2020년 1학기
정보보호이론 과제 10번 (기말)
출제: 6/16(화)
마감: 6/23(화) 23시59분

※ 풀이 과정을 자세히 쓰고, 마감 시간을 꼭 지키시오

(1) AES의 MixColumns에서는 irreducible polynomial=$x^8+x^4+x^3+x+1$인 $GF(2^8)$을 사용한다. ?를 계산하시오.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

×

63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C9
D4	FA	63	82

=

?			

(2) RSA에서 $p=11$이고 $q=5$일 때, 공개 키 e와 개인 키 d가 될 수 있는 쌍이 여러 있다. e가 작은 것부터 세 쌍 (e와 d)을 구하시오.

(3) 1부터 10인 쓰인 10면 주사위를 3번 던져 3개의 수를 빨간색으로 적었다. 다시 3번을 던져 3개의 수를 파란 색으로 적었다. 빨간 수와 파란 수에 같은 수가 공통으로 들어 있을 확률을 구하시오. (소수점 아래 다섯 째 자리에서 반올림하여 넷째 자리까지 쓸 것)

(4) 소수 $p=11$, primitive root $g=6$일 때, Diffie-Hellman key agreement에서
① 6이 primitive root임을 보이시오
② A의 공개정보 $R_1=9$이면, A의 개인정보 x는 무엇인가?
③ B의 공개정보 $R_2=3$이면, 공유비밀 값 K는 무엇인가?

※ 다음 페이지에 계속 됨

(5) 강의 시간에 배운 대로 다음 함수는 $y = a^x \bmod n$을 계산한다. x의 비트를 오른쪽에서 왼쪽으로 읽는다.

```
square_and_multiply(a,x,n)
{
  y←1
  for (i←0 to n_b − 1)
  {
   if (x_i = 1) y←a × y mod n
   a←a^2 mod n
  }
  return y
}
```

비슷하지만 약간 다른, 다음 함수도 $y = a^x \bmod n$을 계산하는데, x의 비트를 왼쪽에서 오른쪽으로 읽으면서 계산한다.

① 두 개의 네모 안에 알맞은 문장을 쓰시오.

```
square_and_multiply(a,x,n)
{
  y←1
  for (i←n_b − 1 to 0)
  {
    [                    ]
    [                    ]
  }
  return y
}
```

② ①의 방법에 따라 $y = 7^{37} \bmod 11$를 계산하는 과정을 보이시오.

※ 과제 작성 주의사항

- 과제를 종이에 쓸 것. 괄호번호 (1), (2), (3), ... 순서대로 풀 것. **풀이 앞에 괄호번호를 꼭 쓰고**, 문제를 못 푼 경우라도 그 문제의 괄호 번호는 꼭 써 놓을 것.

※ 과제 제출

- 손 글씨로 푼 것을 사진 찍어, pdf파일로 변환해서, e-Class에 온라인 제출.
- 파일명에 자기의 이름과 학번을 꼭 넣어서 **홍길순202012345** 과 같이 해주세요.
- 사진이 여러 장이더라도 모두 연결해서, 파일 1개만 제출하세요.