Lab 1 – Nguyễn Thị Thu Hà - 1411010

Part 1:

1. Plaintext 10100010
2. Key 0111111101
3. IP 00110001
4. FK1 10100001
5. SW 00011010
6. Fk2 00101010
7. IP-1  00111000

* Cyphertext: 00111000

Phân tích:

|  |  |  |
| --- | --- | --- |
| Mode | Ưu điểm | Nhược điểm |
| ECB | * Dùng cho các mẩu tin nhỏ * Mã hóa độc lập nên cập nhật dữ liệu từng phần dễn dàng | * Dễ tấn công replay với các mẩu tin giống nhau, mã hóa sẽ giống nhau |
| CBC | * Ngăn chặn cắt xén mẩu tin * Các khối mã phụ thuộc chặt chẽ với nhau và với plaintext * Ngăn chặn tấn công relplay | * IV cân được gửi một cách bí mật |
| CTR | * Xử lý song song, có thể tiền xử lí * Không có sự phụ thuộc lẫn nhau nên cho phép truy chập ngẫu nhiên * Hiệu năng tính toán nhanh | * Phải tin tưởng không bao giờ dùng lại khóa/đếm, nếu không có thể bẻ |
| OFB | * Giống Cho phép mã hóa các khối nhỏ * Tăng tốc độ tính toán | * Người gửi và người nhận phải đồng bộ, có phương pháp khôi phục. |