Nama : Demitries Baskhara Rivaldo Tolla
NIM : 123180137
Kelas : A

Tugas Pertemuan 2

1.**known-plaintext attack(KPA)**

Model serangan untuk kriptanalisis di mana penyerang memiliki akses ke teks biasa , dan versi terenkripsi . Ini dapat digunakan untuk mengungkap informasi rahasia lebih lanjut seperti kunci rahasia dan buku kode.

Selama serangan, penyerang memiliki akses ke teks tersandi dan teks biasa yang sesuai. Tujuannya adalah menebak kunci rahasia (atau sejumlah kunci rahasia) atau mengembangkan algoritma yang memungkinkannya mendekripsi pesan lebih lanjut.

Ini memberi penyerang kemungkinan yang jauh lebih besar untuk memecahkan cipher daripada hanya dengan melakukan serangan ciphertext saja. Namun, dia tidak dapat secara aktif memberikan data yang disesuaikan atau kunci rahasia yang akan diproses oleh sandi.

Serangan teks biasa paling efektif jika digunakan terhadap jenis sandi yang paling sederhana. Misalnya, menerapkannya pada sandi substitusi sederhana memungkinkan penyerang untuk segera memecahkannya.

2.**Analisa Statistik**

Semua algoritma enkripsi sebelum data encryption standard (DES) rentan terhadap analisa statistik, kecuali one-time pad.

Untuk sukses , dibutuhkan pengetahuan empiris mengenai statistik penggunaan huruf, naskah acak yang dapat dianalisa harus cukup besar, rumus atau seminimnya jenis enkripsi harus diketahui jika rumus tidak diketahui tetapi jenis enkripsi diketahui berupa simple substitution, setiap huruf acak harus dipasangkan dengan huruf asli. Untuk analisa frekuensi yang rumit, penggunaan komputer sangat membantu.

3.**Brute-force search**

Dalam ilmu komputer, brute-force search atau exhaustive search, juga dikenal sebagai generate and test, adalah teknik pemecahan masalah yang sangat umum dan paradigma algoritmik yang terdiri dari secara sistematis menghitung semua kandidat yang mungkin untuk solusi dan memeriksa apakah setiap kandidat memenuhi pernyataan masalah .

Contoh kasus dalam ilmu komputer adalah masalah penjual keliling (TSP). Misalkan seorang salesman perlu mengunjungi 10 kota di seluruh negeri. Bagaimana cara menentukan urutan kota mana yang harus dikunjungi sehingga jarak total yang ditempuh diminimalkan ?.

Solusi brute force hanya menghitung jarak total untuk setiap rute yang memungkinkan dan kemudian memilih yang terpendek. Ini tidak terlalu efisien karena dimungkinkan untuk menghilangkan banyak kemungkinan rute melalui algoritma yang cerdas.

Kompleksitas waktu dari brute force adalah O (mn), yang terkadang ditulis sebagai O (n * m). Jadi, jika kita mencari string karakter "n" dalam string karakter "m" menggunakan brute force, itu akan membawa kita mencoba n * m.