Aplikasi Pembelajaran Kriptografi Klasik dengan Visual Basic .NET

Erianto Ongko[1)], Justian[2)]
STMIK IBBI
Jl. Sei Deli No. 18 Medan, Telp 061-4567111 Fax: 061-4527548
e-mail: erianto_ongko@yahoo.co.id, juzzonly@hotmail.com

Abstrak

Kriptografi adalah teknik untuk menyandikan (enkripsi dan dekripsi) informasi yang akan dikirimkan. Enkripsi dilakukan ketika pengiriman informasi dan mengubah informasi asli melalui mekanisme tertentu, sedangkan dekripsi dilakukan pada saat informasi diterima dan diubah yang telah disandikan menjadi informasi asli. Aplikasi pembelajaran kriptografi klasik ini dirancang menggunakan bahasa pemrograman Visual Basic .NET 2012. Algoritma kriptografi yang digunakan dalam aplikasi terdiri dari Hill Cipher, Caesar Cipher, Substitusi, Transposisi, dan XOR. Berdasarkan hasil perancangan dan pengujian didapatkan bahwa aplikasi ini dapat membantu dosen untuk mengajarkan teknik kriptografi klasik kepada mahasiswa, sehingga mahasiswa lebih mudah untuk mempelajari tahap-tahap enkripsi dan dekripsi menggunakan teknik kriptografi klasik.

Kata kunci: *Kriptografi Klasik, Hill Cipher, Caesar Cipher, Substitusi, Transposisi*

Abstract

Cryptography is a technique to encode (encrypt and decrypt) information which will be sent. Encryption is done when information being sent and changed the original information using certain mechanism. Decryption is done when information being accepted and changed back from encoded information to the original information. Classic Cryptography Learning Application is designed using Visual Basic .NET 2012. Some methods included in this application such as Hill Cipher, Caesar Cipher, Substitution method, Transposition method and XOR. Input and output that supported for the encryption and decryption are text. This learning application can be used by lecturer to teach Classic Cryptography to students, so students can learn steps-by-steps of encryption and decryption easier than before.

Keywords*: Classic Cryptography, Hill Cipher, Caesar Cipher, Substitution, Transposition, XOR*

1. Pendahuluan

Keamanan data kini menjadi hal penting yang harus dipertahankan pada era digital. Banyak pihak tidak berwenang yang berusaha mencuri akses terhadap suatu data milik orang lain tanpa izin. Dalam mengirim data, terutama yang bersifat rahasia, data tersebut harus terlebih dahulu diamankan dengan memakai metode kriptografi sebelum dikirimkan. Hal ini dilakukan untuk mencegah orang yang tidak berhak dan tidak berkepentingan untuk mencuri, membuka ataupun mengganti isi dari data yang dikirim.[1]

Kini, metode kriptografi telah berkembang dan memiliki banyak jenisnya. Setiap metode ini memiliki cara yang berbeda dalam mengenkripsi data, serta memiliki kelebihan dan kekurangan tersendiri. Metode dalam kritografi klasik memberikan gambaran awal mengenai proses enkripsi dan dekripsi secara mendasar. Namun, pembelajaran kriptografi pada perkuliahan lebih mengarah kepada teoritis, karena kurangnya aplikasi yang bisa secara langsung mengajarkan kriptografi klasik. Proses belajar mengajar untuk kriptografi klasik hanya melalui penjelasan lisan dan tulisan tanpa ada perangkat lunak yang mendampingi pembelajaran topik tersebut.

Manfaat dari penelitian ini adalah untuk merancang suatu sarana atau aplikasi pembelajaran kriptografi klasik sehingga memudahkan staf pengajar/dosen untuk menjelaskan teknik-teknik kriptografi klasik kepada mahasiswa. Selain itu aplikasi yang dirancang dapat memperkaya materi ajar dalam mata kuliah Kriptografi maupun Keamanan Komputer.

2. Metode Penelitian

Metodologi yang digunakan dalam perancangan aplikasi pembelajaran kriptografi klasik terdiri dari tahapan dan berbagai metode sebagai berikut:

1. Riset Pustaka, dilakukan riset yang mendalam tentang teori maupun algoritma bagaimana suatu metode kriptografi dilakukan. Riset dilakukan dengan mempelajari buku maupun jurnal yang membahas masalah yang sedang dibahas.
2. Analisa dan Perancangan. Setelah teori dan contoh aplikasi yang dibutuhkan telah memadai, maka langkah selanjutnya adalah melakukan analisis kebutuhan metode apa saja yang perlu dibahas. Kemudian berbagai metode yang akan digunakan diterjemahkan ke dalam diagram dia-

gram alir (flowchart) yang menjelaskan rincian proses dari program utama, serta subprogram yang berisi metode-metode kriptografi klasik. Pada langkah ini juga, penulis merancang algoritma dari setiap metode kriptografik klasik yang dimasukkan ke dalam program. Algoritma pada tiap subprogram berbeda dengan yang lain, karena penulis memasukkan metode kriptografi klasik yang beragam dan lebih dari satu.

3. Perancangan Antarmuka, dengan merancang tampilan dari program utama dan subprogram. Tampilan program utama berupa sebuah MDI Form dengan menu bar sebagai sarana navigasi di dalam aplikasi. Untuk tampilan subprogram, tampilan disesuaikan dengan kebutuhan dari tiap metode kriptografi klasik. Form subprogram terdiri dari control tombol dan textbox.
4. Implementasi, Dalam tahapan ini, penulis menuangkan rancangan sebelumnya ke dalam pemrograman. Bahasa pemrograman yang dipilih adalah Visual Basic .NET 2012. Penulis mengimplementasikan rancangan tampilan sebelumnya dan melakukan *coding* sesuai bahasa yang dipilih. Kegiatan yang dilakukan antara lain membuat tampilan form dari program utama dan subprogram, membuat *function* yang dibutuhkan serta perintah yang dibutuhkan pada setiap *control* bersangkutan.
5. Pengujian aplikasi. Tahap pengujian ini adalah tahap terakhir yang dilakukan penulis dalam merancang program ini. Pengujian dilakukan terhadap program yang telah selesai dibuat pada tahap sebelumnya. Pengujian ini perlu dilakukan untuk mengetahui kesalahan-kesalahan (error) yang terjadi ketika program dijalankan, sehingga penulis dapat melakukan revisi dan perbaikan terhadap program.

Caesar Cipher

Caesar Cipher ditemukan oleh Julius Caesar, merupakan salah satu teknik enkripsi tertua di dunia. Caesar Cipher mengelompokkan suatu rangkaian kata menjadi beberapa blok dengan panjang tertentu. Kemudian, susunan blok tersebut diulang beberapa kali, namun dengan urutan alfabet yang naik secara bertahap (increment). Jika kunci yang dipakai adalah 4 misalnya, maka proses susunan itu akan diulang hingga lima kali. Bila dirumuskan, dengan plaintext adalah P dan ciphertext adalah C, serta kunci adalah K, maka proses enkripsi Caesar Cipher sebagai berikut:

$$C = E(P) = (P + K) \bmod 26 \quad \text{.....1)}$$

Metode Substitusi

Metode Substitusi merupakan perkembangan lebih lanjut dari Caesar Cipher. Pada metode substitusi, pengirim pesan bisa menentukan kunci berupa sebuah kata dengan syarat tidak ada karakter berulang dalam kata itu. Bila ada, maka karakter yang muncul pertama yang akan disimpan, dan karakter berulang akan ditiadakan.

Plaintext dalam metode substitusi akan dienkripsi berdasarkan kunci yang dimasukkan. Kunci akan menjadi peubah dalam enkripsi, menggantikan setiap karakter dengan barisan abjad ya ng telah disusun sesuai kunci. Proses ini hampir sama dengan Caesar Cipher, namun prosesnya terikat pada kunci yang dimasukkan sebelumnya itu.

Metode Transposisi

Metode Transposisi memakai permutasi dari setiap karakter plaintext. Metode ini berbeda dari metode sebelumnya yang hanya mengganti karakter dari plaintext menjadi ciphertext. Metode transposisi menukar letak dari setiap karakter dengan aturan dari kunci permutasi, sehingga plaintext menjadi tidak terbaca.

Hill Cipher

Hill Cipher merupakan salah satu proses kriptografi yang termasuk dalam kategori polialfabetik. Polialfabetik berarti setiap karakter alfabet mampu dipetakan ke lebih dari satu macam karakter alfabet. Metode Hill Cipher ditemukan oleh Lester Hill pada tahun 1929. Hill Cipher berbasiskan pada konsep Aljabar Linier. Dalam proses enkripsi Hill Cipher, aljabar linier digunakan dengan menggunakan matriks modulus 26.

Hill Cipher mengubah plaintext menjadi sebuah kombinasi matriks kemudian mengenkripsinya menggunakan kunci yang juga berupa matriks. Pemakaian Hill Cipher mengecilkan kemungkinan adanya frekuensi satu huruf. Bahkan, dengan jumlah elemen matriks yang lebih besar, misalnya 3x3 ataupun 4x4, maka seorang penyadap tidak akan mampu memakai Frequency Analysis untuk mengecek plaintext yang dienkripsi.

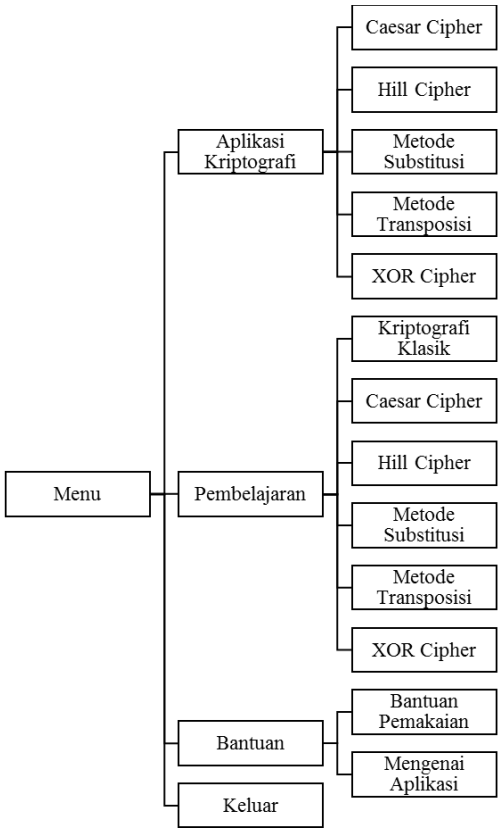
XOR Cipher

Metode XOR memproses plaintext menjadi ciphertext menggunakan operasi gerbang Exclusive OR (XOR). Untuk mengenkripsi, pengirim hanya perlu mensilangkan karakter plaintext dengan kunci dimana keduanya telah diubah dari karakter huruf menjadi ASCII. Logika XOR menyatakan bahwa salah satu sisi bernilai benar saja, maka hasilnya bernilai benar. Namun jika keduanya bernilai salah, ataupun bernilai benar, maka hasilnya adalah salah.

3. Hasil dan Pembahasan

Analisa dan Perancangan

Adapun perancangan *state transition diagram* untuk aplikasi pembelajaran kriptografi klasik dapat digambarkan sebagai berikut:



Gambar 1. State Transition Diagram

Selanjutnya, penulis merancang cara kerja aplikasi dari menu utama hingga aplikasi-aplikasi terpisah yang berisi metode-metode kriptografi klasik yang berbeda-beda. Algoritma ini yang akan dipakai sebagai dasar perancangan tampilan dan sistem kerja aplikasi.

Algoritma Metode Caesar Cipher

Pada metode Caesar Cipher, urutan algoritma pemakaian, proses enkripsi serta dekripsi adalah sebagai berikut:

1. Pengguna memasukkan teks yang akan dienkripsi ke dalam plaintext.
2. Pengguna memilih kunci yang ada, antara 1 hingga 25, dilanjutkan menekan tombol Enkripsi.
3. Proses enkripsi dimulai dengan menggeser abjad sejumlah kunci, sehingga setiap karakter yang ada pada plaintext akan digeser sesuai kunci. Caranya, nilai alfabet karakter akan ditambah dengan nilai kunci. Bila hasil jumlah melebihi Z (atau 26), maka nilai akan dikembalikan ke nilai A (atau 1). Karakter yang telah digeser akan disusun kembali menjadi utuh dan menjadi hasil enkripsi. Hasil enkripsi akan ditampilkan pada kotak Encrypted.
4. Untuk dekripsi, Pengguna hanya perlu menekan tombol dekripsi. Pada saat proses dekripsi, Pengguna tidak dapat mengganti kunci karena proses dekripsi membutuhkan kunci yang

sama seperti digunakan pada proses enkripsi. Proses dekripsi akan mengembalikan karakter yang digeser sebelumnya dengan cara mengurangi nilai alfabet karakter yang telah dienkripsi dengan kunci. Hasil pengurangan yang dibawah nol akan dikembalikan ke abjad Z (atau 26) dan dibawahnya (25, 24…). Hasil dekripsi akan ditampilkan pada kotak Decrypted.

5. Tahap proses enkripsi dan dekripsi dapat dilihat dengan menekan tombol Tampilkan Proses.

Algoritma Metode Hill Cipher

Pada metode Hill Cipher, urutan algoritma pemakaian, proses enkripsi dan dekripsi adalah sebagai berikut:

1. Pengguna memasukkan teks yang akan dienkripsi ke dalam plaintext.
2. Pengguna memasukkan kunci berupa matriks. Matriks yang dimasukkan harus memiliki determinan modulus 26 berupa 1. Angka elemen matriks yang dimasukkan antara 1 hingga 10 untuk setiap elemen. Pengguna bisa memilih secara acak elemen matriks menggunakan tombol Random. Aplikasi akan menghasilkan angka acak pada elemen matriks yang telah memiliki nilai determinan modulus 26 berupa
3. Dengan adanya matriks yang memiliki determinan modulus 26 bukan nol, proses enkrip si dan dekripsi dapat dilakukan. Proses enkripsi dimulai ketika Pengguna menekan tombol Enkripsi. Proses enkripsi bisa dilakukan hanya bila matriks telah diisi dengan elemen yang menghasilkan determinan modulus 26 = 1.
    a. Pertama, plaintext akan dicek terlebih dahulu apakah jumlah karakternya habis dibagi empat. Bila tidak, maka akan disisipkan karakter tambahan secara otomatis oleh aplikasi hingga jumlah karakter bisa habis dibagi angka 4. Hal ini dikarenakan matriks yang dipakai adalah matriks 2x2 dengan jumlah elemen adalah 4.
    b. Kemudian, setiap karakter akan diubah menjadi angka berdasarkan urutan pada alfabet dikurangi 1. Misalnya J menjadi 9, B menjadi 1 dan seterusnya. Angka hasil perubahan plaintext akan dipecah berdasarkan kelipatan 4, kemudian dibagi menjadi matriks. Artinya, karakter ke-1 hingga ke-4 ada pada matriks pertama, dan seterusnya.
    c. Masing-masing matriks akan dikalikan dengan matriks kunci, kemudian di-modulus 26 dan ditambah 1.
    d. Angka-angka elemen matriks dari hasil perkalian matriks diubah kembali menjadi huruf abjad sesuai urutan alfabet. Abjad-abjad ini disusun kembali dan ditampilkan pada kotak Encrypted.
4. Proses dekripsi dimulai ketika Pengguna menekan tombol dekripsi. Pada kondisi ini, Pengguna tidak bisa mengubah kunci matriks.
    a. Kunci matriks akan di-invers terlebih dahulu. Hasil invers menjadi kunci dekripsi.
    b. Hasil enkripsi dipecah kembali menjadi karakter dan diubah menjadi angka. Setiap angka kemudian disusun menjadi matriks 2x2.
    c. Matriks ini dikalikan dengan kunci dekripsi di atas. Hasil perkalian berupa angka dan diubah menjadi karakter.
    d. Bila terdapat karakter tambahan yang disisipkan sebelumnya, maka karakter tersebut akan ditampilkan kembali pada tempat semula. Hasil dekripsi akan ditampilkan pada kotak Decrypted.
5. Tahap proses enkripsi dan dekripsi dapat dilihat dengan menekan tombol Tampilkan Proses.

Algoritma Metode Substitusi

Pada metode substitusi, urutan algoritma pemakaian, proses enkripsi dan dekripsi adalah sebagai berikut:

1. Pengguna memasukkan teks yang akan dienkripsi ke dalam plaintext.
2. Pengguna memasukkan kunci berupa teks tanpa simbol, angka dan spasi. Bila kunci tersebut memiliki abjad yang sama, maka abjad yang muncul kedua kalinya tidak akan dimasukkan menjadi kunci. Misalnya bila kuncinya MAKAN maka kunci yang diambil hanya MAKN.
3. Kunci kemudian disusun menjadi tabel pemetaan alfabet. Abjad pertama pada kunci akan dipetakan dengan huruf A, abjad kedua pada huruf B dan seterusnya. Sisa abjad yang tidak ada pada kunci dipetakan pada abjad-abjad selanjutnya.
4. Proses enkripsi dilakukan pada setiap karakter plaintext. Karakter diubah menjadi abjad baru sesuai tabel pemetaan. Hasilnya ditampilkan pada kotak Encrypted. Proses dekripsi juga sama seperti proses enkripsi, dengan mengubah hasil enkripsi kembali menjadi plaintext dan ditampilkan pada kotak Decrypted.

Algoritma Metode Transposisi

Pada metode transposisi, urutan algoritma pemakaian, proses enkripsi dan dekripsi adalah sebagai berikut:

1. Pengguna memasukkan teks yang akan dienkripsi ke dalam plaintext.
2. Pengguna memasukkan kunci berupa 4 digit angka yang telah diacak. Angka tersebut adalah 1, 2, 3 dan 4, tetapi tidak bisa dimasukkan secara berurutan. Kunci juga bisa diacak secara otomatis dengan memakai tombol Random.
3. Proses enkripsi dimulai dengan menekan tombol Enkripsi.
   a. Pertama, plaintext akan dicek terlebih dahulu apakah jumlah karakternya habis dibagi empat. Bila tidak, maka akan disisipkan karakter tambahan secara otomatis oleh aplikasi hingga jumlah karakter bisa habis dibagi angka 4. Hal ini dikarenakan nantinya karakter plaintext akan dipecah ke dalam tabel yang memiliki jumlah kolom 4.
   b. Karakter plaintext dibagi ke dalam tabel secara horizontal, dan angka kunci dituliskan di atas tabel. c. Tabel kemudian disusun berdasarkan kolom secara berurutan (1, 2, 3, 4). Pembacaan hasil enkripsi juga melalui kolom per kolom. Hasilnya ditampilkan pada kotak Encrypted.
4. Proses dekripsi mirip dengan proses enkripsi. Hasil enkripsi sebelumnya disusun per kolom namun dengan urutan 1, 2, 3 dan 4 di atas tabelnya. Tabel disusun kembali berdasarkan kunci dan dibaca kembali baris per baris. Hasil dekripsi ditampilkan pada kotak Decrypted.

Algoritma Metode XOR Cipher

Pada metode XOR Cipher, urutan algoritma pemakaian, proses enkripsi dan dekripsi adalah sebagai berikut:

1. Pengguna memasukkan teks yang akan dienkripsi ke dalam plaintext.
2. Pengguna memasukkan kunci berupa teks, tanpa simbol, angka ataupun spasi.
3. Proses enkripsi akan mengambil setiap karakter plaintext dan disilangkan sesuai logika XOR terhadap pembagi dari kunci. Karakter pembagi letaknya didapat dari letak karakter plaintext dimodulus panjang kunci ditambah 1, atau dengan melalui persamaan berikut ini:

   (A Mod t) + 1.....2)

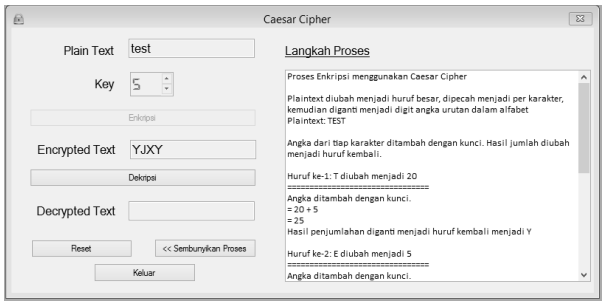
   dengan A = letak karakter plaintext yang sedang aktif dan t = panjang kunci

4. Hasil enkripsi kemudian ditampilkan ke dalam kotak Encrypted.
5. Proses dekripsi sama dengan proses enkripsi, dengan fungsi persamaan yang sama seperti di atas. Hasilnya ditampilkan ke dalam kotak Decrypted.

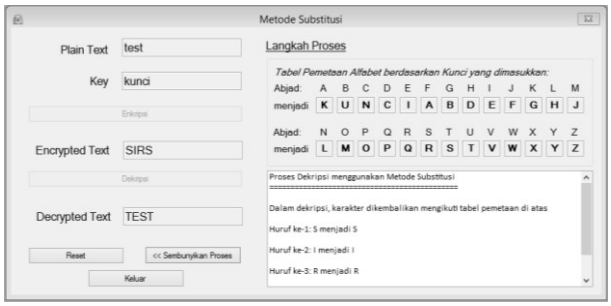
Implementasi dan Pengujian

Adapun tampilan akhir hasil perancangan aplikasi pembelajaran kriptografi klasik dapat dilihat di bawah ini:

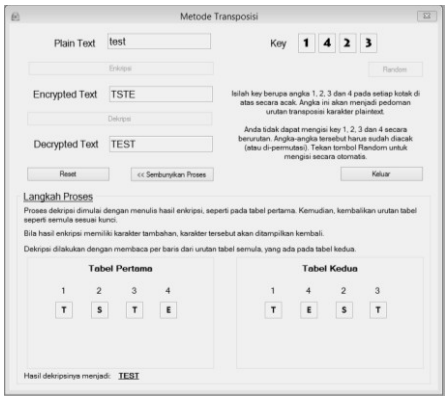
Gambar 2: Tampilan Menu Utama



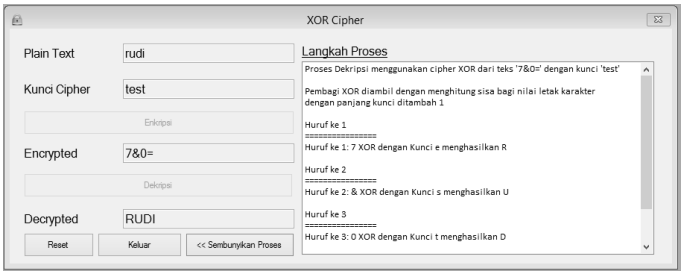
Gambar 3: Tampilan jendela Caesar Cipher dan Hill Cipher



Gambar 4: Tampilan jendela Metode Substitusi



Gambar 5: Tampilan jendela Metode Transposisi



Gambar 6: Tampilan jendela XOR Cipher

4. Kesimpulan

Setelah menyelesaikan perancangan aplikasi pembelajaran kriptografi klasik, penulis menarik kesimpulan sebagai berikut ini:

1. Kriptografi Klasik menjadi bahan pengantar yang tepat untuk menjelaskan proses enkripsi dan dekripsi secara mendasar kepada mahasiswa.
2. Aplikasi yang telah dirancang dapat dipakai sebagai alat bantu pengajaran pengantar kriptografi.
3. Tahapan proses enkripsi dan dekripsi setiap metode kriptografi klasik dapat dilihat secara langsung pada setiap proses enkripsi ataupun dekripsi.
4. Mahasiswa dapat membahas kembali teori-teori kriptografi klasik langsung dari aplikasi yang telah dirancang.

Daftar Pustaka

[1] Ariyus, Dony. 2006. Computer Security. Penerbit Andi, Yogyakarta.
[2] Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi. Penerbit Andi, Yogyakarta
[3] Fairuzabadi, Muhammad. 2010. Implementasi Kriptografi Klasik Menggunakan Borland Delphi. Jurnal Dinamika Informatika 4(2): 65-78.
[4] Konheim, Alan G. 2007. Computer Security and Cryptography. John Wiley & Sons, Inc, New Jersey.
[5] Patterson, Wayne. 1987. Mathematical Cryptology for Computer Scientists and Mathematicians. Rowman & Littlefield, New Jersey.
[6] Stallings, William. 2011. Cryptography and Network Security, Fifth Edition. Prentice Hall, New York.
[7] Vacca, John R. 2009. Computer and Information Security Handbook. Morgan Kaufmann Publishers, Burlington.