Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas 3 IF4020 Kriptografi Semester I Tahun 2021/2022
Modified RC4 dan Steganografi dengan LSB

Batas pengumpulan : Jumat, 1 Oktober 2021
Tempat pengumpulan : Googgle drive
Berkas pengumpulan : File pdf , kode program di google drive/github, link video demo
Per kelompok : Max 3 orang

A. Modifikasi RC4

Buatlah sebuah program *stream cipher* yang memodifikasi RC4 (*modified RC4*) dalam Bahasa C/C++/Java/C++/C#/Python/Golang (pilih salah satu) dengan antarmuka (GUI). Memodifikasi RC4 dapat berarti memodifikasi prosedur KSA atau PRGA di dalam RC4, membuat fungsi permutasi yang lebih kompleks, menambahkan LFSR, dll.

Spesifikasi program adalah sebagai berikut:

1. Program dapat menerima pesan berupa *file* sembarang (file text maupun file biner) atau pesan yang diketikkan dari papan-ketik.
2. Program dapat mengenkripsi plainteks dan mendekripsi cipherteks menjadi plainteks semula.
3. Untuk pesan berupa text, program dapat menampilkan plainteks dan cipherteks di layar.
4. Program dapat menyimpan cipherteks ke dalam *file*.
5. Kunci dimasukkan oleh pengguna. Panjang kunci bebas.

B. Penyembunyian pesan di dalam berkas multimedia

Buatlah program steganografi pada citra digital dan satu lagi pada audio/video (pilih salah satu) dengan metode LSB. Format citra yang digunakan adalah BMP (bitmap) dan PNG (Portable Network Graphics). Format BMP tidak terkompresi, sedangkan format PNG terkompresi dengan metode kompresi *lossless*. Format audio yang digunakan adalah WAV dan format video yang digunakan adalah AVI. Kedua format tersebut tidak terkompresi.

Pada praktekmya, sebelum disisipkan, pesan dapat dienkripsi terlebih dahulu dengan sebuah algoritma enkripsi. Karena anda membuat program modifikasi Rc4, maka algoritma enkripsi yang digunakan adalah *modified RC4*. Pesan yang disisipkan adalah sembarang *file* dengan ukuran yang tidak melebihi kapasitas penyisipan (*payload*). Kapasitas penyisipan dihitung sebelum proses penyisipan.

Jika anda memilih video, maka pesan dapat disisipkan secara sekuensial mulai dari frame pertama dan seterusnya, atau secara acak pada frame-framenya.

Jika anda memilih audio, maka pesan dapat disisipkan secara acak pada data audio (amplitudo) atau secara acak.

Spesifkasi program:

1. Program menerima masukan berupa citra digital dengan format BMP atau PNG, berkas audio/video (pilih salah satu), nama file pesan, dan kunci stego (opsional, jika pengguna memilih untuk mengenkripsi pesan dan/atau jika memilih penyisipan secara acak).
2. Metode steganografi yang digunakan adalah metode LSB.
3. Pengguna dapat memilih apakah pesan dienkripsi atau tidak dienkripsi sebelum disisipkan.
4. Pesan disisipkan secara sekuensial pada pixel-pixel citra atau acak.
5. Untuk citra, hitung PSNR setelah penyisipan. Untuk audio/video, hitung pengukuran *fidelity*-nya (silakan cari rumus untuk menghitungnya).

Tugas A dan B disatukan dalam satu antarmuka program (berbasis GUI). Struktur menu kira-kira sebagai berikut (anda boleh membuat struktur menu yang lain, tidak harus sama dengan di bawah ini):

A. Modified RC4
   1. Enkripsi
   2. Dekripsi

B. Steganografi

   B.1 Penyembunyian pesan

   (x) Tanpa enkripsi ( ) Dengan enkripsi (ket: check box)

   1. Citra
      1.1 Sekuensial
      1.2 Acak

   2. Audio/video
      2.1 Sekuensial
      2.2 Acak

   B.2 Ekstraksi pesan

   1. Citra
   2. Audio/video

Pada waktu ekstraksi pesan, pengguna tidak memilih lagi apakah sekuensial atau acak. Program harus dapat menentukan apakah pada waktu penyisipan pesan dilakuka secara acak atau secara sekuensial. Cara yang paling mudah adalah menyisipkan kode tertentu pada bagian awal citra/audio/video pada frame pertama yang mengindikasikan pilihan sekuensial atau acak pada waktu penyisipan (misalnya kode 11, 12, 21, 22) atau dengan cara yang lain.

Yang dikumpulkan:

1. *Source program* lengkap
2. Tampilan antarmuka program (*print screen/screen shot*)
3. Contoh hasil enkripsi, hasil dekripsi, citra/video hasil penyembunyian pesan, hasil ekstraksi pesan, dll
4. Pranala kode program di google drive/github
5. Pranala video demo (diunggah di *google drive* atau *youtube*) yang berisi fungsionalitas dari program yang dibuat (maksimal durasi 7 menit). Tidak ada demo program secara langsung dengan asisten. Demo program hanya melalui video saja.
6. Alamat pengumpulan: https://forms.gle/dX1ecQjLtVP1i4bk9