Quis 2 TKK

Waktu 120 menit

Tanggal 15 Nopember 2019

Sifat Terbuka khusus nomor 3

Dosen : M. Husni

1. Tujuan dari masalah ini adalah untuk menentukan berapa bilangan prima yang ada. Misalkan ada total n bilangan prima, dengan urutan: p1 = 2 < p2 = 3 < p3 = 5 < ... < pn.

Tentukan X = 1 + p1p2 ... pn. Artinya, X sama dengan satu plus produk dari semua bilangan prima. Carilah bilangan prima pm yang bisa membagi X?

Maaf sebelumnya, karena di soal ada bagian yang kurang jelas. X = 1 + p1p2 ... pn -> tidak jelas p1p2….pn ditambah atau dikali.

Jika ditambah,

Misalkan :

P1 = 2 ; p2 = pn = 3

X=1+2+3=6

X/p2 = 6/3 = 2 -> habis dibagi

Jika dikali,

Bilangan prima memiliki sifat-sifat yang unik. Semua bilangan prima adalah ganjil kecuali 2. Semua memiliki 2 faktor yaitu 1 dan dirinya sendiri. Karena sifat bilangan ganjil jika dikali bilangan genap adalah genap, tentunya hasil perkalian dari bilangan prima adalah genap (p1=2). Kemudian ditambahkan dengan 1 akan menghasilkan bilangan ganjil. Bilangan ganjil tersebut berdasarkan nilai dari n. Pn = bilangan prima terbesar yang dihitung harus merupakan FPB dari X (X = 1 + p1p2 ... pn)

1. Cipher text di bawah ini merupakan hasil dari algoritma Caesar. Gunakan program analisis huruf dalam bahasa Indonesia, dan kembalikan cipher ini menjadi plain text yang berarti.

qirhirkev neaefer mxy om ewiq kihi xmheo oepel xivoinyxrce qeoe wikive me qipsqtexm tmrxy her gitexgitex qiriqym qirerxyrce qeliwe nirev her qerxmrker cerk qivewe fivoitirxmrker type wikive qirkmoyxm om ewiq kihi feverkoepm qivioe hetex qirspsrk qiqfivmoer fifivete oixiverker cerk hmtivpyoer

Jawaban:

Analisis huruf pada cipher text diatas menghasilkan frekuensi huruf sebagai berikut :

A : 1 \*

B : 0

C : 4 \*\*\*\*

D : 0

E : 45 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

F : 6 \*\*\*\*\*\*

G : 2 \*\*

H : 8 \*\*\*\*\*\*\*\*

I : 37 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

J : 0

K : 13 \*\*\*\*\*\*\*\*\*\*\*\*\*

L : 2 \*\*

M : 15 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

N : 3 \*\*\*

O : 13 \*\*\*\*\*\*\*\*\*\*\*\*\*

P : 6 \*\*\*\*\*\*

Q : 17 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

R : 28 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

S : 3 \*\*\*

T : 9 \*\*\*\*\*\*\*\*\*

U : 0

V : 13 \*\*\*\*\*\*\*\*\*\*\*\*\*

W : 6 \*\*\*\*\*\*

X : 14 \*\*\*\*\*\*\*\*\*\*\*\*\*\*

Y : 8 \*\*\*\*\*\*\*\*

Z : 0

Ciphertext diatas diubah menjadi plaintext melalui program Caesar Decryption dengan menggunakan key 4

Hasil Plaintext : mendengar jawaban itu ki asem gede tidak kalah terkejutnya maka segera ia melompati pintu dan cepatcepat menemui menantunya mahesa jenar dan mantingan yang merasa berkepentingan pula segera mengikuti ki asem gede barangkali mereka dapat menolong memberikan beberapa keterangan yang diperlukan

Setelah menemukan plaintextnya, selanjutnya kita analisis frekuensi huruf pada plaintext tersebut melalui program analisis huruf dalam bahasa Indonesia.

Hasil Frekuensi huruf pada plaintext :

A : 45 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

B : 6 \*\*\*\*\*\*

C : 2 \*\*

D : 8 \*\*\*\*\*\*\*\*

E : 37 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

F : 0

G : 13 \*\*\*\*\*\*\*\*\*\*\*\*\*

H : 2 \*\*

I : 15 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

J : 3 \*\*\*

K : 13 \*\*\*\*\*\*\*\*\*\*\*\*\*

L : 6 \*\*\*\*\*\*

M : 17 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

N : 28 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

O : 3 \*\*\*

P : 9 \*\*\*\*\*\*\*\*\*

Q : 0

R : 13 \*\*\*\*\*\*\*\*\*\*\*\*\*

S : 6 \*\*\*\*\*\*

T : 14 \*\*\*\*\*\*\*\*\*\*\*\*\*\*

U : 8 \*\*\*\*\*\*\*\*

V : 0

W : 1 \*

X : 0

Y : 4 \*\*\*\*

Z : 0

Tanda \* (bintang) disebelah angka merupakan presentasi hasil yang didapat dari frekuensi huruf pada plaintext tersebut. Analisis yang didapat dari hasil frekuensi huruf plaintext tersebut, Huruf A merupakan huruf yang paling sering digunakan, Huruf E merupakan huruf urutan kedua yang paling sering digunakan, Huruf N merupakan huruf urutan ketiga yang paling sering digunakan.

1. Tulis esai singkat yang menjelaskan metode enkripsi apa pun yang belum anda kenal atau yang belum kita pelajari. Kemudian jelaskan sejarah dan asal dari algoritma itu. Anda juga harus memberikan beberapa perbandingan dengan algoritma terkenal lainnya.

Jawaban :

Metode Enkripsi

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat terbaca tanpa melalui proses deskripsi. Metode enkripsi yang belum saya ketahui dan pelajari ada banyak, diantarnya yaitu : Triple DES, Blowfish, AES, Twofish, RSA, Diffie-Hellman Key Exchange, Enkripsi Elgamal, ECC.

Triple DES dikembangkan untuk menggantikan algoritma DES asli. Triple DES menyediakan metode sederhana untuk memperluas ukuran kunci DES (dengan menerapkan algoritma DES tiga kali pada setiap blok data). Panjang total kunci hingga 168 bit. Karena serangan meet-in-the-middle (MITM), keamanan yang efektif diberikan hanya 112 bit.

Blowfish dirancang untuk menggantikan DES (Enkripsi Data Standar) karena lebih efektif dan lebih cepat. Blowfish bekerja dengan panjang blok 64 bit dan ukuran kunci variabel berkisar antara 32 bit sampai 448 bit. Enkripsi ini melibatkan 16 putaran Feistel cipher menggunakan kunci S-box yang sangat penting.

AES (Advanced Encryption Standard) adalah penerus DES, dan dipercaya sebagai Enkripsi standar oleh pemerintah Amerika dan berbagai lembaga negara. AES sangat efisien dalam bentuk 128 bit, namun tetap menggunakan kunci 192 dan 256 bit untuk keamanan tingkat tinggi. AES memiliki 10 putaran untuk kunci 128 bit, 12 putaran untuk kunci 192 bit, dan 14 putaran untuk kunci 256 bit.

Twofish dirancang untuk menggantikan Blowfish, pakar keamanan komputer Bruce Schneier adalah orang dibalik penemuan algoritma tersebut.Twofish adalah metode enkripsi kunci simetris yang menggunakan ukuran blok 128 bit dan ukuran kunci hingga 256 bit.Satu setengah dari kunci n-bit digunakan sebagai kunci enkripsi dan yang lainnya digunakan untuk memodifikasi algoritma enkripsi (key-dependent S-boxes).

RSA adalah teknik enkripsi kunci asimetris dan standar untuk mengenkripsi data melalui internet. Kekuatan enkripsi meningkat secara eksponensial dengan peningkatan ukuran kunci, yang biasanya 1024 atau 2048 bit.

Diffie-Hellman adalah teknik kriptografi kunci publik yang merupakan pengembangan dari RSA, Diffie-Hellman memungkinkan dua pihak bersama-sama membangun kunci rahasia melalui saluran tidak aman. Keterbatasan algoritma ini adalah kurangnya otentikasi, data yang menggunakan Diffie-Hellman rentan terhadap serangan man-in-the-middle.

Enkripsi ElGamal adalah kriptografi kunci asimetris berdasarkan Diffie-Hellman Key Exchange. Keamanan ini tergantung pada kesulitan penghitungan log diskrit dalam modulus yang besar. plaintext yang sama memberikan ciphertext yang berbeda setiap kali dienkripsi. Namun ciphertext yang dihasilkan dua kali lebih lama dari plaintext. Enkripsi dapat didefinisikan pada setiap kelompok cyclic dan keamanannya bergantung pada sifat kelompok yang mendasari dan juga skema padding yang digunakan pada plaintext.

Elliptic Curve Cryptography adalah metode enkripsi asimetris yang didasarkan pada struktur aljabar kurva elips. Sebagai pengganti dari pendekatan tradisional yang menghasilkan kunci bilangan prima besar, ECC menciptakan kunci melalui sifat persamaan kurva eliptik. Keamanan ECC didasarkan pada kemampuannya untuk menghitung perkalian, ukuran kurva eliptik menentukan tingkat kesulitan dari masalah. Hal ini dapat memberikan tingkat keamanan dengan kunci 164 bit yang sistem lain (seperti RSA) memerlukan kunci 1024 bit untuk mencapainya.