**Modul 7**

1. **Tujuan**

1. Mampu menjelaskan definisi dan konsep Hill Cipher

2. Mampu memahami konsep dasar Hill Cipher

1. **Dasar teori**
2. **Hill Cipher**

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

Hill Cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher karena teks yang akan diproses akan dibagi menjadi blokblok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula.

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext. Teknik kriptanalisis ini disebut known-plaintext attack.

1. **Algoritma Hill Cipher**

Dasar dari teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K-1 sehingga: Kunci harus memiliki invers karena matriks K-1 tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

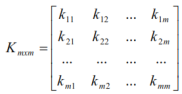
1. **Enkripsi**

Tahapan-tahapan algoritma enkripsi Hill Cipher sebagai berikut :

1. Korespondenkan abjad dengan numerik

*A*→ 1, *B*→ 2, …, *Z*→ 26

1. Buat matriks kunci berukuran m x m, biasanya digunakan kunci 2x2 atau 3x3

[](https://muamalkhoerudin.files.wordpress.com/2015/03/a.png)

1. Matrik K merupakan matriks *yang invertible* yaitu memiliki *multiplicative inverse K*−1 sehingga *K*.*K*−1 = 1
2. Plainteks *P*= *p*1 *p*2 … *pn*,   diblok dengan ukuran sama dengan  baris atau kolom matrik K, sehingga jika menggunakan kunci matriks 2x2, maka plainteks dibuat menjadi matriks 2x1. Jika menggunakan kunci matriks 3x3, maka plainteks diubah menjadi matriks 3x1.
3. Kalikan matriks kunci dengan matriks plainteks menggunakan aturan perkalian matriks.
4. Ubah hasil langkah ke-6 kedalam abjad menggunakan koresponden abjad dengan numerik pada langkah 1 sehingga diperoleh cipherteks
5. **Dekripsi**
6. Korespondekan abjad dengan numerik

*A*→ 1, *B*→ 2, ..., *Z*→ 26

1. Ubah cipherteks kedalam numerik, kemudian buat matriks plainteks sesuai dengan matriks kunci yang digunakan
2. Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matrik kunci *K mxm*. Cara untuk mendapatkan inverse matriks ada pada modul di excel.
3. Menghitung *K*−1
4. Kalikan invers matriks kunci dengan cipherteks transpose dalam modulo 26, diperoleh plainteks transpose *Pt*= *K*−1*C t*
5. Dari langkah ke-5 diperoleh *P*= (*Pt*) *t*
6. Korespondensikan abjad dengan numerik hasil langkah 6 diperoleh plainteks
7. **Keamanan**

Kriptanalisis terhadap Hill Cipher sangat sulit jika dilakukan dengan ciphertext-only attack, terlebih apabila matriks kunci yang digunakan berukuran besar. Kesulitan ini disebabkan oleh ciphertext Hill Cipher yang tidak memiliki pola dan setiap karakter dalam satu blok saling mempengaruhi karakter lainnya.

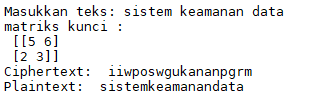
Teknik yang dapat digunakan untuk melakukan kriptanalisis terhadap Hill Cipher adalah knownplaintext attack. Jika kriptanalisis memiliki pecahan plaintext dan ciphertext yang saling berkorespondensi, maka Hill Cipher dapat dipecahkan. Namun proses yang cukup sulit adalah untuk menentukan panjang kunci yang digunakan.

Hal ini menjadi salah satu kekuatan yang dimiliki oleh Hill Cipher. Cara yang dapat dilakukan hanya dengan mencari tahu panjang kunci atau dengan melakukan perkiraan dan percobaan

Berdasarkan pembahasan yang telah dilakukan diatas, maka kesimpulan yang dapat diambil adalah:

1. Hill Cipher adalah algoritma kriptografi klasik yang sangat kuat dilihat dari segi keamanannya.
2. Matriks kunci Hill Cipher harus merupakan matriks yang invertible. Semakin besar suatu matriks kunci maka semakin kuat juga segi keamanannya.
3. Hill Cipher kuat dalam menghadapi ciphertext-only attack namun lemah jika diserang dengan knownplaintext attack.
4. **Program**

Berikut adalah contoh hasil program Hill Chiper



**D. TUGAS INDIVIDU**

1. Membuat fungsi enkripsi dan dekripsi teks menggunakan hill chiper (desain bebas, minimal dapat menampilkan plaintext dan ciphertext sesuai contoh di modul).

* + - Bebas menggunakan bahasa pemrograman apa pun silahkan (Python, Java, PHP, dll).
    - Kata yang akan di enkripsi adalah nama masing-masing. Contoh : Yusuf Fadlila Rachman
    - Kata kunci yang digunakan dapat berupa matriks 2x2 atau 3x3. Nilai matriks bebas
    - Tambahkan dengan **PENJELASAN PROGRAM** yang anda buat (terutama fungsi enkripsi dan dekripsinya). Penjelasan ditulis pakai comment saja boleh, atau di bagian readme Github.

2. Membuat enkripsi dan dekripsi teks di excel. Kata yang dienkripsi sesuai dengan nama lengkap masing-masing. Kunci sesuaikan dengan yang dipakai program. Contoh ada di file excel.

3. Pengumpulan Tugas Praktikum

* **Upload file excel dan kode program di akun github masing-masing.** Kemudian kumpulkan link github di SPADA. Contoh : <https://github.com/fadilrahman46/IoT>
* **Untuk kelas TI E** paling lambat tanggal **11 Oktober 2021 jam 23.59**

**Untuk kelas TI D** paling lambat tanggal **12 Oktober 2021 jam 23.59**

* Format penamaan file SKD\_namakelas\_nim\_nama