

Group 5:

1. Deny Wahyudi Asaloei
2. A. Alfian Tenggara Putra
3. Juan Daniel Titarsole

XOR Layered Cryptosystem

Sistem kriptografi ini menggunakan metode enkripsi berbasis operasi XOR berlapis-lapis dengan empat kunci biner (B1, B2, B3, dan B4) yang dihasilkan dari satu *secret key* melalui fungsi hash MD5. Setiap kunci digunakan secara berurutan untuk melakukan operasi XOR terhadap data plaintext, menciptakan ciphertext.

Proses enkripsi dimulai dengan plaintext yang dikonversi menjadi bentuk integer. Selanjutnya, integer ini dioperasikan dengan XOR bersama empat kunci biner secara berurutan. Dekripsi membalikkan proses tersebut dengan urutan yang sama, sehingga berubah kembali menjadi plaintext asli dari ciphertext.

Sistem ini sederhana namun cukup aman karena menggunakan operasi XOR dengan beberapa lapisan kunci yang diperoleh dari satu secret key.

Contoh Cara Kerja dari Enkripsi hingga Dekripsi:

1. Plaintext: "Hello"
2. Secret Key: "kunci"

Langkah Enkripsi:

1. Plaintext "Hello" dikonversi menjadi integer A.
2. Hash MD5 dari secret key "kunci" dihasilkan dan diambil empat byte pertama sebagai kunci biner B1, B2, B3, dan B4.
3. Integer A di-XOR secara berurutan dengan B1, B2, B3, dan B4 untuk menghasilkan ciphertext C.

Langkah Dekripsi:

1. Ciphertext C diambil.
2. C di-XOR kembali dengan kunci B4, B3, B2, dan B1 secara terbalik untuk mendapatkan kembali nilai A (plaintext dalam bentuk integer).
3. Integer A dikonversi kembali menjadi string, menghasilkan plaintext asli, yaitu "Hello".