# 정보보호 Homework 03 201204025 김대래 담당 교수 : 류재철 과목 : 정보보호 분반 : 00 분반

## Index

|  |  |
| --- | --- |
|  | Page |
| Index | 2 |
| 과제 개요 | 3 |
| 과제\_1 XOR 암호(XOR Cipher) | 4 |
| 과제\_2 무차별 대입공격 (Brute-Force Attack) | 6 |
| 결과 화면 | 8 |

개발 환경

OS: Linux Ubuntu – Virtual Box

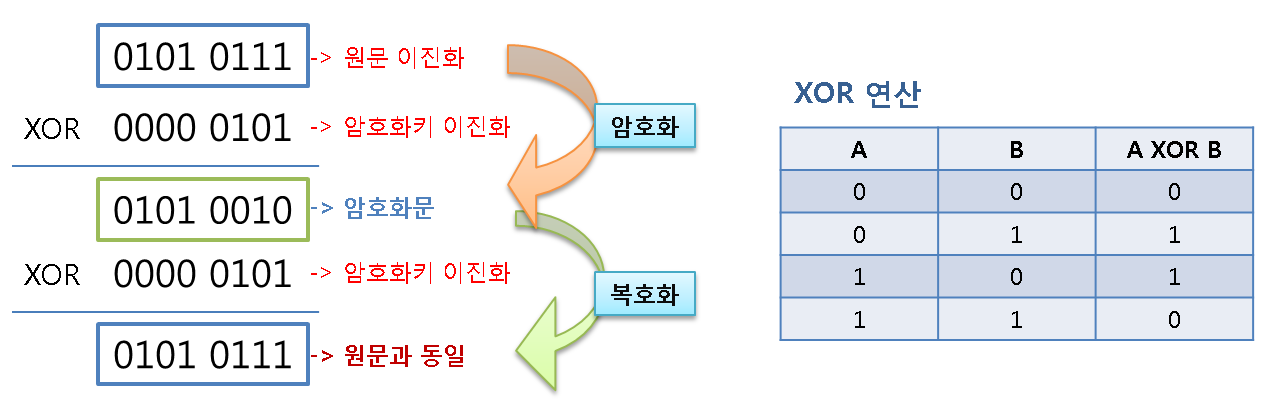
Language: C

Tool: vim

## 과제 개요

* 과제\_1 XOR 암호(XOR Cipher)

XOR 암호는 암호화하고자 하는 내용(평문: plaintext)을 글자마다 16진수로 나타낸 hex 코드를 키(Key) 값에 따라 XOR(비트연산) 하여 다른 알파벳으로 치환하는 방식의 암호이다.



* 과제\_2 무차별 대입 공격(Brute-Force Attack) 구현

무차별 대입 공격(Brute-Force Attack)은 특정한 암호를 풀기 위하여 가능한 모든 값들을 대입해보며 key값을 찾는 방식의 공격방법이다.

## 과제\_1 XOR 암호(XOR Cipher)

* **문제 개요**
* 문제: 평문 또는 암호문과 모드, 키 값을 입력하여 모드에 따라 키에 따른 암호문 또는 평문을 출력한다.
* 평문 예시: Hello Security
* 입력 예시: >> Input File Name : plain.txt  
   >> Input Mode [ 0 : Encrypt, 1 : Decrypt ] : 0  
   >> Input Key : sky
* 출력 예시: ;....y .......s (16진수로 확인하는 xxd 명령어 이용)
* **문제 해결 과정**
* **과정\_1 Encrypt**

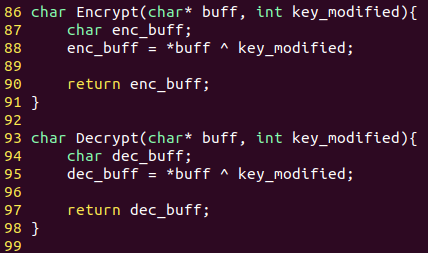
Key 값을 평문(plaintext)길이 만큼 반복하기 위한 인자 key\_modified 이용

* **과정\_2 Encrypt - XOR**

Buff 를 XOR 하기 위한 비트연산자 ^ 이용

* **과정\_3 Decrypt**

Encrypt의 반대 개념이지만 XOR의 경우 동일한 ^ 연산자를 통해 복호화 가능

* **소스 코드**
* **Encrypt / Decrypt**
* ****암호화된 결과를 반환할 char형 변수 enc\_buff 선언
* Plaintext의 일부(글자)인 buff와 key의 반복 위치인 key\_modified를 xor연산을 위한 비트 연산자(^)를 enc\_buff에 저장하여 반환

## 과제\_2 무차별 대입 공격(Brute-Force Attack)

* **문제 개요**
* 문제: 두 개의 무작위 수 a, b(1≤ a, b ≤100)의 곱에 대하여 입력 값에 따른 정/오답 결과 출력.
* 입력 예시: >> a \* b = ?  
   >> Input : ans
* 출력 예시: [?] ans is not answer

[!] Great Job~!

* **문제 해결 과정**
* **과정\_1 무작위 수 생성**

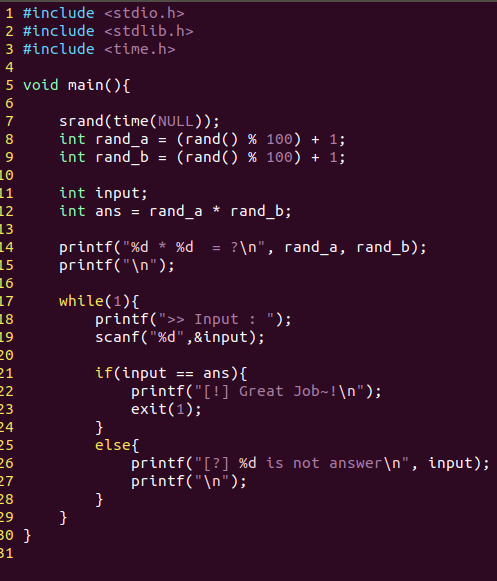
rand() 함수를 이용하여 무작위 수를 생성해 주고 % 연산으로 범위를 지정

* **과정\_2 실행할 때 마다 새로운 무작위 수를 생성**

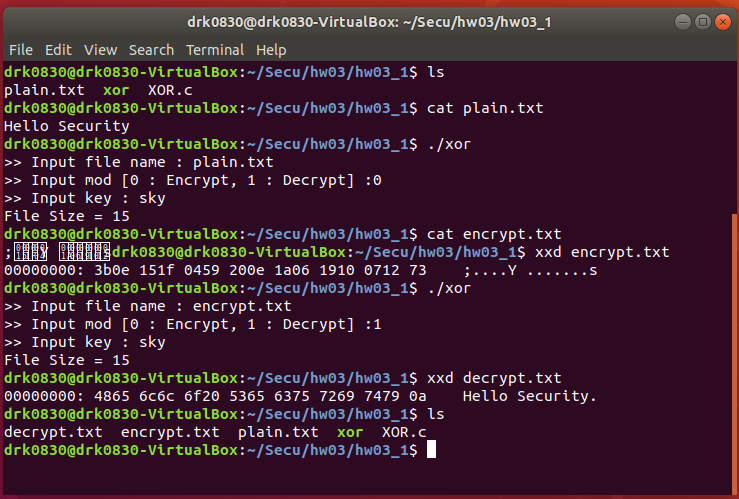
<time.h> 헤더를 include 하여 time() 함수를 사용, srand() 함수를 통해 실행 시 마다 새로운 수 생성

* **과정\_3 입력 값에 따른 답변 출력**

정답일 때 까지 반복을 실행하며 입력 값에 따라 정답 혹은 오답을 출력

* **소스 코드**
* **Encrypt**
* ****<stdlib.h> 표준 라이브러리 헤더를 참조하여 rand() 함수와 srand()함수를 사용
* <time.h> 헤더를 참조하여 time()함수 사용 – 난수 초기화를 위하여
* 1~100 사이의 범위의 난수를 생성
* Ans에 난수 a와 b의 곱을 저장
* 입력 값에 따라 정답과 오답의 결과를 출력
* 만약 정답일 시 프로그램 종료

## 결과 화면

* **과제\_1 XOR 암호**
* **과제\_2 비제네르 암호**

