	G		L	A	W	A	N

0	1	2	3	4	5	6	7	8	9	10
0	L	A	W	A	N		L	A	R	I
1	S	O	B	O	N		S	O	L	U
2	C	E	D	E	N		C	E	S	A
3	F	I	J	I	N		F	I	C	O
4	H	U	M	U	N		H	U	F	E
5	K	A	P	A	N		K	A	H	I
6	T	O	R	O	N		T	O	K	U
7	W	E	L	E	N		W	E	T	A
8	B	I	S	I	N		B	I	W	O
9	D	U	C	U	N		D	U	B	E
10	J	A	F	A	N		J	A	D	I
11	M	O	H	O	N		M	O	J	U
12	P	E	K	E	N		P	E	M	A
13	R	I	T	I	N		R	I	P	O
14	L	U	W	U	N		L	U	R	E
15	S	A	B	A	N		S	A	L	I
16	C	O	D	O	N		C	O	S	U
17	F	E	J	E	N		F	E	C	A
18	H	I	M	I	N		H	I	F	O
19	K	U	P	U	N		K	U	H	E
20	T	A	R	A	N		T	A	K	I
21	W	O	L	O	N		W	O	T	U
22	B	E	S	E	N		B	E	W	A
23	D	I	C	I	N		D	I	B	O
24	J	U	F	U	N		J	U	D	E
25	M	A	H	A	N		M	A	J	I
26	P	O	K	O	N		P	O	M	U
27	R	E	T	E	N		R	E	P	A
28	L	I	W	I	N		L	I	R	O
29	S	U	B	U	N		S	U	L	E
30	C	A	D	A	N		C	A	S	I
31	F	O	J	O	N		F	O	C	U
32	H	E	M	E	N		H	E	F	A
33	K	I	P	I	N		K	I	H	O
34	T	U	R	U	N		T	U	K	E
35	W	A	L	A	N		W	A	T	I

0	1	2	3	4	5	6	7	8	9	10
36	B	O	S	O	N		B	O	W	U
37	D	E	C	E	N		D	E	B	A
38	J	I	F	I	N		J	I	D	O
39	M	U	H	U	N		M	U	J	E
40	P	A	K	A	N		P	A	M	I
41	R	O	T	O	N		R	O	P	U
42	L	E	W	E	N		L	E	R	A
43	S	I	B	I	N		S	I	L	O
44	C	U	D	U	N		C	U	S	E
45	F	A	J	A	N		F	A	C	I
46	H	O	M	O	N		H	O	F	U
47	K	E	P	E	N		K	E	H	A
48	T	I	R	I	N		T	I	K	O
49	W	U	L	U	N		W	U	T	E
50	B	A	S	A	N		B	A	W	I
51	D	O	C	O	N		D	O	B	U
52	J	E	F	E	N		J	E	D	A
53	M	I	H	I	N		M	I	J	O
54	P	U	K	U	N		P	U	M	E
55	R	A	T	A	N		R	A	P	I
56	L	O	W	O	N		L	O	R	U
57	S	E	B	E	N		S	E	L	A
58	C	I	D	I	N		C	I	S	O
59	F	U	J	U	N		F	U	C	E
60	H	A	M	A	N		H	A	F	I
61	K	O	P	O	N		K	O	H	U
62	T	E	R	E	N		T	E	K	A
63	W	I	L	I	N		W	I	T	O
64	B	U	S	U	N		B	U	W	E
65	D	A	C	A	N		D	A	B	I
66	J	O	F	O	N		J	O	D	U
67	M	E	H	E	N		M	E	J	A
68	P	I	K	I	N		P	I	M	O
69	R	U	T	U	N		R	U	P	E
70	L	A	W	A	N		L	A	R	I

0	1	2	3	4	5	6	7	8	9	10		0	1	2	3	4	5	6	7	8	9	10
0	M	U	S	U	H		T	I	B	A		36	K	A	D	A	P		L	U	C	O
1	P	A	C	A	K		W	U	D	O		37	T	O	J	O	R		S	A	F	E
2	R	O	F	O	T		B	A	J	E		38	W	E	M	E	L		C	O	H	I
3	L	E	H	E	W		D	O	M	I		39	B	I	P	I	S		F	E	K	U
4	S	I	K	I	B		J	E	P	U		40	D	U	R	U	C		H	I	T	A
5	C	U	T	U	D		M	I	R	A		41	J	A	L	A	F		K	U	W	O
6	F	A	W	A	J		P	U	L	O		42	M	O	S	O	H		T	A	B	E
7	H	O	B	O	M		R	A	S	E		43	P	E	C	E	K		W	O	D	I
8	K	E	D	E	P		L	O	C	I		44	R	I	F	I	T		B	E	J	U
9	T	I	J	I	R		S	E	F	U		45	L	U	H	U	W		D	I	M	A
10	W	U	M	U	L		C	I	H	A		46	S	A	K	A	B		J	U	P	O
11	B	A	P	A	S		F	U	K	O		47	C	O	T	O	D		M	A	R	E
12	D	O	R	O	C		H	A	T	E		48	F	E	W	E	J		P	O	L	I
13	J	E	L	E	F		K	O	W	I		49	H	I	B	I	M		R	E	S	U
14	M	I	S	I	H		T	E	B	U		50	K	U	D	U	P		L	I	C	A
15	P	U	C	U	K		W	I	D	A		51	T	A	J	A	R		S	U	F	O
16	R	A	F	A	T		B	U	J	O		52	W	O	M	O	L		C	A	H	E
17	L	O	H	O	W		D	A	M	E		53	B	E	P	E	S		F	O	K	I
18	S	E	K	E	B		J	O	P	I		54	D	I	R	I	C		H	E	T	U
19	C	I	T	I	D		M	E	R	U		55	J	U	L	U	F		K	I	W	A
20	F	U	W	U	J		P	I	L	A		56	M	A	S	A	H		T	U	B	O
21	H	A	B	A	M		R	U	S	O		57	P	O	C	O	K		W	A	D	E
22	K	O	D	O	P		L	A	C	E		58	R	E	F	E	T		B	O	J	I
23	T	E	J	E	R		S	O	F	I		59	L	I	H	I	W		D	E	M	U
24	W	I	M	I	L		C	E	H	U		60	S	U	K	U	B		J	I	P	A
25	B	U	P	U	S		F	I	K	A		61	C	A	T	A	D		M	U	R	O
26	D	A	R	A	C		H	U	T	O		62	F	O	W	O	J		P	A	L	E
27	J	O	L	O	F		K	A	W	E		63	H	E	B	E	M		R	O	S	I
28	M	E	S	E	H		T	O	B	I		64	K	I	D	I	P		L	E	C	U
29	P	I	C	I	K		W	E	D	U		65	T	U	J	U	R		S	I	F	A
30	R	U	F	U	T		B	I	J	A		66	W	A	M	A	L		C	U	H	O
31	L	A	H	A	W		D	U	M	O		67	B	O	P	O	S		F	A	K	E
32	S	O	K	O	B		J	A	P	E		68	D	E	R	E	C		H	O	T	I
33	C	E	T	E	D		M	O	R	I		69	J	I	L	I	F		K	E	W	U
34	F	I	W	I	J		P	E	L	U		70	M	U	S	U	H		T	I	B	A
35	H	U	B	U	M		R	I	S	A												

0	1	2	3	4	5	6	7	8	9	10	11
0	K	I	J	A	N	G		S	A	T	U
1	T	U	M	O	N	G		C	O	W	A
2	W	A	P	E	N	G		F	E	B	O
3	B	O	R	I	N	G		H	I	D	E
4	D	E	L	U	N	G		K	U	J	I
5	J	I	S	A	N	G		T	A	M	U
6	M	U	C	O	N	G		W	O	P	A
7	P	A	F	E	N	G		B	E	R	O
8	R	O	H	I	N	G		D	I	L	E
9	L	E	K	U	N	G		J	U	S	I
10	S	I	T	A	N	G		M	A	C	U
11	C	U	W	O	N	G		P	O	F	A
12	F	A	B	E	N	G		R	E	H	O
13	H	O	D	I	N	G		L	I	K	E
14	K	E	J	U	N	G		S	U	T	I
15	T	I	M	A	N	G		C	A	W	U
16	W	U	P	O	N	G		F	O	B	A
17	B	A	R	E	N	G		H	E	D	O
18	D	O	L	I	N	G		K	I	J	E
19	J	E	S	U	N	G		T	U	M	I
20	M	I	C	A	N	G		W	A	P	U
21	P	U	F	O	N	G		B	O	R	A
22	R	A	H	E	N	G		D	E	L	O
23	L	O	K	I	N	G		J	I	S	E
24	S	E	T	U	N	G		M	U	C	I
25	C	I	W	A	N	G		P	A	F	U
26	F	U	B	O	N	G		R	O	H	A
27	H	A	D	E	N	G		L	E	K	O
28	K	O	J	I	N	G		S	I	T	E
29	T	E	M	U	N	G		C	U	W	I
30	W	I	P	A	N	G		F	A	B	U
31	B	U	R	O	N	G		H	O	D	A
32	D	A	L	E	N	G		K	E	J	O
33	J	O	S	I	N	G		T	I	M	E
34	M	E	C	U	N	G		W	U	P	I
35	P	I	F	A	N	G		B	A	R	U

0	1	2	3	4	5	6	7	8	9	10	11
36	R	U	H	O	N	G		D	O	L	A
37	L	A	K	E	N	G		J	E	S	O
38	S	O	T	I	N	G		M	I	C	E
39	C	E	W	U	N	G		P	U	F	I
40	F	I	B	A	N	G		R	A	H	U
41	H	U	D	O	N	G		L	O	K	A
42	K	A	J	E	N	G		S	E	T	O
43	T	O	M	I	N	G		C	I	W	E
44	W	E	P	U	N	G		F	U	B	I
45	B	I	R	A	N	G		H	A	D	U
46	D	U	L	O	N	G		K	O	J	A
47	J	A	S	E	N	G		T	E	M	O
48	M	O	C	I	N	G		W	I	P	E
49	P	E	F	U	N	G		B	U	R	I
50	R	I	H	A	N	G		D	A	L	U
51	L	U	K	O	N	G		J	O	S	A
52	S	A	T	E	N	G		M	E	C	O
53	C	O	W	I	N	G		P	I	F	E
54	F	E	B	U	N	G		R	U	H	I
55	H	I	D	A	N	G		L	A	K	U
56	K	U	J	O	N	G		S	O	T	A
57	T	A	M	E	N	G		C	E	W	O
58	W	O	P	I	N	G		F	I	B	E
59	B	E	R	U	N	G		H	U	D	I
60	D	I	L	A	N	G		K	A	J	U
61	J	U	S	O	N	G		T	O	M	A
62	M	A	C	E	N	G		W	E	P	O
63	P	O	F	I	N	G		B	I	R	E
64	R	E	H	U	N	G		D	U	L	I
65	L	I	K	A	N	G		J	A	S	U
66	S	U	T	O	N	G		M	O	C	A
67	C	A	W	E	N	G		P	E	F	O
68	F	O	B	I	N	G		R	I	H	E
69	H	E	D	U	N	G		L	U	K	I
70	K	I	J	A	N	G		S	A	T	U

0	1	2	3	4	5	6	7	8	9	10	11	12
0	S	E	R	A	N	G		M	U	S	U	H
1	C	I	L	O	N	G		P	A	C	A	K
2	F	U	S	E	N	G		R	O	F	O	T
3	H	A	C	I	N	G		L	E	H	E	W
4	K	O	F	U	N	G		S	I	K	I	B
5	T	E	H	A	N	G		C	U	T	U	D
6	W	I	K	O	N	G		F	A	W	A	J
7	B	U	T	E	N	G		H	O	B	O	M
8	D	A	W	I	N	G		K	E	D	E	P
9	J	O	B	U	N	G		T	I	J	I	R
10	M	E	D	A	N	G		W	U	M	U	L
11	P	I	J	O	N	G		B	A	P	A	S
12	R	U	M	E	N	G		D	O	R	O	C
13	L	A	P	I	N	G		J	E	L	E	F
14	S	O	R	U	N	G		M	I	S	I	H
15	C	E	L	A	N	G		P	U	C	U	K
16	F	I	S	O	N	G		R	A	F	A	T
17	H	U	C	E	N	G		L	O	H	O	W
18	K	A	F	I	N	G		S	E	K	E	B
19	T	O	H	U	N	G		C	I	T	I	D
20	W	E	K	A	N	G		F	U	W	U	J
21	B	I	T	O	N	G		H	A	B	A	M
22	D	U	W	E	N	G		K	O	D	O	P
23	J	A	B	I	N	G		T	E	J	E	R
24	M	O	D	U	N	G		W	I	M	I	L
25	P	E	J	A	N	G		B	U	P	U	S
26	R	I	M	O	N	G		D	A	R	A	C
27	L	U	P	E	N	G		J	O	L	O	F
28	S	A	R	I	N	G		M	E	S	E	H
29	C	O	L	U	N	G		P	I	C	I	K
30	F	E	S	A	N	G		R	U	F	U	T
31	H	I	C	O	N	G		L	A	H	A	W
32	K	U	F	E	N	G		S	O	K	O	B
33	T	A	H	I	N	G		C	E	T	E	D
34	W	O	K	U	N	G		F	I	W	I	J
35	B	E	T	A	N	G		H	U	B	U	M

0	1	2	3	4	5	6	7	8	9	10	11	12
36	D	I	W	O	N	G		K	A	D	A	P
37	J	U	B	E	N	G		T	O	J	O	R
38	M	A	D	I	N	G		W	E	M	E	L
39	P	O	J	U	N	G		B	I	P	I	S
40	R	E	M	A	N	G		D	U	R	U	C
41	L	I	P	O	N	G		J	A	L	A	F
42	S	U	R	E	N	G		M	O	S	O	H
43	C	A	L	I	N	G		P	E	C	E	K
44	F	O	S	U	N	G		R	I	F	I	T
45	H	E	C	A	N	G		L	U	H	U	W
46	K	I	F	O	N	G		S	A	K	A	B
47	T	U	H	E	N	G		C	O	T	O	D
48	W	A	K	I	N	G		F	E	W	E	J
49	B	O	T	U	N	G		H	I	B	I	M
50	D	E	W	A	N	G		K	U	D	U	P
51	J	I	B	O	N	G		T	A	J	A	R
52	M	U	D	E	N	G		W	O	M	O	L
53	P	A	J	I	N	G		B	E	P	E	S
54	R	O	M	U	N	G		D	I	R	I	C
55	L	E	P	A	N	G		J	U	L	U	F
56	S	I	R	O	N	G		M	A	S	A	H
57	C	U	L	E	N	G		P	O	C	O	K
58	F	A	S	I	N	G		R	E	F	E	T
59	H	O	C	U	N	G		L	I	H	I	W
60	K	E	F	A	N	G		S	U	K	U	B
61	T	I	H	O	N	G		C	A	T	A	D
62	W	U	K	E	N	G		F	O	W	O	J
63	B	A	T	I	N	G		H	E	B	E	M
64	D	O	W	U	N	G		K	I	D	I	P
65	J	E	B	A	N	G		T	U	J	U	R
66	M	I	D	O	N	G		W	A	M	A	L
67	P	U	J	E	N	G		B	O	P	O	S
68	R	A	M	I	N	G		D	E	R	E	C
69	L	O	P	U	N	G		J	I	L	I	F
70	S	E	R	A	N	G		M	U	S	U	H

0	1	2	3	4	5	6	7	8	9	10	11
0	K	A	K	I		T	A	N	G	A	N
1	T	O	T	U		W	O	N	G	O	N
2	W	E	W	A		B	E	N	G	E	N
3	B	I	B	O		D	I	N	G	I	N
4	D	U	D	E		J	U	N	G	U	N
5	J	A	J	I		M	A	N	G	A	N
6	M	O	M	U		P	O	N	G	O	N
7	P	E	P	A		R	E	N	G	E	N
8	R	I	R	O		L	I	N	G	I	N
9	L	U	L	E		S	U	N	G	U	N
10	S	A	S	I		C	A	N	G	A	N
11	C	O	C	U		F	O	N	G	O	N
12	F	E	F	A		H	E	N	G	E	N
13	H	I	H	O		K	I	N	G	I	N
14	K	U	K	E		T	U	N	G	U	N
15	T	A	T	I		W	A	N	G	A	N
16	W	O	W	U		B	O	N	G	O	N
17	B	E	B	A		D	E	N	G	E	N
18	D	I	D	O		J	I	N	G	I	N
19	J	U	J	E		M	U	N	G	U	N
20	M	A	M	I		P	A	N	G	A	N
21	P	O	P	U		R	O	N	G	O	N
22	R	E	R	A		L	E	N	G	E	N
23	L	I	L	O		S	I	N	G	I	N
24	S	U	S	E		C	U	N	G	U	N
25	C	A	C	I		F	A	N	G	A	N
26	F	O	F	U		H	O	N	G	O	N
27	H	E	H	A		K	E	N	G	E	N
28	K	I	K	O		T	I	N	G	I	N
29	T	U	T	E		W	U	N	G	U	N
30	W	A	W	I		B	A	N	G	A	N
31	B	O	B	U		D	O	N	G	O	N
32	D	E	D	A		J	E	N	G	E	N
33	J	I	J	O		M	I	N	G	I	N
34	M	U	M	E		P	U	N	G	U	N
35	P	A	P	I		R	A	N	G	A	N

0	1	2	3	4	5	6	7	8	9	10	11
36	R	O	R	U		L	O	N	G	O	N
37	L	E	L	A		S	E	N	G	E	N
38	S	I	S	O		C	I	N	G	I	N
39	C	U	C	E		F	U	N	G	U	N
40	F	A	F	I		H	A	N	G	A	N
41	H	O	H	U		K	O	N	G	O	N
42	K	E	K	A		T	E	N	G	E	N
43	T	I	T	O		W	I	N	G	I	N
44	W	U	W	E		B	U	N	G	U	N
45	B	A	B	I		D	A	N	G	A	N
46	D	O	D	U		J	O	N	G	O	N
47	J	E	J	A		M	E	N	G	E	N
48	M	I	M	O		P	I	N	G	I	N
49	P	U	P	E		R	U	N	G	U	N
50	R	A	R	I		L	A	N	G	A	N
51	L	O	L	U		S	O	N	G	O	N
52	S	E	S	A		C	E	N	G	E	N
53	C	I	C	O		F	I	N	G	I	N
54	F	U	F	E		H	U	N	G	U	N
55	H	A	H	I		K	A	N	G	A	N
56	K	O	K	U		T	O	N	G	O	N
57	T	E	T	A		W	E	N	G	E	N
58	W	I	W	O		B	I	N	G	I	N
59	B	U	B	E		D	U	N	G	U	N
60	D	A	D	I		J	A	N	G	A	N
61	J	O	J	U		M	O	N	G	O	N
62	M	E	M	A		P	E	N	G	E	N
63	P	I	P	O		R	I	N	G	I	N
64	R	U	R	E		L	U	N	G	U	N
65	L	A	L	I		S	A	N	G	A	N
66	S	O	S	U		C	O	N	G	O	N
67	C	E	C	A		F	E	N	G	E	N
68	F	I	F	O		H	I	N	G	I	N
69	H	U	H	E		K	U	N	G	U	N
70	K	A	K	I		T	A	N	G	A	N

0	1	2	3	4	5	6	7	8	9	10		0	1	2	3	4	5	6	7	8	9	10
0	B	A	T	A	S		A	M	A	N		36	C	O	L	O	D		O	K	O	N
1	D	O	W	O	C		O	P	O	N		37	F	E	S	E	J		E	T	E	N
2	J	E	B	E	F		E	R	E	N		38	H	I	C	I	M		I	W	I	N
3	M	I	D	I	H		I	L	I	N		39	K	U	F	U	P		U	B	U	N
4	P	U	J	U	K		U	S	U	N		40	T	A	H	A	R		A	D	A	N
5	R	A	M	A	T		A	C	A	N		41	W	O	K	O	L		O	J	O	N
6	L	O	P	O	W		O	F	O	N		42	B	E	T	E	S		E	M	E	N
7	S	E	R	E	B		E	H	E	N		43	D	I	W	I	C		I	P	I	N
8	C	I	L	I	D		I	K	I	N		44	J	U	B	U	F		U	R	U	N
9	F	U	S	U	J		U	T	U	N		45	M	A	D	A	H		A	L	A	N
10	H	A	C	A	M		A	W	A	N		46	P	O	J	O	K		O	S	O	N
11	K	O	F	O	P		O	B	O	N		47	R	E	M	E	T		E	C	E	N
12	T	E	H	E	R		E	D	E	N		48	L	I	P	I	W		I	F	I	N
13	W	I	K	I	L		I	J	I	N		49	S	U	R	U	B		U	H	U	N
14	B	U	T	U	S		U	M	U	N		50	C	A	L	A	D		A	K	A	N
15	D	A	W	A	C		A	P	A	N		51	F	O	S	O	J		O	T	O	N
16	J	O	B	O	F		O	R	O	N		52	H	E	C	E	M		E	W	E	N
17	M	E	D	E	H		E	L	E	N		53	K	I	F	I	P		I	B	I	N
18	P	I	J	I	K		I	S	I	N		54	T	U	H	U	R		U	D	U	N
19	R	U	M	U	T		U	C	U	N		55	W	A	K	A	L		A	J	A	N
20	L	A	P	A	W		A	F	A	N		56	B	O	T	O	S		O	M	O	N
21	S	O	R	O	B		O	H	O	N		57	D	E	W	E	C		E	P	E	N
22	C	E	L	E	D		E	K	E	N		58	J	I	B	I	F		I	R	I	N
23	F	I	S	I	J		I	T	I	N		59	M	U	D	U	H		U	L	U	N
24	H	U	C	U	M		U	W	U	N		60	P	A	J	A	K		A	S	A	N
25	K	A	F	A	P		A	B	A	N		61	R	O	M	O	T		O	C	O	N
26	T	O	H	O	R		O	D	O	N		62	L	E	P	E	W		E	F	E	N
27	W	E	K	E	L		E	J	E	N		63	S	I	R	I	B		I	H	I	N
28	B	I	T	I	S		I	M	I	N		64	C	U	L	U	D		U	K	U	N
29	D	U	W	U	C		U	P	U	N		65	F	A	S	A	J		A	T	A	N
30	J	A	B	A	F		A	R	A	N		66	H	O	C	O	M		O	W	O	N
31	M	O	D	O	H		O	L	O	N		67	K	E	F	E	P		E	B	E	N
32	P	E	J	E	K		E	S	E	N		68	T	I	H	I	R		I	D	I	N
33	R	I	M	I	T		I	C	I	N		69	W	U	K	U	L		U	J	U	N
34	L	U	P	U	W		U	F	U	N		70	B	A	T	A	S		A	M	A	N
35	S	A	R	A	B		A	H	A	N												

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	S	E	R	A	N	G		M	U	S	U	H		K	I	T	A
1	C	I	L	O	N	G		P	A	C	A	K		T	U	W	O
2	F	U	S	E	N	G		R	O	F	O	T		W	A	B	E
3	H	A	C	I	N	G		L	E	H	E	W		B	O	D	I
4	K	O	F	U	N	G		S	I	K	I	B		D	E	J	U
5	T	E	H	A	N	G		C	U	T	U	D		J	I	M	A
6	W	I	K	O	N	G		F	A	W	A	J		M	U	P	O
7	B	U	T	E	N	G		H	O	B	O	M		P	A	R	E
8	D	A	W	I	N	G		K	E	D	E	P		R	O	L	I
9	J	O	B	U	N	G		T	I	J	I	R		L	E	S	U
10	M	E	D	A	N	G		W	U	M	U	L		S	I	C	A
11	P	I	J	O	N	G		B	A	P	A	S		C	U	F	O
12	R	U	M	E	N	G		D	O	R	O	C		F	A	H	E
13	L	A	P	I	N	G		J	E	L	E	F		H	O	K	I
14	S	O	R	U	N	G		M	I	S	I	H		K	E	T	U
15	C	E	L	A	N	G		P	U	C	U	K		T	I	W	A
16	F	I	S	O	N	G		R	A	F	A	T		W	U	B	O
17	H	U	C	E	N	G		L	O	H	O	W		B	A	D	E
18	K	A	F	I	N	G		S	E	K	E	B		D	O	J	I
19	T	O	H	U	N	G		C	I	T	I	D		J	E	M	U
20	W	E	K	A	N	G		F	U	W	U	J		M	I	P	A
21	B	I	T	O	N	G		H	A	B	A	M		P	U	R	O
22	D	U	W	E	N	G		K	O	D	O	P		R	A	L	E
23	J	A	B	I	N	G		T	E	J	E	R		L	O	S	I
24	M	O	D	U	N	G		W	I	M	I	L		S	E	C	U
25	P	E	J	A	N	G		B	U	P	U	S		C	I	F	A
26	R	I	M	O	N	G		D	A	R	A	C		F	U	H	O
27	L	U	P	E	N	G		J	O	L	O	F		H	A	K	E
28	S	A	R	I	N	G		M	E	S	E	H		K	O	T	I
29	C	O	L	U	N	G		P	I	C	I	K		T	E	W	U
30	F	E	S	A	N	G		R	U	F	U	T		W	I	B	A
31	H	I	C	O	N	G		L	A	H	A	W		B	U	D	O
32	K	U	F	E	N	G		S	O	K	O	B		D	A	J	E
33	T	A	H	I	N	G		C	E	T	E	D		J	O	M	I
34	W	O	K	U	N	G		F	I	W	I	J		M	E	P	U
35	B	E	T	A	N	G		H	U	B	U	M		P	I	R	A

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
36	D	I	W	O	N	G		K	A	D	A	P		R	U	L	O
37	J	U	B	E	N	G		T	O	J	O	R		L	A	S	E
38	M	A	D	I	N	G		W	E	M	E	L		S	O	C	I
39	P	O	J	U	N	G		B	I	P	I	S		C	E	F	U
40	R	E	M	A	N	G		D	U	R	U	C		F	I	H	A
41	L	I	P	O	N	G		J	A	L	A	F		H	U	K	O
42	S	U	R	E	N	G		M	O	S	O	H		K	A	T	E
43	C	A	L	I	N	G		P	E	C	E	K		T	O	W	I
44	F	O	S	U	N	G		R	I	F	I	T		W	E	B	U
45	H	E	C	A	N	G		L	U	H	U	W		B	I	D	A
46	K	I	F	O	N	G		S	A	K	A	B		D	U	J	O
47	T	U	H	E	N	G		C	O	T	O	D		J	A	M	E
48	W	A	K	I	N	G		F	E	W	E	J		M	O	P	I
49	B	O	T	U	N	G		H	I	B	I	M		P	E	R	U
50	D	E	W	A	N	G		K	U	D	U	P		R	I	L	A
51	J	I	B	O	N	G		T	A	J	A	R		L	U	S	O
52	M	U	D	E	N	G		W	O	M	O	L		S	A	C	E
53	P	A	J	I	N	G		B	E	P	E	S		C	O	F	I
54	R	O	M	U	N	G		D	I	R	I	C		F	E	H	U
55	L	E	P	A	N	G		J	U	L	U	F		H	I	K	A
56	S	I	R	O	N	G		M	A	S	A	H		K	U	T	O
57	C	U	L	E	N	G		P	O	C	O	K		T	A	W	E
58	F	A	S	I	N	G		R	E	F	E	T		W	O	B	I
59	H	O	C	U	N	G		L	I	H	I	W		B	E	D	U
60	K	E	F	A	N	G		S	U	K	U	B		D	I	J	A
61	T	I	H	O	N	G		C	A	T	A	D		J	U	M	O
62	W	U	K	E	N	G		F	O	W	O	J		M	A	P	E
63	B	A	T	I	N	G		H	E	B	E	M		P	O	R	I
64	D	O	W	U	N	G		K	I	D	I	P		R	E	L	U
65	J	E	B	A	N	G		T	U	J	U	R		L	I	S	A
66	M	I	D	O	N	G		W	A	M	A	L		S	U	C	O
67	P	U	J	E	N	G		B	O	P	O	S		C	A	F	E
68	R	A	M	I	N	G		D	E	R	E	C		F	O	H	I
69	L	O	P	U	N	G		J	I	L	I	F		H	E	K	U
70	S	E	R	A	N	G		M	U	S	U	H		K	I	T	A

0	1	2	3	4	5	6	7	8	9		0	1	2	3	4	5	6	7	8	9
0	T	A	N	A	M		B	O	M		36	L	O	N	O	K		C	E	K
1	W	O	N	O	P		D	E	P		37	S	E	N	E	T		F	I	T
2	B	E	N	E	R		J	I	R		38	C	I	N	I	W		H	U	W
3	D	I	N	I	L		M	U	L		39	F	U	N	U	B		K	A	B
4	J	U	N	U	S		P	A	S		40	H	A	N	A	D		T	O	D
5	M	A	N	A	C		R	O	C		41	K	O	N	O	J		W	E	J
6	P	O	N	O	F		L	E	F		42	T	E	N	E	M		B	I	M
7	R	E	N	E	H		S	I	H		43	W	I	N	I	P		D	U	P
8	L	I	N	I	K		C	U	K		44	B	U	N	U	R		J	A	R
9	S	U	N	U	T		F	A	T		45	D	A	N	A	L		M	O	L
10	C	A	N	A	W		H	O	W		46	J	O	N	O	S		P	E	S
11	F	O	N	O	B		K	E	B		47	M	E	N	E	C		R	I	C
12	H	E	N	E	D		T	I	D		48	P	I	N	I	F		L	U	F
13	K	I	N	I	J		W	U	J		49	R	U	N	U	H		S	A	H
14	T	U	N	U	M		B	A	M		50	L	A	N	A	K		C	O	K
15	W	A	N	A	P		D	O	P		51	S	O	N	O	T		F	E	T
16	B	O	N	O	R		J	E	R		52	C	E	N	E	W		H	I	W
17	D	E	N	E	L		M	I	L		53	F	I	N	I	B		K	U	B
18	J	I	N	I	S		P	U	S		54	H	U	N	U	D		T	A	D
19	M	U	N	U	C		R	A	C		55	K	A	N	A	J		W	O	J
20	P	A	N	A	F		L	O	F		56	T	O	N	O	M		B	E	M
21	R	O	N	O	H		S	E	H		57	W	E	N	E	P		D	I	P
22	L	E	N	E	K		C	I	K		58	B	I	N	I	R		J	U	R
23	S	I	N	I	T		F	U	T		59	D	U	N	U	L		M	A	L
24	C	U	N	U	W		H	A	W		60	J	A	N	A	S		P	O	S
25	F	A	N	A	B		K	O	B		61	M	O	N	O	C		R	E	C
26	H	O	N	O	D		T	E	D		62	P	E	N	E	F		L	I	F
27	K	E	N	E	J		W	I	J		63	R	I	N	I	H		S	U	H
28	T	I	N	I	M		B	U	M		64	L	U	N	U	K		C	A	K
29	W	U	N	U	P		D	A	P		65	S	A	N	A	T		F	O	T
30	B	A	N	A	R		J	O	R		66	C	O	N	O	W		H	E	W
31	D	O	N	O	L		M	E	L		67	F	E	N	E	B		K	I	B
32	J	E	N	E	S		P	I	S		68	H	I	N	I	D		T	U	D
33	M	I	N	I	C		R	U	C		69	K	U	N	U	J		W	A	J
34	P	U	N	U	F		L	A	F		70	T	A	N	A	M		B	O	M
35	R	A	N	A	H		S	O	H											

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	M	A	T	A		M	A	T	A		M	U	S	U	H
1	P	O	W	O		P	O	W	O		P	A	C	A	K
2	R	E	B	E		R	E	B	E		R	O	F	O	T
3	L	I	D	I		L	I	D	I		L	E	H	E	W
4	S	U	J	U		S	U	J	U		S	I	K	I	B
5	C	A	M	A		C	A	M	A		C	U	T	U	D
6	F	O	P	O		F	O	P	O		F	A	W	A	J
7	H	E	R	E		H	E	R	E		H	O	B	O	M
8	K	I	L	I		K	I	L	I		K	E	D	E	P
9	T	U	S	U		T	U	S	U		T	I	J	I	R
10	W	A	C	A		W	A	C	A		W	U	M	U	L
11	B	O	F	O		B	O	F	O		B	A	P	A	S
12	D	E	H	E		D	E	H	E		D	O	R	O	C
13	J	I	K	I		J	I	K	I		J	E	L	E	F
14	M	U	T	U		M	U	T	U		M	I	S	I	H
15	P	A	W	A		P	A	W	A		P	U	C	U	K
16	R	O	B	O		R	O	B	O		R	A	F	A	T
17	L	E	D	E		L	E	D	E		L	O	H	O	W
18	S	I	J	I		S	I	J	I		S	E	K	E	B
19	C	U	M	U		C	U	M	U		C	I	T	I	D
20	F	A	P	A		F	A	P	A		F	U	W	U	J
21	H	O	R	O		H	O	R	O		H	A	B	A	M
22	K	E	L	E		K	E	L	E		K	O	D	O	P
23	T	I	S	I		T	I	S	I		T	E	J	E	R
24	W	U	C	U		W	U	C	U		W	I	M	I	L
25	B	A	F	A		B	A	F	A		B	U	P	U	S
26	D	O	H	O		D	O	H	O		D	A	R	A	C
27	J	E	K	E		J	E	K	E		J	O	L	O	F
28	M	I	T	I		M	I	T	I		M	E	S	E	H
29	P	U	W	U		P	U	W	U		P	I	C	I	K
30	R	A	B	A		R	A	B	A		R	U	F	U	T
31	L	O	D	O		L	O	D	O		L	A	H	A	W
32	S	E	J	E		S	E	J	E		S	O	K	O	B
33	C	I	M	I		C	I	M	I		C	E	T	E	D
34	F	U	P	U		F	U	P	U		F	I	W	I	J
35	H	A	R	A		H	A	R	A		H	U	B	U	M

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
36	K	O	L	O		K	O	L	O		K	A	D	A	P
37	T	E	S	E		T	E	S	E		T	O	J	O	R
38	W	I	C	I		W	I	C	I		W	E	M	E	L
39	B	U	F	U		B	U	F	U		B	I	P	I	S
40	D	A	H	A		D	A	H	A		D	U	R	U	C
41	J	O	K	O		J	O	K	O		J	A	L	A	F
42	M	E	T	E		M	E	T	E		M	O	S	O	H
43	P	I	W	I		P	I	W	I		P	E	C	E	K
44	R	U	B	U		R	U	B	U		R	I	F	I	T
45	L	A	D	A		L	A	D	A		L	U	H	U	W
46	S	O	J	O		S	O	J	O		S	A	K	A	B
47	C	E	M	E		C	E	M	E		C	O	T	O	D
48	F	I	P	I		F	I	P	I		F	E	W	E	J
49	H	U	R	U		H	U	R	U		H	I	B	I	M
50	K	A	L	A		K	A	L	A		K	U	D	U	P
51	T	O	S	O		T	O	S	O		T	A	J	A	R
52	W	E	C	E		W	E	C	E		W	O	M	O	L
53	B	I	F	I		B	I	F	I		B	E	P	E	S
54	D	U	H	U		D	U	H	U		D	I	R	I	C
55	J	A	K	A		J	A	K	A		J	U	L	U	F
56	M	O	T	O		M	O	T	O		M	A	S	A	H
57	P	E	W	E		P	E	W	E		P	O	C	O	K
58	R	I	B	I		R	I	B	I		R	E	F	E	T
59	L	U	D	U		L	U	D	U		L	I	H	I	W
60	S	A	J	A		S	A	J	A		S	U	K	U	B
61	C	O	M	O		C	O	M	O		C	A	T	A	D
62	F	E	P	E		F	E	P	E		F	O	W	O	J
63	H	I	R	I		H	I	R	I		H	E	B	E	M
64	K	U	L	U		K	U	L	U		K	I	D	I	P
65	T	A	S	A		T	A	S	A		T	U	J	U	R
66	W	O	C	O		W	O	C	O		W	A	M	A	L
67	B	E	F	E		B	E	F	E		B	O	P	O	S
68	D	I	H	I		D	I	H	I		D	E	R	E	C
69	J	U	K	U		J	U	K	U		J	I	L	I	F
70	M	A	T	A		M	A	T	A		M	U	S	U	H

0	1	2	3	4	5	6	7	8	9	10
0	J	A	L	A	N		S	E	P	I
1	M	O	S	O	N		C	I	R	U
2	P	E	C	E	N		F	U	L	A
3	R	I	F	I	N		H	A	S	O
4	L	U	H	U	N		K	O	C	E
5	S	A	K	A	N		T	E	F	I
6	C	O	T	O	N		W	I	H	U
7	F	E	W	E	N		B	U	K	A
8	H	I	B	I	N		D	A	T	O
9	K	U	D	U	N		J	O	W	E
10	T	A	J	A	N		M	E	B	I
11	W	O	M	O	N		P	I	D	U
12	B	E	P	E	N		R	U	J	A
13	D	I	R	I	N		L	A	M	O
14	J	U	L	U	N		S	O	P	E
15	M	A	S	A	N		C	E	R	I
16	P	O	C	O	N		F	I	L	U
17	R	E	F	E	N		H	U	S	A
18	L	I	H	I	N		K	A	C	O
19	S	U	K	U	N		T	O	F	E
20	C	A	T	A	N		W	E	H	I
21	F	O	W	O	N		B	I	K	U
22	H	E	B	E	N		D	U	T	A
23	K	I	D	I	N		J	A	W	O
24	T	U	J	U	N		M	O	B	E
25	W	A	M	A	N		P	E	D	I
26	B	O	P	O	N		R	I	J	U
27	D	E	R	E	N		L	U	M	A
28	J	I	L	I	N		S	A	P	O
29	M	U	S	U	N		C	O	R	E
30	P	A	C	A	N		F	E	L	I
31	R	O	F	O	N		H	I	S	U
32	L	E	H	E	N		K	U	C	A
33	S	I	K	I	N		T	A	F	O
34	C	U	T	U	N		W	O	H	E
35	F	A	W	A	N		B	E	K	I

0	1	2	3	4	5	6	7	8	9	10
36	H	O	B	O	N		D	I	T	U
37	K	E	D	E	N		J	U	W	A
38	T	I	J	I	N		M	A	B	O
39	W	U	M	U	N		P	O	D	E
40	B	A	P	A	N		R	E	J	I
41	D	O	R	O	N		L	I	M	U
42	J	E	L	E	N		S	U	P	A
43	M	I	S	I	N		C	A	R	O
44	P	U	C	U	N		F	O	L	E
45	R	A	F	A	N		H	E	S	I
46	L	O	H	O	N		K	I	C	U
47	S	E	K	E	N		T	U	F	A
48	C	I	T	I	N		W	A	H	O
49	F	U	W	U	N		B	O	K	E
50	H	A	B	A	N		D	E	T	I
51	K	O	D	O	N		J	I	W	U
52	T	E	J	E	N		M	U	B	A
53	W	I	M	I	N		P	A	D	O
54	B	U	P	U	N		R	O	J	E
55	D	A	R	A	N		L	E	M	I
56	J	O	L	O	N		S	I	P	U
57	M	E	S	E	N		C	U	R	A
58	P	I	C	I	N		F	A	L	O
59	R	U	F	U	N		H	O	S	E
60	L	A	H	A	N		K	E	C	I
61	S	O	K	O	N		T	I	F	U
62	C	E	T	E	N		W	U	H	A
63	F	I	W	I	N		B	A	K	O
64	H	U	B	U	N		D	O	T	E
65	K	A	D	A	N		J	E	W	I
66	T	O	J	O	N		M	I	B	U
67	W	E	M	E	N		P	U	D	A
68	B	I	P	I	N		R	A	J	O
69	D	U	R	U	N		L	O	M	E
70	J	A	L	A	N		S	E	P	I

0	1	2	3	4	5	6	7	8		0	1	2	3	4	5	6	7	8
0	P	O	S		A	M	A	N		36	T	E	D		O	K	O	N
1	R	E	C		O	P	O	N		37	W	I	J		E	T	E	N
2	L	I	F		E	R	E	N		38	B	U	M		I	W	I	N
3	S	U	H		I	L	I	N		39	D	A	P		U	B	U	N
4	C	A	K		U	S	U	N		40	J	O	R		A	D	A	N
5	F	O	T		A	C	A	N		41	M	E	L		O	J	O	N
6	H	E	W		O	F	O	N		42	P	I	S		E	M	E	N
7	K	I	B		E	H	E	N		43	R	U	C		I	P	I	N
8	T	U	D		I	K	I	N		44	L	A	F		U	R	U	N
9	W	A	J		U	T	U	N		45	S	O	H		A	L	A	N
10	B	O	M		A	W	A	N		46	C	E	K		O	S	O	N
11	D	E	P		O	B	O	N		47	F	I	T		E	C	E	N
12	J	I	R		E	D	E	N		48	H	U	W		I	F	I	N
13	M	U	L		I	J	I	N		49	K	A	B		U	H	U	N
14	P	A	S		U	M	U	N		50	T	O	D		A	K	A	N
15	R	O	C		A	P	A	N		51	W	E	J		O	T	O	N
16	L	E	F		O	R	O	N		52	B	I	M		E	W	E	N
17	S	I	H		E	L	E	N		53	D	U	P		I	B	I	N
18	C	U	K		I	S	I	N		54	J	A	R		U	D	U	N
19	F	A	T		U	C	U	N		55	M	O	L		A	J	A	N
20	H	O	W		A	F	A	N		56	P	E	S		O	M	O	N
21	K	E	B		O	H	O	N		57	R	I	C		E	P	E	N
22	T	I	D		E	K	E	N		58	L	U	F		I	R	I	N
23	W	U	J		I	T	I	N		59	S	A	H		U	L	U	N
24	B	A	M		U	W	U	N		60	C	O	K		A	S	A	N
25	D	O	P		A	B	A	N		61	F	E	T		O	C	O	N
26	J	E	R		O	D	O	N		62	H	I	W		E	F	E	N
27	M	I	L		E	J	E	N		63	K	U	B		I	H	I	N
28	P	U	S		I	M	I	N		64	T	A	D		U	K	U	N
29	R	A	C		U	P	U	N		65	W	O	J		A	T	A	N
30	L	O	F		A	R	A	N		66	B	E	M		O	W	O	N
31	S	E	H		O	L	O	N		67	D	I	P		E	B	E	N
32	C	I	K		E	S	E	N		68	J	U	R		I	D	I	N
33	F	U	T		I	C	I	N		69	M	A	L		U	J	U	N
34	H	A	W		U	F	U	N		70	P	O	S		A	M	A	N
35	K	O	B		A	H	A	N										

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	J	A	G	A		B	A	T	A	S		K	O	T	A	36	H	O	G	O		C	O	L	O	D		R	E	L	O
1	M	O	G	O		D	O	W	O	C		T	E	W	O	37	K	E	G	E		F	E	S	E	J		L	I	S	E
2	P	E	G	E		J	E	B	E	F		W	I	B	E	38	T	I	G	I		H	I	C	I	M		S	U	C	I
3	R	I	G	I		M	I	D	I	H		B	U	D	I	39	W	U	G	U		K	U	F	U	P		C	A	F	U
4	L	U	G	U		P	U	J	U	K		D	A	J	U	40	B	A	G	A		T	A	H	A	R		F	O	H	A
5	S	A	G	A		R	A	M	A	T		J	O	M	A	41	D	O	G	O		W	O	K	O	L		H	E	K	O
6	C	O	G	O		L	O	P	O	W		M	E	P	O	42	J	E	G	E		B	E	T	E	S		K	I	T	E
7	F	E	G	E		S	E	R	E	B		P	I	R	E	43	M	I	G	I		D	I	W	I	C		T	U	W	I
8	H	I	G	I		C	I	L	I	D		R	U	L	I	44	P	U	G	U		J	U	B	U	F		W	A	B	U
9	K	U	G	U		F	U	S	U	J		L	A	S	U	45	R	A	G	A		M	A	D	A	H		B	O	D	A
10	T	A	G	A		H	A	C	A	M		S	O	C	A	46	L	O	G	O		P	O	J	O	K		D	E	J	O
11	W	O	G	O		K	O	F	O	P		C	E	F	O	47	S	E	G	E		R	E	M	E	T		J	I	M	E
12	B	E	G	E		T	E	H	E	R		F	I	H	E	48	C	I	G	I		L	I	P	I	W		M	U	P	I
13	D	I	G	I		W	I	K	I	L		H	U	K	I	49	F	U	G	U		S	U	R	U	B		P	A	R	U
14	J	U	G	U		B	U	T	U	S		K	A	T	U	50	H	A	G	A		C	A	L	A	D		R	O	L	A
15	M	A	G	A		D	A	W	A	C		T	O	W	A	51	K	O	G	O		F	O	S	O	J		L	E	S	O
16	P	O	G	O		J	O	B	O	F		W	E	B	O	52	T	E	G	E		H	E	C	E	M		S	I	C	E
17	R	E	G	E		M	E	D	E	H		B	I	D	E	53	W	I	G	I		K	I	F	I	P		C	U	F	I
18	L	I	G	I		P	I	J	I	K		D	U	J	I	54	B	U	G	U		T	U	H	U	R		F	A	H	U
19	S	U	G	U		R	U	M	U	T		J	A	M	U	55	D	A	G	A		W	A	K	A	L		H	O	K	A
20	C	A	G	A		L	A	P	A	W		M	O	P	A	56	J	O	G	O		B	O	T	O	S		K	E	T	O
21	F	O	G	O		S	O	R	O	B		P	E	R	O	57	M	E	G	E		D	E	W	E	C		T	I	W	E
22	H	E	G	E		C	E	L	E	D		R	I	L	E	58	P	I	G	I		J	I	B	I	F		W	U	B	I
23	K	I	G	I		F	I	S	I	J		L	U	S	I	59	R	U	G	U		M	U	D	U	H		B	A	D	U
24	T	U	G	U		H	U	C	U	M		S	A	C	U	60	L	A	G	A		P	A	J	A	K		D	O	J	A
25	W	A	G	A		K	A	F	A	P		C	O	F	A	61	S	O	G	O		R	O	M	O	T		J	E	M	O
26	B	O	G	O		T	O	H	O	R		F	E	H	O	62	C	E	G	E		L	E	P	E	W		M	I	P	E
27	D	E	G	E		W	E	K	E	L		H	I	K	E	63	F	I	G	I		S	I	R	I	B		P	U	R	I
28	J	I	G	I		B	I	T	I	S		K	U	T	I	64	H	U	G	U		C	U	L	U	D		R	A	L	U
29	M	U	G	U		D	U	W	U	C		T	A	W	U	65	K	A	G	A		F	A	S	A	J		L	O	S	A
30	P	A	G	A		J	A	B	A	F		W	O	B	A	66	T	O	G	O		H	O	C	O	M		S	E	C	O
31	R	O	G	O		M	O	D	O	H		B	E	D	O	67	W	E	G	E		K	E	F	E	P		C	I	F	E
32	L	E	G	E		P	E	J	E	K		D	I	J	E	68	B	I	G	I		T	I	H	I	R		F	U	H	I
33	S	I	G	I		R	I	M	I	T		J	U	M	I	69	D	U	G	U		W	U	K	U	L		H	A	K	U
34	C	U	G	U		L	U	P	U	W		M	A	P	U	70	J	A	G	A		B	A	T	A	S		K	O	T	A
35	F	A	G	A		S	A	R	A	B		P	O	R	A																

0	1	2	3	4	5	6	7	8	9	10	11	12
0	M	U	S	U	H		M	E	N	A	N	G
1	P	A	C	A	K		P	I	N	O	N	G
2	R	O	F	O	T		R	U	N	E	N	G
3	L	E	H	E	W		L	A	N	I	N	G
4	S	I	K	I	B		S	O	N	U	N	G
5	C	U	T	U	D		C	E	N	A	N	G
6	F	A	W	A	J		F	I	N	O	N	G
7	H	O	B	O	M		H	U	N	E	N	G
8	K	E	D	E	P		K	A	N	I	N	G
9	T	I	J	I	R		T	O	N	U	N	G
10	W	U	M	U	L		W	E	N	A	N	G
11	B	A	P	A	S		B	I	N	O	N	G
12	D	O	R	O	C		D	U	N	E	N	G
13	J	E	L	E	F		J	A	N	I	N	G
14	M	I	S	I	H		M	O	N	U	N	G
15	P	U	C	U	K		P	E	N	A	N	G
16	R	A	F	A	T		R	I	N	O	N	G
17	L	O	H	O	W		L	U	N	E	N	G
18	S	E	K	E	B		S	A	N	I	N	G
19	C	I	T	I	D		C	O	N	U	N	G
20	F	U	W	U	J		F	E	N	A	N	G
21	H	A	B	A	M		H	I	N	O	N	G
22	K	O	D	O	P		K	U	N	E	N	G
23	T	E	J	E	R		T	A	N	I	N	G
24	W	I	M	I	L		W	O	N	U	N	G
25	B	U	P	U	S		B	E	N	A	N	G
26	D	A	R	A	C		D	I	N	O	N	G
27	J	O	L	O	F		J	U	N	E	N	G
28	M	E	S	E	H		M	A	N	I	N	G
29	P	I	C	I	K		P	O	N	U	N	G
30	R	U	F	U	T		R	E	N	A	N	G
31	L	A	H	A	W		L	I	N	O	N	G
32	S	O	K	O	B		S	U	N	E	N	G
33	C	E	T	E	D		C	A	N	I	N	G
34	F	I	W	I	J		F	O	N	U	N	G
35	H	U	B	U	M		H	E	N	A	N	G

0	1	2	3	4	5	6	7	8	9	10	11	12
36	K	A	D	A	P		K	I	N	O	N	G
37	T	O	J	O	R		T	U	N	E	N	G
38	W	E	M	E	L		W	A	N	I	N	G
39	B	I	P	I	S		B	O	N	U	N	G
40	D	U	R	U	C		D	E	N	A	N	G
41	J	A	L	A	F		J	I	N	O	N	G
42	M	O	S	O	H		M	U	N	E	N	G
43	P	E	C	E	K		P	A	N	I	N	G
44	R	I	F	I	T		R	O	N	U	N	G
45	L	U	H	U	W		L	E	N	A	N	G
46	S	A	K	A	B		S	I	N	O	N	G
47	C	O	T	O	D		C	U	N	E	N	G
48	F	E	W	E	J		F	A	N	I	N	G
49	H	I	B	I	M		H	O	N	U	N	G
50	K	U	D	U	P		K	E	N	A	N	G
51	T	A	J	A	R		T	I	N	O	N	G
52	W	O	M	O	L		W	U	N	E	N	G
53	B	E	P	E	S		B	A	N	I	N	G
54	D	I	R	I	C		D	O	N	U	N	G
55	J	U	L	U	F		J	E	N	A	N	G
56	M	A	S	A	H		M	I	N	O	N	G
57	P	O	C	O	K		P	U	N	E	N	G
58	R	E	F	E	T		R	A	N	I	N	G
59	L	I	H	I	W		L	O	N	U	N	G
60	S	U	K	U	B		S	E	N	A	N	G
61	C	A	T	A	D		C	I	N	O	N	G
62	F	O	W	O	J		F	U	N	E	N	G
63	H	E	B	E	M		H	A	N	I	N	G
64	K	I	D	I	P		K	O	N	U	N	G
65	T	U	J	U	R		T	E	N	A	N	G
66	W	A	M	A	L		W	I	N	O	N	G
67	B	O	P	O	S		B	U	N	E	N	G
68	D	E	R	E	C		D	A	N	I	N	G
69	J	I	L	I	F		J	O	N	U	N	G
70	M	U	S	U	H		M	E	N	A	N	G

0	1	2	3	4	5	6	7	8	9	10
0	M	I	S	I		G	A	G	A	L
1	P	U	C	U		G	O	G	O	S
2	R	A	F	A		G	E	G	E	C
3	L	O	H	O		G	I	G	I	F
4	S	E	K	E		G	U	G	U	H
5	C	I	T	I		G	A	G	A	K
6	F	U	W	U		G	O	G	O	T
7	H	A	B	A		G	E	G	E	W
8	K	O	D	O		G	I	G	I	B
9	T	E	J	E		G	U	G	U	D
10	W	I	M	I		G	A	G	A	J
11	B	U	P	U		G	O	G	O	M
12	D	A	R	A		G	E	G	E	P
13	J	O	L	O		G	I	G	I	R
14	M	E	S	E		G	U	G	U	L
15	P	I	C	I		G	A	G	A	S
16	R	U	F	U		G	O	G	O	C
17	L	A	H	A		G	E	G	E	F
18	S	O	K	O		G	I	G	I	H
19	C	E	T	E		G	U	G	U	K
20	F	I	W	I		G	A	G	A	T
21	H	U	B	U		G	O	G	O	W
22	K	A	D	A		G	E	G	E	B
23	T	O	J	O		G	I	G	I	D
24	W	E	M	E		G	U	G	U	J
25	B	I	P	I		G	A	G	A	M
26	D	U	R	U		G	O	G	O	P
27	J	A	L	A		G	E	G	E	R
28	M	O	S	O		G	I	G	I	L
29	P	E	C	E		G	U	G	U	S
30	R	I	F	I		G	A	G	A	C
31	L	U	H	U		G	O	G	O	F
32	S	A	K	A		G	E	G	E	H
33	C	O	T	O		G	I	G	I	K
34	F	E	W	E		G	U	G	U	T
35	H	I	B	I		G	A	G	A	W

0	1	2	3	4	5	6	7	8	9	10
36	K	U	D	U		G	O	G	O	B
37	T	A	J	A		G	E	G	E	D
38	W	O	M	O		G	I	G	I	J
39	B	E	P	E		G	U	G	U	M
40	D	I	R	I		G	A	G	A	P
41	J	U	L	U		G	O	G	O	R
42	M	A	S	A		G	E	G	E	L
43	P	O	C	O		G	I	G	I	S
44	R	E	F	E		G	U	G	U	C
45	L	I	H	I		G	A	G	A	F
46	S	U	K	U		G	O	G	O	H
47	C	A	T	A		G	E	G	E	K
48	F	O	W	O		G	I	G	I	T
49	H	E	B	E		G	U	G	U	W
50	K	I	D	I		G	A	G	A	B
51	T	U	J	U		G	O	G	O	D
52	W	A	M	A		G	E	G	E	J
53	B	O	P	O		G	I	G	I	M
54	D	E	R	E		G	U	G	U	P
55	J	I	L	I		G	A	G	A	R
56	M	U	S	U		G	O	G	O	L
57	P	A	C	A		G	E	G	E	S
58	R	O	F	O		G	I	G	I	C
59	L	E	H	E		G	U	G	U	F
60	S	I	K	I		G	A	G	A	H
61	C	U	T	U		G	O	G	O	K
62	F	A	W	A		G	E	G	E	T
63	H	O	B	O		G	I	G	I	W
64	K	E	D	E		G	U	G	U	B
65	T	I	J	I		G	A	G	A	D
66	W	U	M	U		G	O	G	O	J
67	B	A	P	A		G	E	G	E	M
68	D	O	R	O		G	I	G	I	P
69	J	E	L	E		G	U	G	U	R
70	M	I	S	I		G	A	G	A	L

RIWAYAT HIDUP

Alfiatus Sholehah lahir di Bondowoso pada tanggal 13 Juni 1998 dan memiliki nama panggilan Vivi. Tempat tingalnya beralamat di Desa Wringin RT 03/01 Kecamatan Wringin, Kabupaten Bondowoso. Merupakan anak kedua dari 2 bersaudara.

Pendidikan yang pernah ditempuh yaitu TK Pertiwi Tunas Harapan, kemudian dilanjutkan di Sekolah Dasar Negeri 1 Wringin dan lulus pada tahun 2011. Setelahnya melanjutkan pendidikan di SMP Negeri 2 Bondowoso sampai tahun 2014 lalu setelahnua melanjutkan sekolah di SMA Nurul Jadid Paiton – Probolinggo.

Pada tahun 2017 melanjutkan pendidikan strata 1 di Jurusan Matematika, Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Selama kuliah aktif di beberapa kegiatan organisasi intra dan ekstra seperti Himpunan Mahasiswa Jurusan, Dewan Eksekutif Mahasiswa Fakultas dan Universitas, Pergerakan Mahasiswa Islam Indonesia dan beberapa komunitas.

KEMENTRIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp./Fax.(0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Alfiatus Sholehah
NIM : 17610082
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Modifikasi *Caesar Cipher* untuk Menghasilkan *Readable Ciphertext*
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Dr. H. Imam Sujarwo, M.Pd

No	Tanggal	Hal	Tanda Tangan
1	14 Oktober 2021	Konfirmasi Bimbingan Proposal Skripsi	1
2	18 Oktober 2021	Konfirmasi Bimbingan Proposal Skripsi	2
3	18 November 2021	Bimbingan Bab I, II, III	3
4	22 November 2022	Bimbingan Kajian Agama	4
5	28 November 2022	Acc Pendaftaran Seminar Proposal	5
6	31 Maret 2022	Bimbingan Revisi Seminar Proposal	6
7	1 Maret 2022	Bimbingan Revisi Seminar Proposal	7
8	7 April 2022	Revisi Penulisan	8
9	30 Mei 2022	Bimbingan Revisi dan Acc Seminar Hasil	9
10	31 Mei 2022	Bimbingan Revisi dan Acc Seminar Hasil	10

Malang, 23 Juni 2022
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP.19741129 200012 2 005