Jurusan Teknik Informatika

Cryptography

Kebutuhan

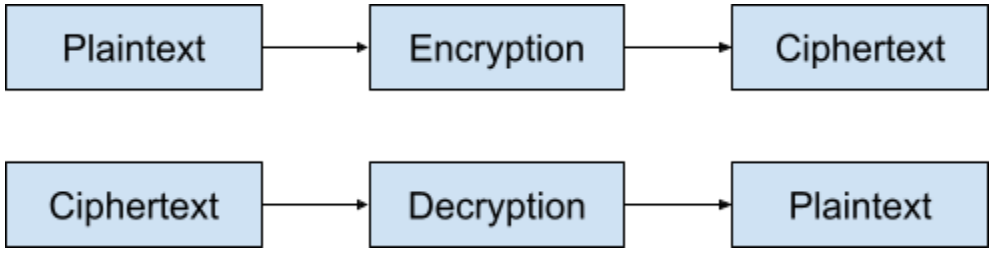
Untuk menjalankan modul ini dengan lancar, Mahasiswa disarankan menggunakan sistem operasi linux. Modul ini akan memaksimalkan penggunaan terminal dan text editor vim. Mahasiswa dapat menyesuaikan dengan menginstall virtual machine atau perangkat sejenis.

Tujuan Praktikum

1. Mahasiswa mampu memahami konsep dasar kriptografi.
2. Mahasiswa memahami perbedaan enkripsi, encoding, dan hashing
3. Mahasiswa mampu mempraktikkan konsep kriptografi klasik dalam bahasa pemrograman python.

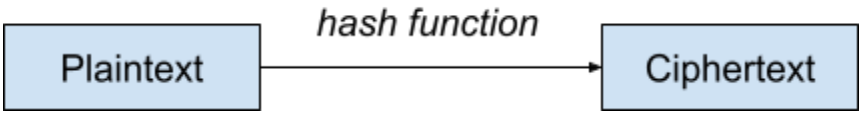
Dasar Teori

Kriptografi adalah metode perlindungan informasi dan komunikasi dengan menggunakan kode tertentu, sehingga hanya pengirim dan penerima yang bisa membacanya. Secara bahasa, ‘crypt-’ bermakna ‘tersembunyi’ dan ‘-graphy’ bermakna ‘tulisan’. Berikut proses dasar dari kriptografi:



Proses dimana plaintext (teks asli) diubah menjadi ciphertext (teks tersandi) disebut sebagai encryption (enkripsi). Sedangkan proses perubahan dari ciphertext (teks tersandi) ke plaintext (teks asli) disebut decryption (dekripsi). Jika dilihat dari gambar diatas, plaintext dan cipher text dapat dibentuk dan dikembalikan sedia kala (*two ways*). Disisi lain, ada metode

kriptografis yang hanya dapat menjadi ciphertext tanpa kemampuan ke plaintext (not recoverable). Metode ini disebut dengan hash function (*one-way cryptography*).



Percobaan

Hashing

1. Pastikan `md5sum` telah terinstall di perangkat yang digunakan.
2. Download file pada tautan berikut (kamu bisa menggunakan command wget) dan ekstrak.
    a. message1.bin & message2.bin

```
wget
https://github.com/isfahany/infosec-module-downloadable-file/raw/master/collision-example/file.zip
```

3. Jalankan command berikut pada file terkait.
    a. sha1sum

```
sha1sum message1.bin message2.bin
```

Penjelasan output

    b. sha256sum

```
sha256sum message1.bin message2.bin
```

Penjelasan output

c. md5sum

```
md5sum message1.bin message2.bin
```

Penjelasan output

4. Analisislah output dari nomor tiga. Menurutmu, mengapa hal tersebut bisa terjadi? Hash function mana yang lebih aman digunakan?

Encoding

1. Pastikan python telah terinstall di perangkat yang digunakan

```
python3 --version
```

2. Buka file dengan nama encode.py (file akan langsung terbuat), lalu *copy-paste* kode berikut:

```
import binascii
import base64
```

```
text = "Road to Security Engineer"
text_utf8 = text.encode("utf-8")
text_b64 = base64.b64encode(text_utf8)
text_hex = binascii.hexlify(text_utf8)

print("text             = " + text)
print("utf8 encode      = " + str(text_utf8))
print("base64 encode    = " + str(text_b64))
print("hexadec encode   = " + str(text_hex))
```

Apa yang dilakukan kode tersebut?

3. Tambahkan fungsionalitas untuk mengembalikan base64 dan hexadecimal encode pada source code python tersebut menjadi semula.

Enkripsi

1. Pastikan python telah terinstall di perangkat yang digunakan

```
python3 --version
```

2. Buka file dengan nama caesar.py (file akan langsung terbuat), lalu *copy-paste* kode berikut:

```
#!/usr/bin/python3

plaintext = "Infosec"
ciphertext = ""
for i in range(len(plaintext)):
      if(plaintext[i].isupper()):
            ciphertext += chr((ord(plaintext[i]) + 7 - 65) % 26 + 65)
      else:
            ciphertext += chr((ord(plaintext[i]) + 7 - 97) % 26 + 97)
print("plaintext = " + plaintext)
print("ciphertext = " + ciphertext)
```

3. Apa yang terjadi pada line 7 dan 9? Mengapa ada angka 65, 97, dan 26 disana?

4. Kriptografi apakah kode tersebut? Bagaimana caranya bekerja?

5. Optimalkan cara kerja algoritma kriptografi tersebut! Ambil input dari user dan juga shift lompatan angka dari user (interactive) !

Tugas

1. Jelaskan perbedaan hash, enkripsi, dan encoding!

2. Diberikan source code berikut, buatlah dekripsi dalam bahasa pemrograman python:

```
#!usr/bin/python3

def encrypt(plaintext):
   plaintext = plaintext[::-1]
   ciphertext = ""
   for i in plaintext:
      copy = "X" * ((ord(i) ^ 0x50) + 9)
      copy += "-"
      ciphertext += copy
   return ciphertext

print ("Infosec Module Encryptor")
plaintext = input("Masukkan string yang ingin di-encrypt: ")
print ("Result : ")
print (encrypt(plaintext))

# decrypt string ini:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-
```

3. Jelaskan source code yang telah anda buat pada nomor 2

4. Jelaskan perbedaan antara
    a. Asymmetric encryption dan symmetric encryption

    b. Stream cipher dan block cipher

Extra Miles

Jika tertarik mendalami kriptografi lebih lanjut kalian bisa mengambil mata kuliah kriptografi. Kalian juga bisa mendalaminya diwaktu luang pada tautan berikut:

- cryptohack.org (tantangan kriptografi yang digamekan dan memiliki leaderboard)
- cryptopals.com (seperti cryptohack, tetapi lebih berfokus pada tantangan)
- www.khanacademy.org/computing/computer-science/cryptography (media pembelajaran dengan video learning dan penjelasan yang apik)