KEAMANAN PERANGKAT LUNAK

Topic: Steganography

Disusun Oleh:

Resa Halen Manurung

11322048

D-III Teknologi Informasi-02

FAKULTAS VOKASI
INSTITUT TEKNOLOGI DEL

Review Questions

Week 9 Steganography

* Review Questions

1) What is steganography?

Jawab: Steganography adalah teknik penyamaran informasi atau pesan rahasia dalam media digital (seperti gambar, audio, atau video) untuk menyembunyikan dari pandangan orang lain. Informasi yang disembunyikan tersebut hanya dapat dibuka atau diekstraksi oleh penerima yang mengetahui cara membuka pesan tersebut.

2) How many media can use a steganography technique?

Jawab: Teknik steganografi dapat diterapkan pada berbagai jenis media, antara lain:

① Gambar
- Media paling umum untuk steganografi, seperti format PNG, BMP, atau JPEG.
- Teknik seperti LSB (Least Significant Bit) sering digunakan untuk mengganti kan bit-bit data gambar dengan bit dari pesan rahasia.

② Audio
- Informasi rahasia dapat disisipkan ke dalam file audio menggunakan teknik seperti LSB dalam waveform atau mengubah frekuensi yang tidak terdengar oleh manusia.
- Contoh format: WAV, MP3.

③ Video
- Steganography video dapat memanfaatkan frame atau piksel untuk menyisipkan data rahasia.
- format populer: MP4, AVI, MKV

④ Dokumen Teks

Menyisipkan pesan dengan mengubah format teks (misalnya, jarak antara baris atau font yang berbeda) atau menyembunyikan karakter tertentu di dokumen teks.

⑤ Protokol jaringan.

Informasi rahasia dapat disisipkan dalam header paket jaringan, data dummy, atau aliran data lainnya di dalam protokol komunikasi.

3) what is the difference between cryptography and steganography?

Jawab :

Aspek	Cryptography	Steganography
Definisi	Seni dan ilmu mengamankan informasi dengan mengenkripsi atau mengacak data menggunakan algoritma.	Seni dan ilmu menyembunyikan informasi rahasia dalam media lain sehingga keberadaannya tidak terlihat.
Keberadaan Pesan	Pesan terlihat, tetapi tidak dapat dibaca tanpa kunci deskripsi	Pesan tersembunyi dan keberadaannya sulit dideteksi.
Teknologi umum	AES, RSA, SHA dan algoritma enkripsi lainnya.	LSB, DCT (Discrete Cosine Transform), dan metode penyembunyian lainnya.
Keamanan	Bergantung pada algoritma dan kekuatan kunci enkripsi.	Bergantung pada metode penyisipan dan ketidakmampuan deteksi oleh pihak ketiga.
Tujuan utama	Mengubah pesan menjadi bentuk yg sulit dimengerti tanpa kunci.	Menyembunyikan pesan agar keberadaannya tidak diketahui

4) What is the difference between MSB and LSB?

Jawab:

Aspek	MSB (Most Significant Bit)	LSB (Least Significant Bit)
Definisi	Bit paling signifikan, biasanya bit paling kiri dalam representasi biner suatu angka atau data	Bit paling tidak signifikan, biasanya bit paling kanan dalam representasi biner suatu angka atau data.
Pengaruh.	Perubahan pada MSB memiliki dampak besar pada nilai data.	Perubahan pada LSB memiliki dampak kecil pada nilai data.
Penggunaan	Jarang digunakan dalam steganography karena perubahan dapat merusak data asli secara drastis.	Sering digunakan dalam steganografi karena perubahan hampir tidak memengaruhi kualitas media asli.
Contoh Penggunaan	Mengubah warna dominan pada gambar (misalnya mengganti intensitas merah secara signifikan).	Menyisipkan informasi rahasia dalam piksel gambar tanpa mengubah warna yang terlihat secara visual.

Computer Programming (C#)

Code using Microsoft Visual Studio.

In this class, you will get the hybrid cryptography and steganography.

The system has implement 2 cryptography, namely: playfair (classic cryptography) and ElGamal

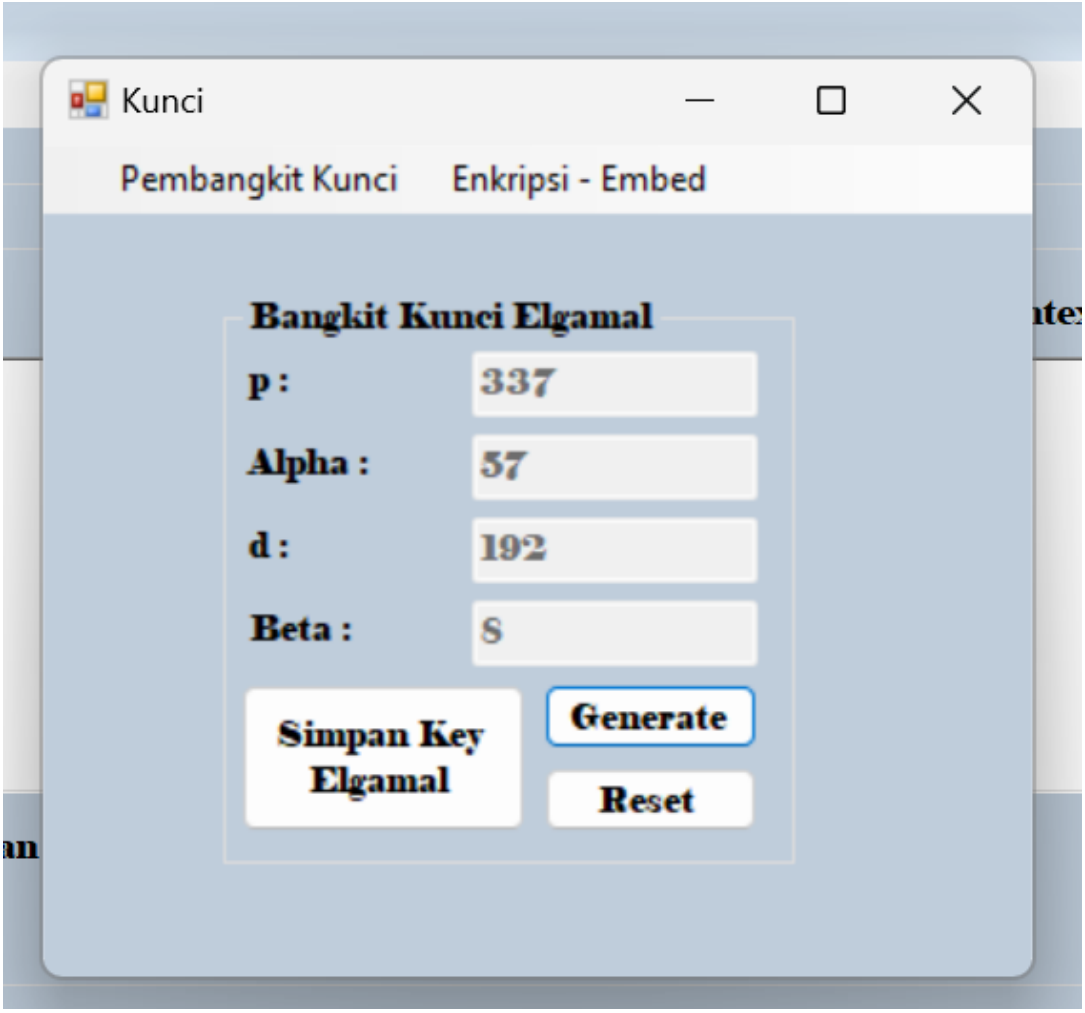
(modern cryptography)

The ciphertext will embed to image using LSB steganography techiques.

How to run:

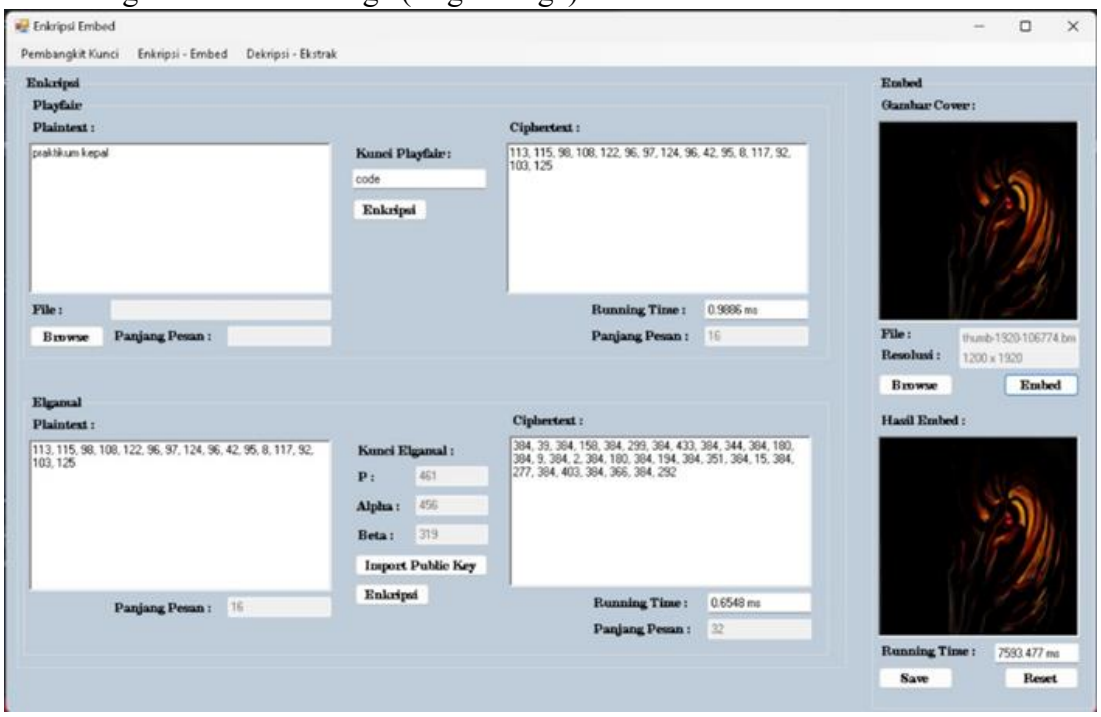
Encryption and embedding

1. Open the tab of key to generate the ElGamal public and private key
2. Click generate and save the key. Don't forget your directory.



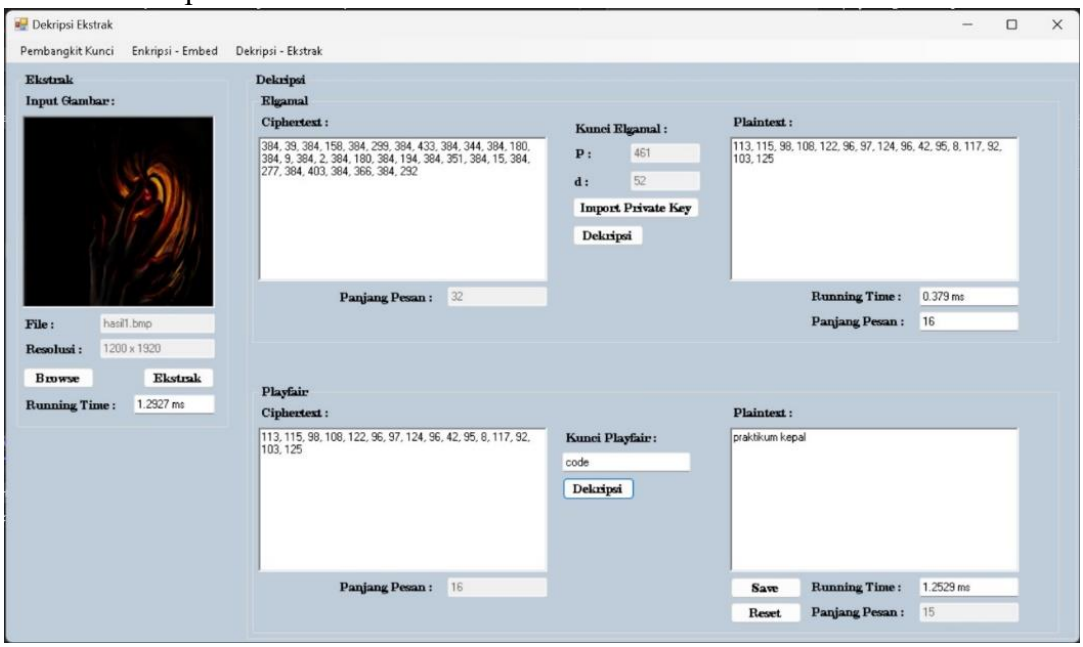
3. Go to Enkripsi-Embed menu. Start to Enkripsi with Playfair, you can add text and key of playfair (its up to you). In ElGamal you have to import Public Key, and click Enkripsi Button. The ciphertext will show on the textbox.
4. Now we want to embed the ciphertext to image, click browse to choose the image, and click Embed.

5. Don’t forget to save the image (stego-image)



Extraction and Decryption

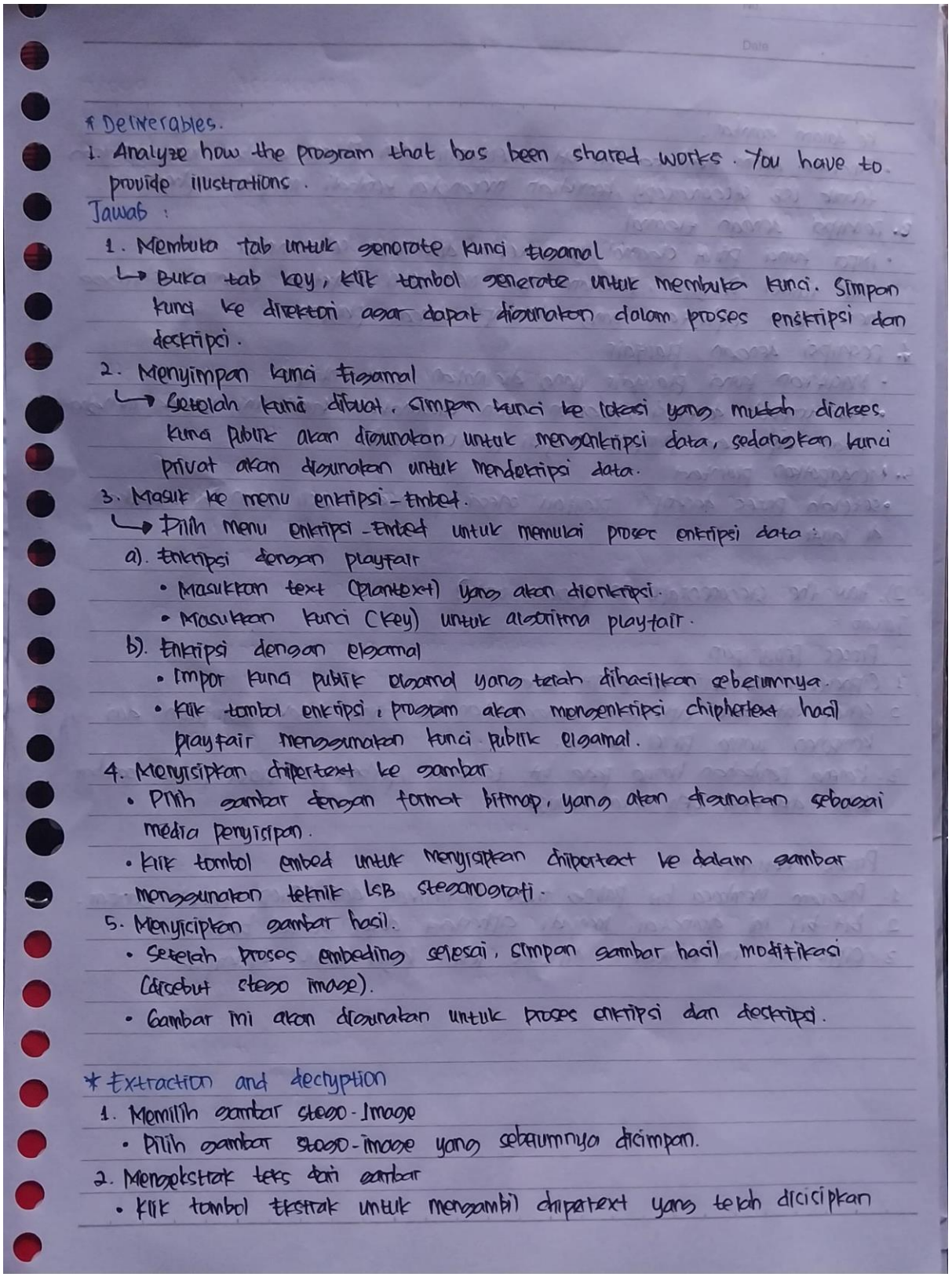
1. Choose the stego-image by click Browse Button.
2. Click Ekstrak to extract the text
3. Move to the ElGamal algorithm, you have to import the Private Key, and Decrypt
4. Move to the Playfair algorithm, input the key and click Dekripsi.
5. You have a plaintext.



Deliverables:

1. Analyze how the program that has been shared works. You have to provide illustrations.

2. How the steganography in the program work?



* Deliverables.
1. Analyze how the program that has been shared works. You have to provide illustrations.
Jawab :
1. Membuka tab untuk generate kunci elgamal
↳ Buka tab key, klik tombol generate untuk membuka kunci. Simpan kunci ke direktori agar dapat digunakan dalam proses enkripsi dan dekripsi.
2. Menyimpan kunci elgamal
↳ Setelah kunci dibuat, simpan kunci ke lokasi yang mudah diakses. Kunci publik akan digunakan untuk mengenkripsi data, sedangkan kunci privat akan digunakan untuk mendekripsi data.
3. Masuk ke menu enkripsi - embed.
↳ Pilih menu enkripsi - embed untuk memulai proses enkripsi data :
a). enkripsi dengan playfair
• Masukkan text (plaintext) yang akan dienkripsi.
• Masukkan kunci (key) untuk algoritma playfair.
b). Enkripsi dengan elgamal
• Impor kunci publik elgamal yang telah dihasilkan sebelumnya.
• Klik tombol enkripsi, program akan mengenkripsi chipertext hasil playfair menggunakan kunci publik elgamal.
4. Menyisipkan chipertext ke gambar
• Pilih gambar dengan format bitmap, yang akan digunakan sebagai media penyisipan.
• Klik tombol embed untuk menyisipkan chipertext ke dalam gambar menggunakan teknik LSB steganografi.
5. Menyiciptan gambar hasil.
• Setelah proses embeding selesai, simpan gambar hasil modifikasi (disebut steso image).
• Gambar ini akan digunakan untuk proses enkripsi dan dekripsi.

* Extraction and decryption
1. Memilih gambar steso-Image
• Pilih gambar steso-image yang sebelumnya dicimpan.
2. Mengekstrak teks dari gambar
• Klik tombol ekstrak untuk mengambil chipertext yang telah diciciptkan

ke dalam gambar.
- Program akan membaca bit-bit tersembunyi dari piksel gambar menggunakan teknik LSB steganography, kemudian merangkai kembali menjadi ciphertext.

3. Deskripsi dengan Elgamal
- Impor kunci privat elgamal yang telah dihasilkan sebelumnya.
- Klik tombol Decrypt, program akan mendeteksi chipetext Elgamal, sehingga menghasilkan ciphertext yang dienkripsi dengan playfair.

4. Deskripsi dengan playfair
- Masukkan kunci playfair yang digunakan saat enkripsi.
- Klik tombol deskripsi, program akan digunakan kunci ini untuk mengha-silkan ciphertext playfair menjadi plantext asli.

5. Mendapatkan plaintext
- setelah proses deskripsi playfair selesai, plaintext asli akan ditampilkan di layar.

2). How the steganography in program work?

Jawab :

Proses penyisipan

1. Ciphertext dikonversi ke format biner.
2. Setiap bit dari ciphertext menggantikan bit paling tidak signifikan dari komponen warna piksel gambar.
3. Karena perubahan hanya pada bit terakhir, perbedaan visual pada gambar sulit dideteksi oleh mata manusia.

Proses Ekstraksi

1. Program membaca bit paling tidak signifikan dari setiap piksel gambar.
2. Bit-bit ini dirangkai menjadi ciphertext dalam format biner
3. Ciphertext ini kemudian diproses lebih lanjut untuk deskripsi.