2020년 1학기
정보보호이론 과제 1번
출제: 4/2(목)
마감: 4/9(목) 23시59분

(1) 세 집합 Z, Z_n, Z_n^*에 대해서 각각 설명하시오.

(2) Extended Euclidean algorithm을 이용하여 아래 숫자 쌍에 대하여 최대공약수(gcd)와 s값, t값을 구하시오.

(a) 291과 42
(b) 4와 7

(3) 평문 하나를 암호 하여 암호문을 얻었다. 이 평문의 한 글자를 다른 글자로 바꾸어 암호하면, 암호문에서는 최대 몇 글자가 바뀔까?

(a) additive cipher
(b) Vigenere cipher
(c) Auto-key cipher

※ 숙제 작성 주의사항
- 숙제를 종이에 쓸 것. 괄호번호 (1), (2), (3), ... 순서대로 풀 것. **풀이 앞에 괄호 번호를 꼭 쓰고**, 문제를 못 푼 경우라도 그 문제의 괄호 번호는 꼭 써 놓을 것.

※ 숙제 제출
- 종이에 푼 것을 사진 찍어, pdf파일로 변환해서, e-Class에 온라인 제출