

## 정보개 중간 정리(존역세때)

### 1. 진법계산으로 5문제

1. 1
2. 2
3. 3
4. 4
5. 5

**십진수 : 925**

**2진수 :**

**8진수 :**

**16진수 :**

1.

2. 시스템 메모리 강조 부분 ( 4가지로 나뉨 ) - 주관식
  1. 코드 영역 : 실행할 프로그램의 명령어 저장

2. 데이터 영역 : 전역 변수, 정적변수 저장
3. 힙(Heap)영역 : 동적으로 생성된 데이터 저장
4. 스택(Stack) 영역 : 함수 호출 시 데이터 저장

[맞는지 확인필요]

### 3. hdd와 sdd 데이터 복구 ? 땜에 어렵다고 함

1. SSD는 전기적 신호로 데이터를 쓰고 지우며, 데이터를 관리하는 방식이 HDD와 다르기 때문에 데이터 복구에 특별한 어려움이 있음 . SSD는 성능을 최적화하기 위해 Garbage Collection이라는 기능을 사용 . 이 기능은 불필요한 데이터(예: 사용자가 삭제한 파일)를 자동으로 지우고 빈 공간으로 만들기 때문에, 데이터 복구를 어렵게 만든다 . TRIM 명령은 SSD의 성능을 유지하기 위해 운영체제가 삭제된 데이터의 위치를 SSD에 알려주는 기능

### 4. 트로이목마 종류

1. (6주차)
2. sub7 -백도어형
3. GameThief - 게임 계정 탈취용
4. FAke Antivirus - 가짜 백신 pg
5. 백도어 트로이목마 - 원격 접속
6. 뱅킹 트로이목마 - 온라인 결제시
7. 다운로더 트로이 목마 - 스스로 피해 주지 X , 다른 악성코드를 컴퓨터에 몰래 다운로드하고 설치하는 역할
8. DDoS트로이목마 - 좀비 컴퓨터
9. 가짜 백신 트로이 목마 - 진짜 백신마냥
10. 랜섬 트로이 목마 - 암호화 하여 사용 못하게
11. SMS 트로이 목마 - 스마트폰에 침투 후 문자 보내거나 가로채는
12. 게임시프 트로이 목마 - 온라인 개인 개인정보
13. 메일 파인더 트로이 목마 - 이메일 주소록 수집
14. 트로이 목마 스파이 - 컴퓨터 감시 후 정보 수집

### 5. 저번주 한 것

1. 단일 치환 암호화
2. RSA 알고리즘 깨질 수 있음 > 소인수분해
3. 암호문이 나오는게 아니라 뭔 숫자가 나옴
4. DES 알고리즘 - 비밀키 사용 후 복잡한 방식으로 바꿔줌
  1. 64비트 평문을 54비트 암호화로 사용
  2. 16번 반복
  3. XOR연산
5. 트리플 DES
  1. 2개의 암호화 키 이용

## 6. 비대칭 암호화

1. RSA - 소수 2개를 만든다. 큰 수 & 소수여야함.
2. RSA - 복호화 - 작은수 사용
  1. 암호화 할 때  $p$   $q$   $N$  알고 있어야함