BAB II
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Penelitian tentang perancangan aplikasi keamanan pesan teks dengan algoritma kriptografi *vigenere cipher* pernah dilakukan dan memuat teori-teori dari penelitian sejenis. Di bawah ini adalah kutipan dan acuan dari beberapa penelitian antara lain :

Pada penelitiannya yang berjudul "Implementasi Enkripsi Data Dengan Algoritma *Vigenere Cipher*" menjelaskan tentang Implementasi program enkripsi data dengan algoritma *vigenere cipher* dapat meningkatkan tingkat keamanan pendataan penjualan, pada data harga dan dapat meningkatkan keakuratan informasi, khususnya pada perhitungan harga jual (Arjana, 2012)

Pada penelitiannya yang berjudul "Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher* " menjelaskan bahwa cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Algoritma *vigenere cipher* merupakan salah satu metode kriptografi untuk penyandian teks. Penelitian ini bertujuan untuk membuat suatu aplikasi kriptografi yang dapat menyandikan teks dan mengirimkan teks yang terenkripsi melalui jaringan berdasarkan algoritma *vigenere cipher*. Aplikasi ini melakukan kriptografi pada teks berupa huruf, angka dan simbol. Kunci yang digunakan berupa *alfanumerik* yang merupakan gabungan huruf, angka dan simbol. Hasil dari penelitian ini adalah berupa aplikasi yang dapat melakukan pengiriman pesan teks yang telah terenkripsi melalui jaringan LAN (*Local Area Network*) sehingga kerahasiaan dari pesan tersebut dapat terjaga keamanannya (Yulianingsih, 2014).

Pada penelitiannya yang berjudul "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher" menjelaskan bahwa aplikasi kriptografi ini memungkinkan untuk melakukan enkripsi dan dekripsi pesan berbasis teks agar kerahasiaan data aslinya tetap terjaga dengan cara

menyembunyikan pesan penting yang bisa dibaca menjadi tidak bisa dibaca (Efrandi, 2014).

Pada penelitiannya yang berjudul "*Implementasi Algotitma Affine Cipher dan Vigenere Cipher Untuk Keamanan Login*" tujuan dari penelitian ini adalah untuk merancang keamanan *login* pada sistem inventori TB Mita menggunakan *enkripsi Affine Cipher* dan *Vigenere Cipher*, membuat *enkripsi password login* pada sitem inventori TB Mita menjadi lebih aman digunakan serta merancang enkripsi *password login* agar dapat diterapkan pada sitem inventori TB Mita menggunakan PHP (Religia, 2015).

Pada penelitiannya yang berjudul "Pengembangan Algoritma *Vigenere Cipher* Menggunakan Pergeseran Kunci Berbasis Biner" menjelaskan bahwa dalam pengimplementasian algoritma kriptografi *Vigenere Cipher* dapat dianggap tidak aman setelah disusunya metode kasiski yang dapat memecahkan cipherteks. Pada kesempatan ini penulis mengembangkan algoritma *Vigenere Cipher* dengan menerapkan kunci bergeser dan penerapan fungsi kriptografi modern yaitu dengan penerapan fungsi operasi *XOR* dan *bit shifting* dalam pembentukan plainteks dan kunci baru (Ardiansyah, 2014).

2.2 Landasan Teori

2.2.1 Pesan

Pesan adalah setiap pemberitahuan, kata, atau komunikasi baik lisan maupun tertulis, yang dikirimkan dari satu orang ke orang lain. Pesan menjadi inti dari setiap proses komunikasi yang terjalin. Dan dalam kamus besar bahasa indonesia pesan itu berarti perintah, nasihat, permintaan, amanat yg disampaikan lewat orang lain. Agar pesan dapat diterima dari pengguna satu ke pengguna lain, proses pengiriman pesan memerlukan sebuah media perantara agar pesan yang dikirimkan oleh sumber (*source*) dapat diterima dengan baik oleh penerima (*receiver*). Dalam proses pengiriman tersebut, pesan harus dikemas sebaik

mungkin untuk mengatasi gangguan yang muncul dalam transmisi pesan, agar tidak mengakibatkan perbedaan makna yang diterima oleh penerima (*receiver*). Secara umum, jenis pesan terbagi menjadi dua, yakni pesan *verbal* dan *non-verbal*. Pesan verbal adalah jenis pesan yang penyampaiannya menggunakan kata-kata, dan dapat dipahami isinya oleh penerima berdasarkan apa yang didengarnya. Sedangkan, pesan non-verbal adalah jenis pesan yang penyampaiannya tidak menggunakan kata-kata secara langsung, dan dapat dipahami isinya oleh penerima berdasarkan gerak-gerik, tingkah laku, mimik wajah, atau ekspresi muka pengirim pesan (Winanto, 2013)

2.2.2 Teks

Teks adalah wacana (berarti lisan) yang difiksasikan dalam bentuk tulisan. Dengan demikian jelas bahwa teks adalah fiksasi atau pelembagaan sebuah peristiwa wacana lisan dalam bentuk tulisan.

Salah satu definisi teks yang paling dikenal luas adalah pandangan *de Beaugrande* dan *Dressler* yang mengatakan bahwa teks adalah sebuah peristiwa komunikatif yang harus memenuhi beberapa syarat, yakni tujuh kriteria teks yang akan dikaji pada pembahasan selanjutnya.

Menurut definisi ini, tanda lalu lintas, artikel di surat kabar, argument, dan novel semuanya merupakan teks yang berhubungan dengan kaidah genre-genre atau tipe teks tertentu semua genre yang disebutkan memiliki ciri-ciri linguistik tertentu, memenuhi fungsi tertentu dan terikat pada situasi-situasi pemroduksian dan penerimaan tertentu. Oleh sebab itu, terdapat kondisi-kondisi makna yang bersifat internal teks maupun eksternal teks yang akhirnya berhadapan dengan cara mendefinisikan dan menganalisis konteks ekstralinguistik.

Dalam teori bahasa, apa yang dinamakan teks tidak lebih dari himpunan huruf yang membentuk kata dan kalimat, yang dirangkai dengan sistem tanda yang yang disepakati oleh masyarakat, sehingga sebuah teks ketika dibaca bisa mengungkapkan makna yang dikandungnya.

2.2.3 Visual Studio .Net 2012

Visual Studio.NET 2012 merupakan salah satu produk pengembangan aplikasi yang diproduksi oleh Microsoft. Visual Studio.NET 2012 dapat digunakan untuk pengembangan aplikasi *Web ASP .NET, XML Web Service*, aplikasi dekstop dan juga aplikasi *mobile*. Dalam Visual Studio.NET 2012 terdapat beberapa *tool* yang dapat dipilih untuk pengembangan aplikasi. *Tool-tool* tersebut antara lain adalah Visual Basic, Visual C# dan Visual C++. *Tool-tool* pada Visual Studio.NET 2012 tersebut menggunakan IDE (*Integrated Development Environment*) yang sama sehingga dapat selain berbagi pakai fasilitas dalam pengembangan aplikasi.

Pada *Visual Basic.NET 2012* banyak sekali fasilitas *wizard* yang disediakan untuk memudahkan para pengembang aplikasi. Dengan fasilitas ini, pengembangan aplikasi dapat dilakukan dengan cepat. Ini memungkinkan para pemula untuk belajar lebih cepat dalam pengembangan aplikasi.

2.2.4 Pengertian Kriptografi

Kriptografi adalah ilmu untuk mempelajari penulisan secara rahasia dengan tujuan bahwa komunikasi dan data dapat dikodekan (*encode/encrypt*) dan dikodekan (*decode/decrypt*) kembali untuk mencegah pihak-pihak lain yang ingin mengetahui isinya. Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *kryptos* yang artinya tersembunyi. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi kebentuk tertentu yang sulit untuk dimengerti (Sadikin, 2012).

Proses yang dilakukan untuk mengubah *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *encipherment* sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut dekripsi (*decryption*) atau *decipherment*. Kriptografi memerlukan parameter untuk proses konversi yang dikendalikan oleh sebuah kunci atau beberapa kunci. Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman

pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut berdasarkan algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berhak atas data, informasi dan dokumen tersebut. Di dalam kriptografi akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang harus diketahui yaitu:

a. Pesan, *plaintext* dan *ciphertext*

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *ciphertext* atau kriptogram. *Ciphertext* harus dapat ditransformasikan kembali menjadi *plaintext* semula agar dapat diterima dan bisa dibaca.

b. Pengirim dan penerima

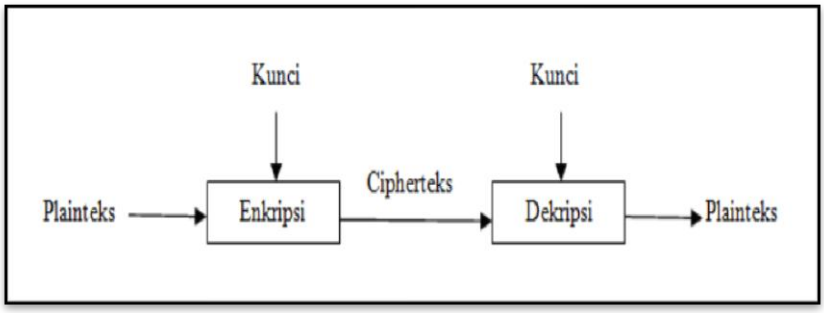
   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Pengirim tentu menginginkan pesan dapat dikirm secara aman, yaitu pengirim yakin bahwa pihak lain tidak dapat membaca isi pesan yang dikirim. Solusinya adalah dengan cara menyandikan pesan menjadi *ciphertext*.

c. Enkripsi dan dekripsi

   Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*) atau *deciphering*.

d. Cipher dan kunci

Algoritma kriptografi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*.



Gambar 2. 1 Skema Enkripsi dan Dekripsi

e. Sistem kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem Kriptografi. Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua *plaintext* dan *ciphertext* yang mungkin dan kunci. Di dalam kriptografi, *cipher* hanyalah salah satu komponen saja.

f. Penyadap

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan *ciphertext*. Nama lain penyadap : *enemy, adversary, intruder, interceptor, bad guy*.

g. Kriptanalisis dan kriptologi

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalisis (*cryptanalysis*) adalah

ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer (*cryptographer*) mentransformasikan *plaintext* menjadi *ciphertext* dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan *ciphertext* tersebut untuk menemukan *plaintext* atau kunci. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

2.2.5 Dasar Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Secrecy* (kerahasiaan), layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka maupun menghapus informasi yang telah disandi.
2. *Authentication,* berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Dimana inforamsi yang dikirimkan melalui kanal harus diautentifikasi keaslian, isi datanya, waktu pengiriman dan lain-lain.
3. Hak Akses terhadap suatu *file* atau fasilitas lain dalam sebuah sistem pemrosesan informasi masih dalam area lain dimana gagasan kriptografi telah diterapkan.

2.2.6 Tujuan Kriptografi

Kriptografi bertujuan untuk layanan keamanan yang memiliki beberapa aspek keamanan yang memiliki beberapa aspek keamanan, antara lain sebagai berikut :

1. *Confidelity* (kerahasiaan)

   layanan agar isi pesan yang dikirimkan tetaprahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima/pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma

matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

2. *Data integrity* (keutuhan data)
   layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
3. *Authentication* (keotentikan)
   layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
4. *Non-repudiation* (anti-penyangkalan)
   layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya)..

2.2.7 Serangan Kriptografi

Tujuan utama kriptografi adalah untuk menjaga agar *plaintext* tetap aman dari para penyadap yang mencoba untuk mendapatkan informasi tentang *plaintext*. Kriptografi diharapkan dapat pula menjamin integritas pesan. Kriptanalisis merupakan ilmu yang mempelajari serangan kriptografi. Serangan terhadap kriptografi dikelompokan menjadi beberapa cara.

a. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu :

   1. Serangan pasif (*passive attack*) pada jenis serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuanya adalah untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :

      a. *Wiretapping* : penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.

b. *Electromagnetic eavesdropping* : penyadap mencegat data yang ditrasnmisikan melalui saluran *wireless*, misalnya radio dan *microwave*.

c. *Acoustic eavesdropping* : menangkap gelombang suara yang dihasilkan oleh suara manusia.

2. Serangan aktif (*active attack*), pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya. Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian *ciphertext*, mengubah *ciphertext*, menyisipkan potongan *ciphertext* palsu, me-*replay* pesan lama, mengubah informasi yang tersimpan dan sebagainya.

b. Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, dikelompokan menjadi beberapa jenis.:

1. *Ciphertext-only attack*, ini adalah jenis serangan yang paling umum namun paling sulit, karena informasi yang tersedia hanyalah *ciphertext* saja.

2. *Known-plaintext attack*, ini adalah jenis serangan dimana kriptanalis memiliki pasangan *plaintext* dan *ciphertext* yang berkoresponden.

3. *Chosen-plaintext attack*, serangan jenis ini lebih hebat dari pada *known-plaintext attack*, karena kriptanalis dapat memilih *plaintext* yang dimilikinya untuk di*enkripsi*kan, yaitu *plaintext-plaintext* yang lebih banyak dan banyak yang mengarahkan penemuan kekunci tersebut.

4. *Chosen-ciphertext attack*, ini adalah jenis serangan dimana kriptanalis memilih *ciphertext* untuk diserang dan didekripsi*k*an dan memiliki *akses* ke *plaintext* hasil dekripsi.

c. Berdasarkan Teknik yang digunakan dalam menemukan kunci, serangan dibagi atas :

1. *Exhaustive attack,* atau *bruforce attack* adalah serangan untuk mengungkap *plaintext* menggunakan semua kemungkinan kunci.

2. *Analytical attack,* adalah serangan dengan menganalisis kelemahan algritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada.

2.2.8 Jenis Kriptografi

a. Kriptografi`Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang (*plaintext*). Kriptografi ini hanya melakukan pengacakan pada huruf A-Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern (Hartini & Primaini, 2013)

b. Kriptografi Modern

Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptogarfi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern :

a. Algoritma Simetris

Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara *real time*.

b. Algoritma Asimetris

Algoritma Asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi *deskripsi*. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (*Rivest, Shamir dan Adleman*).

2.2.9 Algoritma Vigenere Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553. Cara kerja dari *Vigenère cipher* ini mirip dengan *Caesar cipher*, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. *Vigenère cipher* adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjadmajemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti *Caesar cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama (Hallim, 2010).

Vigenère cipher yang menerapkan metode substitusi abjad-majemuk tidak memiliki permasalahan tersebut karena setiap huruf pada pesan yang dienkripsi dengan Vigenère cipher ini akan digeser dengan nilai yang berbeda tergantung dengan kunci yang diberikan. Kunci yang digunakan pada *Vigenère cipher* berbeda dengan yang digunakan pada *Caesar cipher*. Jika pada *Caesar cipher* kuncinya hanya satu nilai saja, maka pada *Vigenère cipher* kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan

memungkinkan setiap huruf *plainteks* untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang *plainteks*. Algoritma ini akan meminimalkan kemungkinan dipecahkannya *cipherteks* jika satu huruf plainteks diketahui. rumus dari enkripsi dan dekripsi dengan *vigenere chiper* adalah :

Enkripsi

$Ci \rightarrow (Pi + Ki) Mod\ 65$ ..... **(2.1)**

Keterangan :

Ci : Nilai ciphertext
Pi : Nilai Plaintext
Ki : Nilai Kunci
Mod 65 : Modulus 65 Karakter

Sebagai contoh kalimat “SAYASHENI” akan dilakukan proses enkripsi dengan menggunakan kunci “TUGAS” :

Pi = S A Y A S H E N I
Ki = T U G A S T U GA

Perhitungan :

(S + T) mod 65 = (83 + 84) mod 65 = 37+65= f
(A + U) mod 65 = (65 + 85) mod 65 = 20+65= U
(Y + G) mod 65 = (89 + 71) mod 65 = 30+65 = _
(A + A) mod 65 = (65+ 65) mod 65 = 0+65 = A
(S + S) mod 65 = (83+ 83) mod 65 = 36+65 = e
(H + T) mod 65 = (72 + 84) mod 65 = 26+65 = [
(E + U) mod 65 = (69 + 85) mod 65 = 24+65 = Y
(N + G) mod 65 = (78 + 71) mod 65 = 19+65 = T
(I + A) mod 65 = (73 + 65) mod 65 = 8+65= I
Jadi hasil dari enkripsi adalah : fU_Ae[YTI

Deskripsi

$$Pi \rightarrow (Ci - Ki) Mod\ 65 \quad \text{.....} \textbf{(2.2)}$$

Selanjutnya adalah proses dekripsi dari karakter ”fU_Ae[YTI” dengan menggunakan Kunci “TUGAS”.

(f - T) mod 65 = (102 - 84) mod 65 = (18+65) = S

(U - U) mod 65 = (85 - 85) mod 65 = (0+65) = A

(_ - G) mod 65 = (95 - 71) mod 65 = (24+65) = Y

(A - A) mod 65 = (65 - 65) mod 65 = (0+65) = A

(e - S) mod 65 = (101 - 83) mod 65 = (18+65) = S

([- T) mod 65 = (91 - 84) mod 65 = (7+65) = H

(Y - U) mod 65 = (89 - 85) mod 65 = (4+65) = E

(T - G) mod 65 = (84 - 71) mod 65 = (13+65) = N

(I - A) mod 65 = (73 - 65) mod 65 = (8+65) = I

Jadi hasil dari dekripsi adalah : SAYASHENI

Karakter pada setiap akan dikonversi menjadi sebuah nilai, misalnya A = 65, B = 66, sampai dengan karakter selanjutnya.