종합시험 안내	**암호기술과 응용**	시험시간: 90분

☆☆☆ Open Book, Open Lecture Note ☆☆☆

☞ 출제범위: 교재 2장 ~ 15장 (단, 3장은 제외)
- 암호학과 네트워크 보안, 손승원, 이재광, 임종인, 전태일 공역, 한국맥그로힐(주), 2008년
- 원서 : Cryptography and Network Security, Behrouz A. Forouzan, McGraw Hill
- 2019년 1학기부터 3장이 추가로 포함되었으나, 종합시험 응시대상자에 2018학년도 이전 수강생이 포함되어 있으므로 3장을 시험 범위에서 제외함

☞ 문제유형, 예시와 배점:

※(1~5) 다음 문장의 내용이 맞으면 ○표, 틀리면 ✗표를 답하시오. [3점×5문항=15점]

- $GF(2^4)$에서 x^3+x+1의 모듈로 x^4+x+1 곱셈에 대한 역원은 x^2+1 이다

  [정답] ○

※(6~10) 다음 괄호에 알맞은 값이나 용어를 채워 넣으시오. [3점×5문항=15점]

- 한 메시지가 1500비트로 구성되고 만약 64비트 블록암호를 사용한다면, 마지막 메시지 블록에 덧붙여야 할 비트 수는 ( ) 비트 이다.

  [정답] 36

- ( ) (이)란 $y=f(x)$에서 f는 계산이 쉽지만 f^{-1}은 계산이 어려운 함수로서, 특히 y값과 트랩도어(비밀)을 알면 x값을 쉽게 계산할 수 있는 함수를 말한다.

  [정답] 트랩도어 일방향 함수(trapdoor one-way function)

※(11~15) 각각의 용어의 개념이나 정의를 100자 내외로 간단히 설명하시오. [6점×5=30점]

- 아핀 암호(affine cipher)

  [정답] (ax+b) mod 26에 기반(덧셈암호와 곱셈암호를 함께 사용)한 단일 문자 치환 암호

※(16~20) 각각의 질문에 대하여 계산 과정과 함께 결과 값을 구하거나, 최대 200자 이내로 답하시오. [8점×5=40점] (단, 오답이라도 계산 과정이나 일부 설명에 대한 부분점수는 부여 가능)

- 3과 7로 나누었을 때 나머지가 2이고, 10으로 나누었을 때 나머지가 8인 정수를 구하여라.

  [정답] 128 (mod 201) **단, 정답이 틀리더라도 풀이 과정에 대한 부분점수 부여 가능**

- 비밀메시지 전달이라는 관점에서 암호(cryptography)와 스테가노그래피(steganography)의 차이점이 무엇인지 설명하여라.

  [정답] 암호는 메시지의 내용을 읽을 수 없게 하는 수단으로서 메시지 노출 방지가 목적인 반면에 스테가노그래피는 메시지 존재 자체를 숨기기 위한 메시지 은닉 기술을 말한다.