Cryptography

Anggota Kelompok 7 :
Alicia Juanita Lisal / 0806022310002
Alvin Yuga Pramana / 0806022310004
Jason Bintang Setiawan / 0806022310011

Cryptography adalah ilmu dan seni untuk menjaga kerahasiaan informasi dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Kriptografi digunakan untuk melindungi data agar hanya pihak yang memiliki izin yang dapat mengaksesnya, baik dalam proses komunikasi, penyimpanan data, maupun transaksi elektronik. Tujuan utama kriptografi adalah menjaga kerahasiaan (confidentiality), integritas (integrity), keaslian (authenticity), dan ketersediaan (availability) dari informasi.

- ★ Enkripsi adalah proses mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) dengan menggunakan algoritma tertentu, yang dikenal sebagai cipher. Hasil dari enkripsi adalah ciphertext, yang hanya bisa dipahami jika seseorang memiliki kunci untuk mendekripsinya. Proses ini digunakan untuk melindungi informasi dari akses yang tidak sah.

- ★ Dekripsi adalah kebalikan dari enkripsi. Dekripsi mengubah ciphertext kembali menjadi plaintext yang dapat dipahami. Dekripsi hanya bisa dilakukan jika penerima memiliki kunci yang benar untuk membalikkan proses enkripsi.

Berikut adalah penjelasan mengenai kode enkripsi-dekripsi kami. Dalam contoh ini, password yang dimasukkan adalah ‘grouP7Pass’.

1. **Hashed Key**:
   Dengan menggunakan `secret_key = 'hiddenKey'` untuk membuat *hash* SHA-256 hingga menghasilkan deretan angka panjang yang disebut dengan **Hashed Key**
   Lalu, kita mendapatkan hasil arraynya:
   Hashed key: [123, 239, 12, 255, 65, 45, 37, 162, ...]
   Selanjutnya, berdasarkan kode, kami mengambil indeks 0 - indeks ketiga sebagai nilai dari B1, B2, B3, dan B4 seperti dibawah.
   - ➔ B1 = 123 (01111011)
   - ➔ B2 = 239 (11101111)
   - ➔ B3 = 12 (00001100)
   - ➔ B4 = 255 (11111111)

2. **Konversi Password ke ASCII**:
   Setiap karakter pada password diubah ke nilai ASCII (decimal), lalu diubah lagi ke biner.
   - `g` → 103 → 01100111
   - `r` → 114 → 01110010
   - `o` → 111 → 01101111

- `u` → 117 → 01110101
- `P` → 80 → 01010000
- `7` → 55 → 00110111
- `P` → 80 → 01010000
- `a` → 97 → 01100001
- `s` → 115 → 01110011
- `s` → 115 → 01110011

3. **Langkah Enkripsi**:
   Setiap nilai ASCII di-XOR dengan B1, B2, B3, dan B4 secara berurutan.
   - ➔ Enkripsi `g` (01100111):
     XOR dengan B1 (01111011): 01100111 XOR 01111011 = 00011100
     XOR dengan B2 (11101111): 00011100 XOR 11101111 = 11110011
     XOR dengan B3 (00001100): 11110011 XOR 00001100 = 11111111
     XOR dengan B4 (11111111): 11111111 XOR 11111111 = 00000000

     Ciphertext `g` = 00000000

   - ➔ Enkripsi `r` (01110010):
     XOR dengan B1 (01111011): 01110010 XOR 01111011 = 00001001
     XOR dengan B2 (11101111): 00001001 XOR 11101111 = 11100110
     XOR dengan B3 (00001100): 11100110 XOR 00001100 = 11101010
     XOR dengan B4 (11111111): 11101010 XOR 11111111 = 00010101

     Ciphertext `r` = 00010101

   - ➔ Enkripsi `o` (01101111):
     XOR dengan B1 (01111011): 01101111 XOR 01111011 = 00010100
     XOR dengan B2 (11101111): 00010100 XOR 11101111 = 11111011
     XOR dengan B3 (00001100): 11111011 XOR 00001100 = 11110111
     XOR dengan B4 (11111111): 11110111 XOR 11111111 = 00001000

     Ciphertext `o` = 00001000

   - ➔ Enkripsi `u` (01110101):
     XOR dengan B1 (01111011): 01110101 XOR 01111011 = 00001110
     XOR dengan B2 (11101111): 00001110 XOR 11101111 = 11100001
     XOR dengan B3 (00001100): 11100001 XOR 00001100 = 11101101
     XOR dengan B4 (11111111): 11101101 XOR 11111111 = 00010010

     Ciphertext `u` = 00010010

   - ➔ Enkripsi `P` (01010000):
     XOR dengan B1 (01111011): 01010000 XOR 01111011 = 00101011

XOR dengan B2 (11101111): 00101011 XOR 11101111 = 11000100
XOR dengan B3 (00001100): 11000100 XOR 00001100 = 11001000
XOR dengan B4 (11111111): 11001000 XOR 11111111 = 00110111

Ciphertext `P` = 00110111

➔ Enkripsi `7` (00110111):
XOR dengan B1 (01111011): 00110111 XOR 01111011 = 01001100
XOR dengan B2 (11101111): 01001100 XOR 11101111 = 10100011
XOR dengan B3 (00001100): 10100011 XOR 00001100 = 10101111
XOR dengan B4 (11111111): 10101111 XOR 11111111 = 01010000

Ciphertext `7` = 01010000

➔ Enkripsi `P` (01010000):
Sama seperti proses di atas, hasilnya tetap 00110111.

➔ Enkripsi `a` (01100001):
XOR dengan B1 (01111011): 01100001 XOR 01111011 = 00011010
XOR dengan B2 (11101111): 00011010 XOR 11101111 = 11110101
XOR dengan B3 (00001100): 11110101 XOR 00001100 = 11111001
XOR dengan B4 (11111111): 11111001 XOR 11111111 = 00000110
Ciphertext `a` = 00000110

➔ Enkripsi `s` (01110011):
Sama seperti sebelumnya, hasilnya:
s pertama → 00010100
s kedua → 00010100

4. **Hasil Enkripsi (Dalam Biner)**:
['00000000', '00010101', '00001000', '00010010', '00110111', '01010000', '00110111', '00000110', '00010100', '00010100']

5. **Konversi Hasil Enkripsi Biner ke Karakter**:
Hasilnya dikonversi ke bentuk karakter berdasarkan nilai ASCII dari hasil enkripsi biner:
   - 00000000 → karakter ASCII \x00 (karakter kosong)
   - 00010101 → karakter ASCII \x15
   - 00001000 → karakter ASCII \x08
   - 00010010 → karakter ASCII \x12
   - 00110111 → karakter ASCII 7
   - 01010000 → karakter ASCII P
   - 00110111 → karakter ASCII 7
   - 00000110 → karakter ASCII \x06
   - 00010100 → karakter ASCII \x14

- 00010100 → karakter ASCII \x14

Sehingga, hasil enkripsi karakternya adalah: '\x00\x15\x08\x127P7\x06\x14\x14'
Hasil enkripsi yang diawali dengan `\x` menunjukkan **non-printable characters**, yaitu karakter yang tidak bisa ditampilkan secara langsung atau tidak memiliki representasi visual yang mudah dikenali.

Jadi, dalam string '\x00\x15\x08\x127P7\x06\x14\x14', berikut penjelasannya:

- \x00: Karakter dengan kode ASCII 0, sering disebut sebagai NUL (null character), dan ini adalah karakter kosong.
- \x15: Karakter ASCII dengan kode 21, yang merupakan karakter kendali non-printable.
- \x08: Karakter ASCII dengan kode 8, dikenal sebagai BACKSPACE.
- \x12: Karakter ASCII dengan kode 18, juga karakter non-printable (kendali).
- 7: Karakter ASCII 55, yaitu angka '7', bisa ditampilkan.
- P: Karakter ASCII 80, yaitu huruf 'P', bisa ditampilkan.
- 7: Sama seperti di atas, angka '7'.
- \x06: Karakter ASCII dengan kode 6, dikenal sebagai ACK, non-printable.
- \x14: Karakter ASCII dengan kode 20, juga non-printable.

6. **Proses Dekripsi Bagian I (Konversi ASCII kembali ke Biner)**:
   Setiap karakter enkripsi diubah kembali ke biner:
   - \x00 → 00000000
   - \x15 → 00010101
   - \x08 → 00001000
   - \x12 → 00010010
   - 7 → 00110111
   - P → 01010000
   - 7 → 00110111
   - \x06 → 00000110
   - \x14 → 00010100
   - \x14 → 00010100

7. **Proses Dekripsi Bagian II (Konversi Binerkembali ke Biner)**:
   Untuk mendekripsi, kita menggunakan B1, B2, B3, B4 secara terbalik (mulai dari B4 hingga B1):

   ➔ Dekripsi 00000000 (karakter g)
   XOR dengan B4: 00000000 XOR 11111111 = 11111111
   XOR dengan B3: 11111111 XOR 00001100 = 11110011
   XOR dengan B2: 11110011 XOR 11101111 = 00011100
   XOR dengan B1: 00011100 XOR 01111011 = 01100111

   ASCII: 01100111 = 'g'

➔ Dekripsi 00010101 (karakter r)
XOR dengan B4: 00010101 XOR 11111111 = 11101010
XOR dengan B3: 11101010 XOR 00001100 = 11100110
XOR dengan B2: 11100110 XOR 11101111 = 00001001
XOR dengan B1: 00001001 XOR 01111011 = 01110010

ASCII: 01110010 = 'r'

➔ Dekripsi 00001000 (karakter o)
XOR dengan B4: 00001000 XOR 11111111 = 11110111
XOR dengan B3: 11110111 XOR 00001100 = 11111011
XOR dengan B2: 11111011 XOR 11101111 = 00010100
XOR dengan B1: 00010100 XOR 01111011 = 01101111

ASCII: 01101111 = 'o'

➔ Dekripsi 00010010 (karakter u)
XOR dengan B4: 00010010 XOR 11111111 = 11101101
XOR dengan B3: 11101101 XOR 00001100 = 11100001
XOR dengan B2: 11100001 XOR 11101111 = 00001110
XOR dengan B1: 00001110 XOR 01111011 = 01110101

ASCII: 01110101 = 'u'

➔ Dekripsi 00110111 (karakter P)
XOR dengan B4: 00110111 XOR 11111111 = 11001000
XOR dengan B3: 11001000 XOR 00001100 = 11000100
XOR dengan B2: 11000100 XOR 11101111 = 00101011
XOR dengan B1: 00101011 XOR 01111011 = 01010000

ASCII: 01010000 = 'P'

➔ Dekripsi 01010000 (karakter 7)
XOR dengan B4: 01010000 XOR 11111111 = 10101111
XOR dengan B3: 10101111 XOR 00001100 = 10100011
XOR dengan B2: 10100011 XOR 11101111 = 01001100
XOR dengan B1: 01001100 XOR 01111011 = 00110111

ASCII: 00110111 = '7'

➔ Dekripsi 00110111 (karakter P)
Ini sama seperti langkah 5, jadi hasilnya adalah 'P'.

➔ Dekripsi 00000110 (karakter a)
XOR dengan B4: 00000110 XOR 11111111 = 11111001
XOR dengan B3: 11111001 XOR 00001100 = 11110101
XOR dengan B2: 11110101 XOR 11101111 = 00011010
XOR dengan B1: 00011010 XOR 01111011 = 01100001

ASCII: 01100001 = 'a'

➔ Dekripsi 00010100 (karakter s)
XOR dengan B4: 00010100 XOR 11111111 = 11101011
XOR dengan B3: 11101011 XOR 00001100 = 11100111
XOR dengan B2: 11100111 XOR 11101111 = 00001000
XOR dengan B1: 00001000 XOR 01111011 = 01110011

ASCII: 01110011 = 's'

➔ Dekripsi 00010100 (karakter s)
Proses ini sama seperti langkah 9, hasilnya juga 's'.

Kesimpulan:
Cryptography adalah sistem keamanan yang berperan penting dalam menjaga data dan komunikasi, dengan mengubah sebuah infromasi ke kalimat yang tidak dapat dibaca. Dalama hal ini, terdapat 2 proses yaitu enkripsi dan deskripsi. Enkripsi merupakan sebuah proses untuk mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dibaca (chipertext). Sedangkan, dekripsi adalah kebalikan dari enkripsi yaitu mengubah data dari *ciphertext* menjadi plaintext. Berdasarkan proses enkripsi dan dekripsi menggunakan teknik XOR dan kunci B1-B4 hasil hashing secret key berjalan dengan benar, dan setelah dekripsi, kita berhasil mendapatkan kembali password aslinya dalam bentuk biner dan teks.