3번 문제 답안

정답)

Recommendations for preventing novel coronavirus infection
1. Wash your hands with soap and running water.
2. Cover your mouth with your sleeve when coughing!
3. If you experience respiratory symptoms such as cough, must wear a mask.
4. Inform medical staffs of your travel history when visiting selected clinics.
5. Consult with your local public health center or call '1339' or 'Area Code+120' if you are suspicious of contract an infectious disease.

풀이)

1. 개요

1.1 블록암호 운영모드 암호화 과정

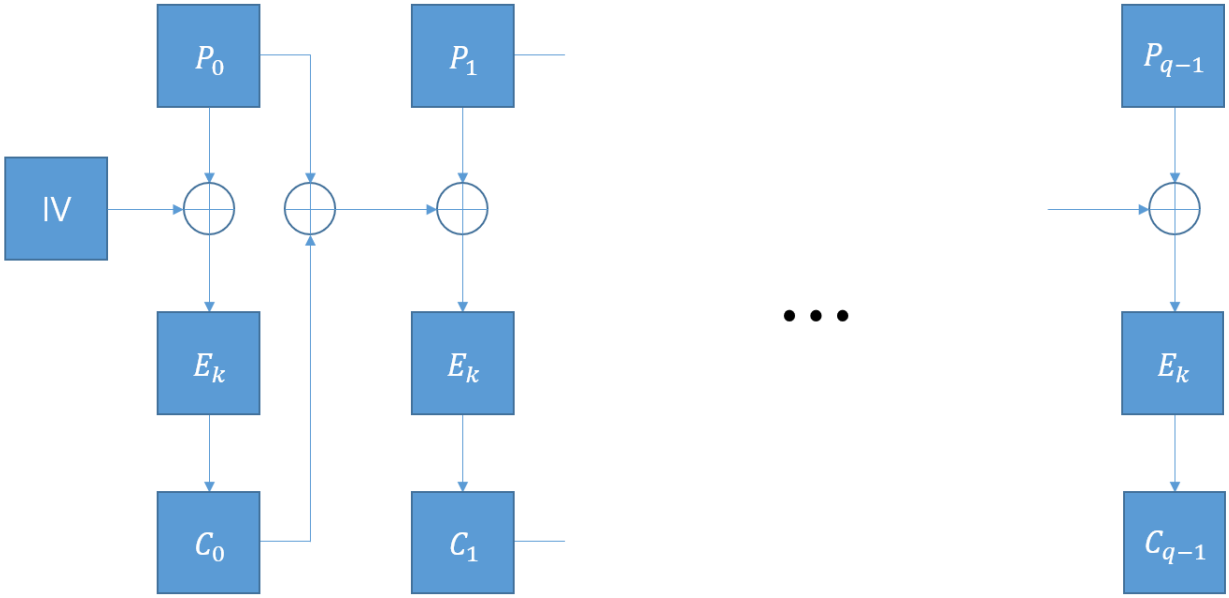
입력: 평문 P
출력: 암호문 C

1. $P = \{P_0, P_1, P_2, \ldots, P_{q-1}\}$, q는 입력된 평문 블록 수
2. $G_0 = IV$
3. for i in $(0, q-1)$:
4. $\quad C_i = E_K(P_i \oplus G_i)$
5. $\quad G_{i+1} = P_i \oplus C_i$
6. return $C = \{C_0, C_1, C_2, \ldots, C_{q-1}\}$

< 그림 1. 블록암호 운영모드 암호화 과정 pseudo-code >

문제에서 주어진 블록암호 운영모드 암호화 과정을 pseudo-code로 나타내면 <그림 1>과 같다.

3번 문제 답안



< 그림 2. 블록암호 운영모드 암호화 과정 >

문제에서 주어진 블록암호 운영모드 암호화 과정을 그림으로 나타내면 <그림 2>와 같다.

1.2 패딩 수행 과정

입력: 평문 P
출력: 패딩이 수행된 평문 P^*

1. $P = \{P_0, P_1, P_2, \dots, P_{t-1}\}$, t는 입력된 평문 블록 수
2. $n = 16$
3. if $(ByteLength(P_{t-1}) < n)$ {
4. $P_{t-1} = P_{t-1} || 80 || 00^{n-ByteLength(P_{t-1})-1}$
5. $P^* = \{P_0, P_1, P_2, \dots, P_{t-1}\}$ }
6. else $(ByteLength(P_{t-1}) = n)$ {
7. $P_q = 80 || 00^{n-1}$
8. $P^* = \{P_0, P_1, P_2, \dots, P_{t-1}, P_t\}$ }
9. return P^*

< 그림 3. 패딩 수행 과정 pseudo-code>

문제에서 주어진 패딩 수행 과정을 pseudo-code로 나타내면 <그림 3>과 같다. 입력된 평문의 마지막 블록이 16바이트보다 작다면 80을 이어붙이고 남는 바이트만큼 00을 이어 붙인다. 만약 입력된 평문의 마지막 블록이 16바이트라면, $80||00^{15}$을 뒤에 이어 붙인다.

3번 문제 답안

그리고 문제에서는 입력된 암호문에 대해 복호화 된 결과에 대한 패딩 형식이 올바른지에 대한 판별 결과를 얻을 수 있다.

2. 방법

암호문에서 첫 블록을 보자. 그 블록과 문제에서 주어진 IV를 가지고 API를 이용하면, 반환 값 INVALID를 얻을 것이다. 만약 IV에서 제일 끝 바이트를 0x00~0xff까지 하나씩 넣어본다면, 이 중 하나가 VALID 값이 나올 것이다. 왜냐하면 복호화를 진행했을 때 복호화 된 평문의 제일 끝 바이트가 0x80이 되는 경우가 있을 것이기 때문이다. 이는 올바른 패딩이기 때문에 VALID를 반환할 것이다. 이를 통해 $IV \oplus P_0$의 제일 마지막 바이트를 알아낼 수 있다.

그 다음 바이트를 알아내려면 P_0의 마지막 두 바이트가 0x8000이 되어야 한다. 지금 현재 $IV \oplus P_0$의 마지막 바이트 값을 알고 있으므로 P_0의 마지막 바이트를 0x00으로 만들기 위한 IV 값을 조작할 수 있다 ($\because IV \oplus P_0 \oplus P_0 = IV$). 이렇게 IV의 제일 마지막 바이트를 설정하고 그 다음 바이트의 P_0가 0x80이 되게 하는 IV 값을 찾으면 된다. 이를 통해 $IV \oplus P_0$의 뒤에서 2번째 바이트 값을 알아낼 수 있다.

위 과정을 반복하면 모든 $IV \oplus P_0$ 값을 알 수 있다. $IV \oplus P_0$와 IV를 알고 있으므로 P_0도 알 수 있다. 다음 블록부터는 IV 값 대신 앞에 블록의 평문과 암호문의 xor 값을 넣어주면 되고 나머지 과정은 같다.

3. 복호화

2의 방법으로 복호화하여 나온 값을 아스키코드로 변환하면, 아래 평문을 얻을 수 있다.

Recommendations for preventing novel coronavirus infection
1. Wash your hands with soap and running water.
2. Cover your mouth with your sleeve when coughing!
3. If you experience respiratory symptoms such as cough, must wear a mask.
4. Inform medical staffs of your travel history when visiting selected clinics.
5. Consult with your local public health center or call '1339' or 'Area Code+120' if you are suspicious of contract an infectious disease.