20241_Discrete Mathematics A
Cryptography System

Kelompok 2
Apryadi Dwi Putra Tangalayuk
Calvin Richie Rumendong
Aryo Karel Merentek
Leonard Widjaja

Pendahuluan

Di era digital saat ini, keamanan informasi menjadi aspek yang sangat penting. Setiap hari, jutaan data pribadi, transaksi keuangan, dan komunikasi rahasia dikirimkan melalui jaringan digital. Untuk memastikan bahwa data tersebut tidak jatuh ke tangan yang salah, kita memerlukan cara untuk melindungi informasi tersebut. Di sinilah peran cryptography menjadi sangat penting.

Cryptography adalah ilmu yang mempelajari teknik untuk mengamankan informasi sehingga hanya pihak yang berwenang yang dapat mengakses atau memahami data tersebut. Dengan menggunakan berbagai metode matematika, cryptography memastikan bahwa data tetap rahasia, integritasnya terjaga, dan hanya bisa diakses oleh pihak yang memiliki kunci yang benar.

Salah satu konsep inti dalam cryptography adalah **enkripsi**. **Enkripsi** adalah proses mengubah informasi yang dapat dibaca (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext), menggunakan algoritma enkripsi dan kunci tertentu. Proses ini bertujuan untuk menjaga kerahasiaan data sehingga meskipun data tersebut jatuh ke tangan yang tidak berwenang, mereka tidak dapat memahaminya tanpa kunci dekripsi.

Di sisi lain, **dekripsi** adalah proses kebalikan dari enkripsi, di mana data yang telah dienkripsi (ciphertext) diubah kembali menjadi bentuk aslinya (plaintext). Proses ini hanya dapat dilakukan oleh pihak yang memiliki kunci yang tepat, sehingga memastikan bahwa informasi hanya bisa diakses oleh pihak yang sah.

Pembahasan

Pada tugas kali ini, kunci rahasia yang Kami gunakan adalah "sukabelajardiskrit" yang kemudian akan diolah menggunakan algoritma SHA-256 untuk menghasilkan nilai hash 256-bit yang kemudian dikonversi menjadi bentuk biner. Nilai hash ini kemudian dipisahkan menjadi empat blok, yaitu B1, B2, B3, dan B4, yang akan digunakan dalam proses enkripsi dan dekripsi. Empat blok itu antara lain:

- **B1:**
  11011101110011001100101100001100100001110011111100000101000101 10
- **B2:**
  00000110011011111111000001011110010000101011001000000001111011 001
- **B3:**
  10110100001000101010111000111001000010111101011000110111111001 001
- **B4:**
  01001111111000011010010111100001011010110011010001001011100110 00 0

Selanjutnya, kata yang akan Kami enkripsi adalah **"halo"** dengan mengubah setiap karakternya menjadi biner 8-bit dan dioperasikan secara berurutan dengan kunci B1, B2, B3, dan B4 menggunakan XOR.

- **Karakter 'h' (ASCII 104 / biner 01101000)**
  1. XOR dengan B1 = 10110101
  2. XOR dengan B2 = 10110011
  3. XOR dengan B3 = 00000111
  4. XOR dengan B4: 01001000

  Biner 01001000 = Huruf 'H'

- **Karakter 'a' (ASCII 97 / biner 01100001)**
  1. XOR dengan B1 = 11011010

2. XOR dengan B2 = 11010110
3. XOR dengan B3 = 10111110
4. XOR dengan B4 = 00100001

Biner 00100001= Karakter '!'

- **Karakter 'l' (ASCII 108 / biner 01101100)**
    1. XOR dengan B1 = 00011011
    2. XOR dengan B2 = 00000010
    3. XOR dengan B3 = 11010010
    4. XOR dengan B4 = 11101101

    Biner 11101101 = Karakter 'í'

- **Karakter 'o' (ASCII 111 / biner 01101111)**
    1. XOR dengan B1 = 10000001
    2. XOR dengan B2 = 10110010
    3. XOR dengan B3 = 00010011
    4. XOR dengan B4 = 01101100

    Biner 01101100 = Karakter 'l'

Proses enkripsi akan menghasilkan ciphertext "H!íl" sesuai dengan yang ada di kode phyton.

Selanjutnya, Kami akan mendekripsi kembali "H!íl" menjadi “halo” kembali dengan langkah-langkah berikut:

- **Karakter 'H' (ASCII 72 / biner 01001000)**
    1. XOR dengan B4 = 00000111
    2. XOR dengan B3 = 10110011
    3. XOR dengan B2 = 10110101
    4. XOR dengan B1 = 01101000

    Biner 01101000 = Karakter 'h'

- **Karakter '!' (ASCII 33 / biner 00100001)**
    1. XOR dengan B4 = 10111110

2. XOR dengan B3 = 11010110
3. XOR dengan B2 = 11011010
4. XOR dengan B1 = 01100001

Biner 01100001 = Karakter 'a'

- **Karakter 'í' (ASCII 237 / biner 11101101)**
    1. XOR dengan B4 = 11010010
    2. XOR dengan B3 = 00000010
    3. XOR dengan B2 = 00011011
    4. XOR dengan B1 = 01101100

    Biner 01101100 = Karakter 'l'

- **Karakter 'l' (ASCII 108 / biner 01101100)**
    1. XOR dengan B4 = 00010011
    2. XOR dengan B3 = 10110010
    3. XOR dengan B2 = 10000001
    4. XOR dengan B1 = 01101111

    Biner 01101111 = Karakter '0'

Proses dekripsi akan menghasilkan decrypted text "halo" sesuai dengan yang ada di kode phyton.

Kesimpulan

Project ini mengembangkan sistem kriptografi QuadXOR yang menggunakan hash SHA-256 untuk menghasilkan empat blok kunci. Teks asli diubah menjadi biner dan dienkripsi melalui empat tahap XOR berturut-turut. Dengan kunci rahasia "sukabelajardiskrit", proses ini menghasilkan ciphertext yang aman dan bisa didekripsi kembali ke teks asli dengan langkah yang tepat. Sistem yang Kami buat ini menawarkan keamanan tinggi untuk menjaga integritas data.