Tugas 2 Kriptografi

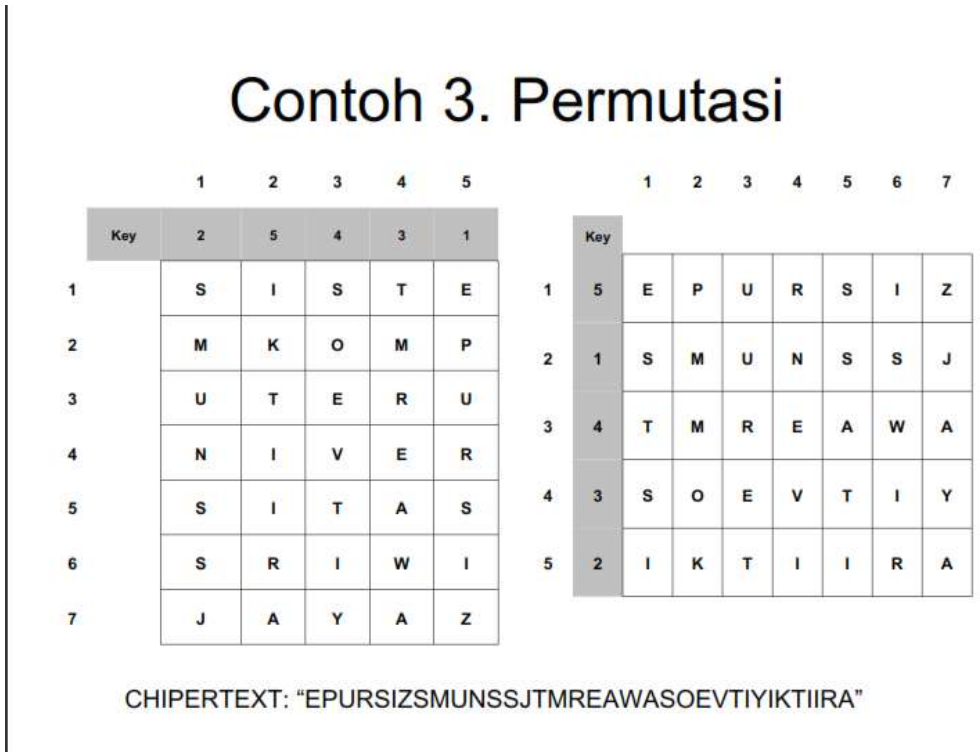
Nama: Ahmad Fitri Rashad

Kelas: SK7Pil

NIM: 09121001023

Kriptografi Simetris adalah: Kode Hill atau lebih dikenal dengan Hill cipher merupakan salah satu algoritma kriptografi kunci simetris dan merupakan salah satu kripto polyalphabetic. Hill cipher diciptakan oleh Lester S. Hill pada tahun 1929. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Berbeda dengan caesar cipher, hill cipher tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada cipherteks karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Karena menggunakan matriks sebagai kunci, Hill cipher merupakan algoritma kriptografi kunci simetris yang sulit dipecahkan, karena teknik kriptanalisis seperti analisis frekuensi tidak dapat diterapkan dengan mudah untuk memecahkan algoritma ini. Hill cipher sangat sulit dipecahkan jika kriptanalis hanya memiliki ciphertext saja (chipertext-only), namun dapat dipecahkan dengan mudah jika kriptanalis memiliki ciphertext dan potongan dari plaintext-nya (known-plaintext).



Contoh gambar diatas merupakan sebuah contoh dari kriptografi invers, dengan kunci 1 (2) 2 (5) 3 (4) 4 (3) 5 (1), matriks A_{7x5} dan kalimatnya adalah SISTEM KOMPUTER UNIVERSITAS SRIWIJAYA. Cara kerja enkripsi kriptografi jenis matriks invers tersebut adalah dengan cara misalnya matriks A dan B masing-masing adalah matriks persegi, sehingga AB=BA=I, maka matriks B adalah invers matriks A dan ditulis $B = A^{-1}$ dan matriks A adalah invers matriks B dan ditulis $A = B^{-1}$. Matriks A dan B adalah matriks yang saling invers. Dengan menggunakan key 1 2 3 4 5, kalimat pada baris 2 dibalik / diinvers menjadi kolom 2, ini merupakan cara kerja sebuah matriks invers, yaitu kolom menjadi baris. Setelah semua baris tersebut menjadi kolom, maka akan didapatkan ciphertext dengan kata: "EPURSIZSMUNSSJTMREAWASOEVTIYIKIIRA". Dengan catatan, ditambahkan huruf 'Z' pada kalimat teresebut agar tidak ada terjadi kata yang kosong dalam pada baris tersebut.

Untuk mendekripsi matriks invers dari kalimat diatas, maka kita gunakan key 1 (5) 2 (1) 3 (4) 4 (3) 5 (2), kemudian kita urutkan menjadi kalimat yang hasilnya adalah seperti kalimat awal: SISTEM KOMPUTER UNIVERSITAS SRIWIJAYA.

NB: pada contoh diatas, diketahui bahwa ada 2 key, yaitu untuk menenkripsi data dan mendekripsi data.