

컴퓨터보안 실습

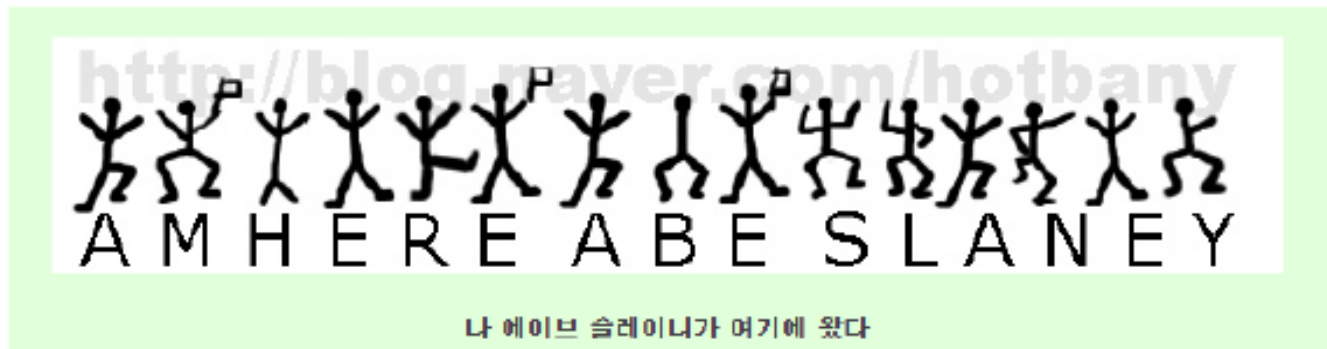
CIA(기밀성, 무결성, 가용성)

컴퓨터보안 실습

- **컴퓨터 보안**은 컴퓨터의 안전과 직결되며 컴퓨터를 기반으로 하는 시스템들의 취약점들을 파악하는 것은 가동 산업을 유지시키는 데 중요한 역할을 함
- 이론 컴퓨터 시스템과 실제 컴퓨터 시스템에 적용되는 정보 보안의 하위 분류인 동시에 컴퓨터의 운영에서 보안의 강화를 말하는 컴퓨터 과학의 하위 분류를 말함
- 정보보안의 고전 암호부터 시작하여 현대 보안의 해킹 및 보안 실습을 진행함
- 정보를 보안하기 위해 셜록 홈즈 소설에 등장하는 고전 암호를 알아내며 기밀성, 무결성, 가용성에 각 분류를 실습함

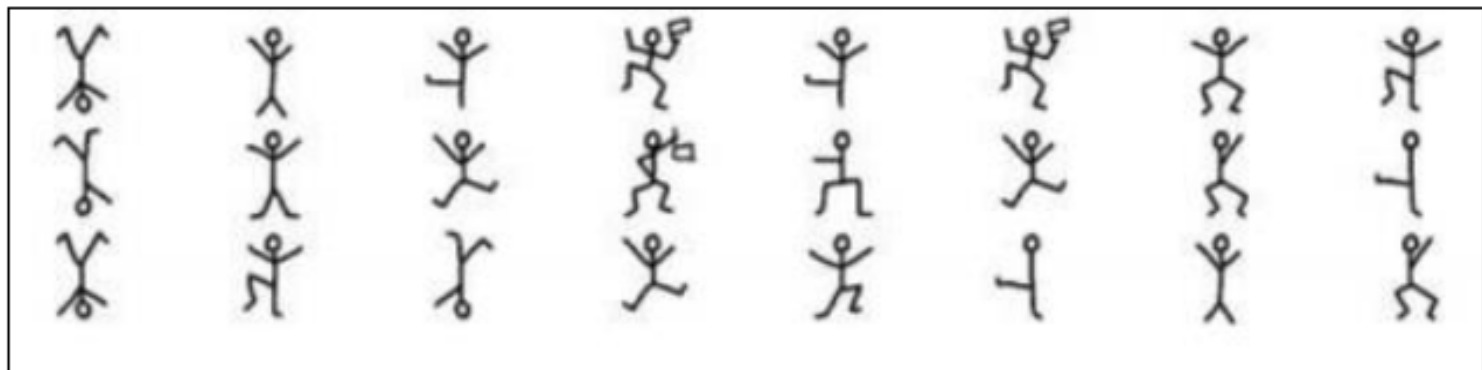
대치 암호

- 춤추는 사람 인형



- <http://blog.naver.com/PostView.nhn?blogId=thdgnstjs&logNo=50077677206>

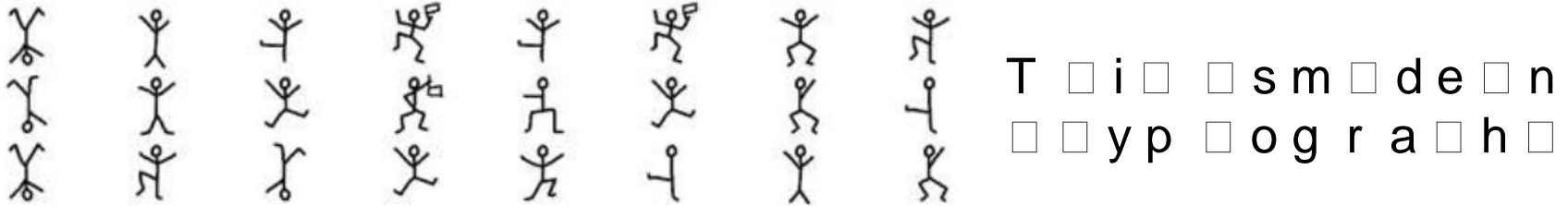
- 실습 : 아래 그림을 복호화



컴퓨터보안 실습

[첫번째] Confidentiality, 기밀성 (실습)

- 기밀성은 암호화와 밀접한 관계가 있음 (춤추는 사람 그림 암호)



[두번째] Integrity, 무결성 (실습, <http://www.convertstring.com/ko/Hash/MD5>)

- 해시함수(실습하는 MD5 Sum 외에도 수 많은 Hash function 프로그램이 존재) 는 역산, 충돌에 안전해야한다.



[세번째] Availability, 가용성

- 가용성을 해치기 위한 주요 공격 위협으로는 DoS (Denial of Service)가 있음.

- DoS 공격에 대해 알아본다

Q & A