Soal UAS Kriptografi UI

ENCE608044 - 646884

Semester Genap, tahun 2020/2021

Dosen : Dr. Yohan Suryanto, ST. MT.

Soal Nomor 1:

Kunci AES bagian word pertama (kolom pertama) dienkrip menggunakan RSA per word menggunakan RSA dengan kunci private (d=59102551 dan n) yang disusun dari 2 bilangan prima p = 6959 dan q = 13417.

Hasil enkripsi Kunci AES word pertama tersebut adalah: 59573159 (dalam bentuk hexa 038D03A7)

03	00	00	00
8D	00	00	00
03	00	00	00
A7	00	00	00

Temukanlah pasangan kunci publik yang digunakan, serta plaintext kunci AES-nya.

Soal Nomor 2:

Gunakan kunci AES yang didapatkan dari soal nomor 1 untuk men-decipher gambar cipherImage.png. Gambar tersebut dienkrip menggunakan AES per matrik 4x4 untuk semua komponen warna. Jelaskan cara anda mendapatkan gambar asli (hasil decipher), tunjukkan gambar tersebut, dan sertakan file gambar hasil deciphernya.

Soall Nomor 3:

Misalnya File_soal_nomor_3.rtf dikirim oleh Iwan kepada Budi. Diketahui Iwan juga mengirim MD5 file tersebut, dengan ketentuan 7 hexa terakhir dari MD5 file tersebut dienkrip menggunakan kunci private Iwan dengan hasil MD5: c17b830d9043ee6eb76496549**4bb326a** (7 angka hexa warna merah merupakan hasil enkripsi dari 7 angka hexa original MD5 file tersebut, dienkrip sebagai sebuah bilangan)

Jelaskan dan simulasikan menggunakan program RSA yang anda buat, bagaimana Budi memastikan bahwa pesan tersebut memang berasal dari Iwan, jika diketahui kunci publik Iwan (e = 1223; dan n= 93184991);

Gunakan hash calculator, misalnya seperti: https://emn178.github.io/online-tools/md5_checksum.html