2021 국민대학교 정보보안암호수학과 암호분석경진대회

1번 문제 - 고전 암호 (출제: CaS, CO2, PEPSI)

정암수 학술동아리 CaS, CO2, PEPSI가 연합하여 암호 CCP를 만들었다! 해당 암호의 암호화 알고리즘은 메시지 M과 키 K를 입력으로 하며, 키 K의 범위는 다음과 같이 정의된다.

$$CCP\_Enc(M, K) = C_K, \qquad K \in [0x30, 0x39]$$

또한 해당 암호화 알고리즘의 출력 값 C_K는 입력 메시지 M과 길이가 같은 특징을 가지고 있다. CCP_Enc의 연산 방식은 다음의 비트열에서 힌트를 얻을 수 있다.

[CCP_Enc 연산 방식 힌트]

01010010
01001001
01000111
01001000
01010100
01010010
01101111
01110100
01100001
01110100
01001001
01101111
01101110

[문제 (100점)]

CCP 암호화 알고리즘의 연산 방식을 서술하고, 해당 알고리즘의 입력으로 특정 메시지 M과 키 $0x39$를 넣어 출력된 암호문 C_{0x39}가 다음과 같이 표현될 때, 해당 암호문을 복호화하여 숨겨진 문장을 복구하시오.

[암호문 C_{0x39}]

0001 0000

1010 0100

0011 0010

1011 0110

0011 0110

0011 0111

1010 1011

1011 0111

1011 1001

0011 0110

0011 0010