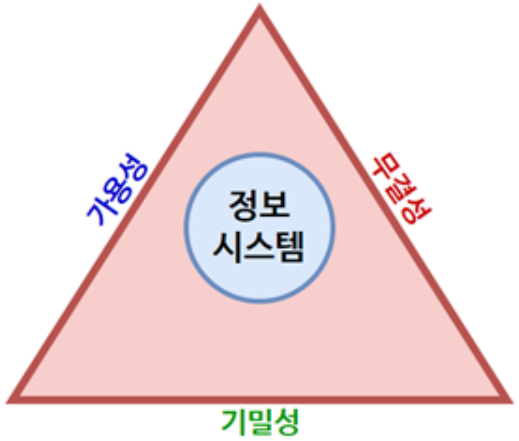
정보보호론 실습

1. CIA(기밀성, 무결성, 가용성)

정보보호론 실습



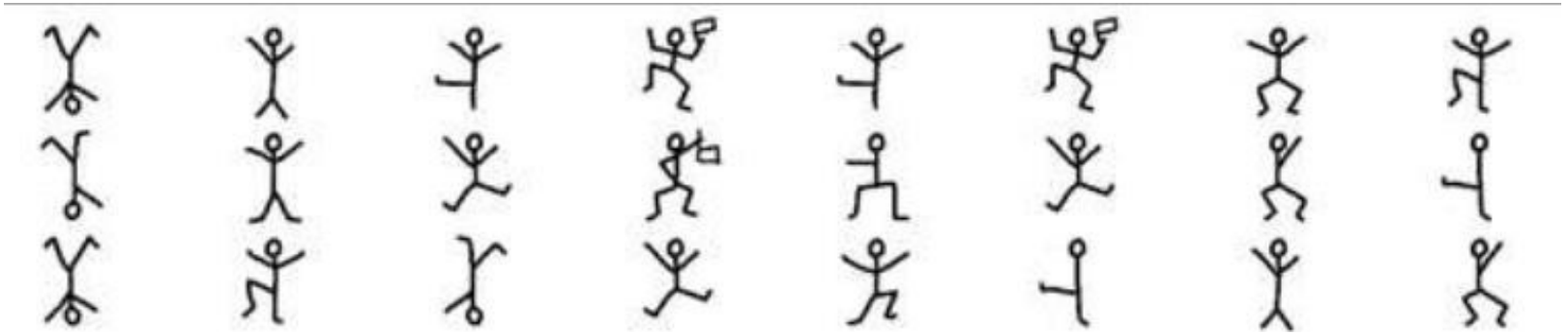
- **컴퓨터에 대한 보안**은 컴퓨터의 안전과 직결되며 컴퓨터를 기반으로 하는 시스템들의 취약점들을 파악하는 것은 가동 산업을 유지시키는 데 중요한 역할을 함

- 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

1. 기밀성 – 춤추는 사람 그림 암호

[첫번째] Confidentiality, 기밀성 (실습)
-기밀성은 암호화와 밀접한 관계가 있음 (춤추는 사람 그림 암호)



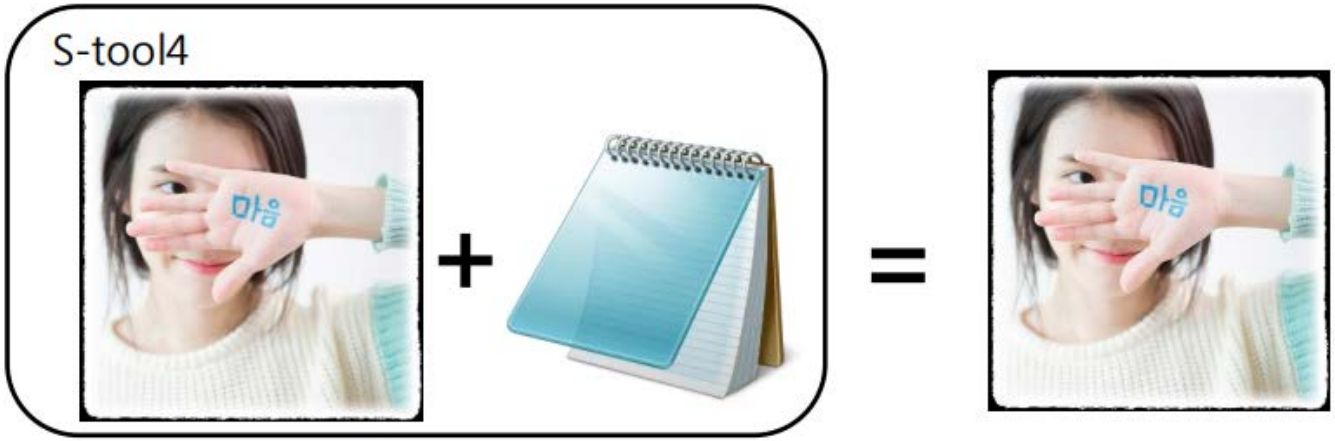
T □i□ □s m□d e□n
□ □y p□o g r a□h□

실습 1번 : 해당 문장 전체를 완성

2. 기밀성 - 스테가노그래피

[두번째] Confidentiality, 기밀성 (실습)

스테가노그래피 툴



이미지 파일

텍스트 파일
(암호화를 위한 메시지)

비트맵(BMP)
형식 그림파일

툴 다운로드 : https://packetstormsecurity.com/files/download/21688/s-tools4.zip

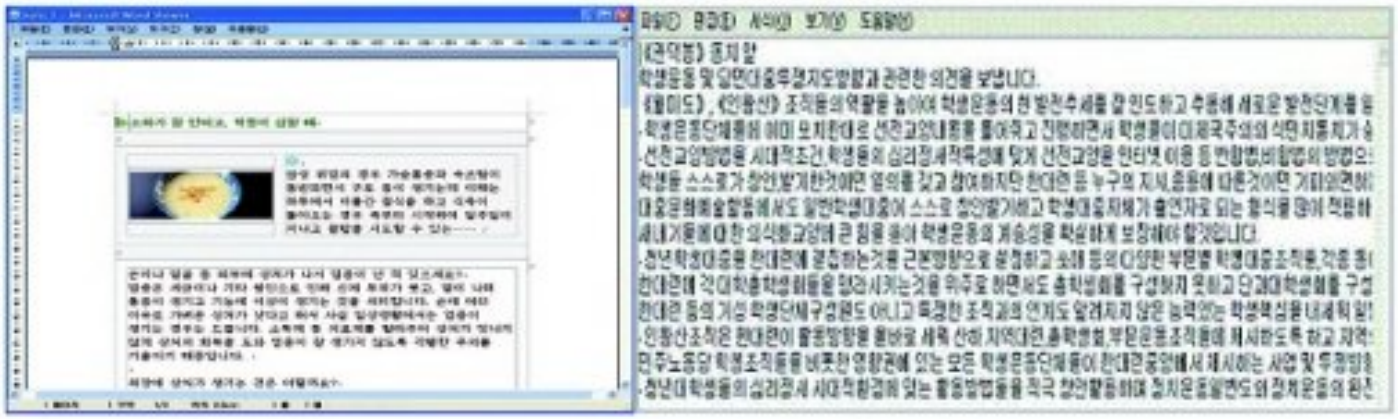
이미지 다운로드 :

2. 기밀성 - 스테가노그래피

스테가노그래피란?

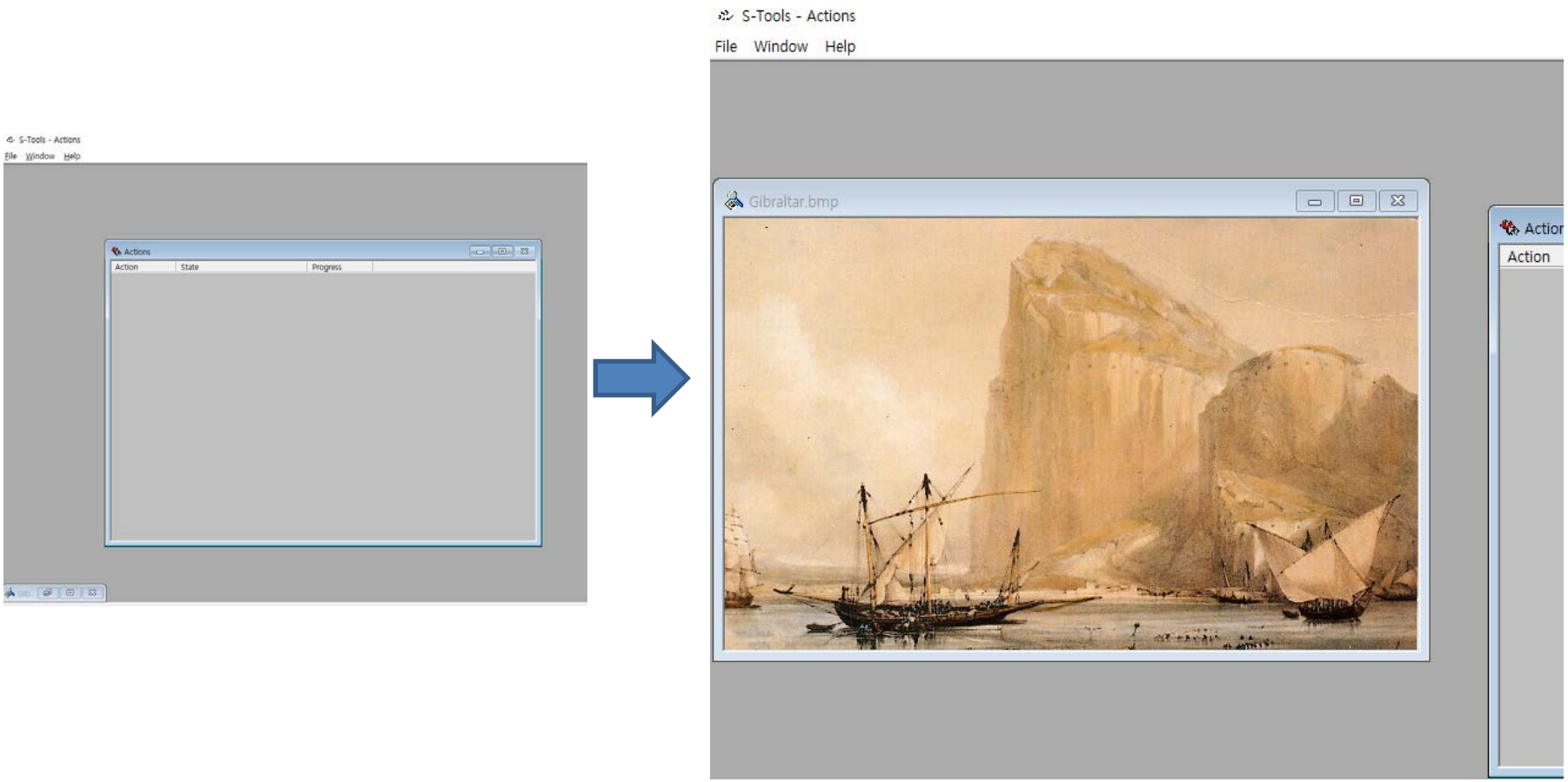
- 그리스어로 "감추어져있다"라는 뜻인 "stegano"와 그리스어로 "쓰다, 그리다"라는 뜻인 "graphos"의 합성어로, "감추어쓰다"라는 의미
- 암호화가 아닌 단순히 정보를 숨기는데 목적
- 이미지, 영상 파일등의 디지털 포맷에 메시지를 숨기는 방법
- 이미지 자체를 변조시켜 데이터를 숨기는 기법도 존재
- 인간의 인식 능력의 한계를 이용한 프레임, 화소단위에서 데이터 조작 가능
    - 이미지는 7%, 영상은 24프레임 범위 내에서 데이터 조작 가능

2. 기밀성 - 스테가노그래피



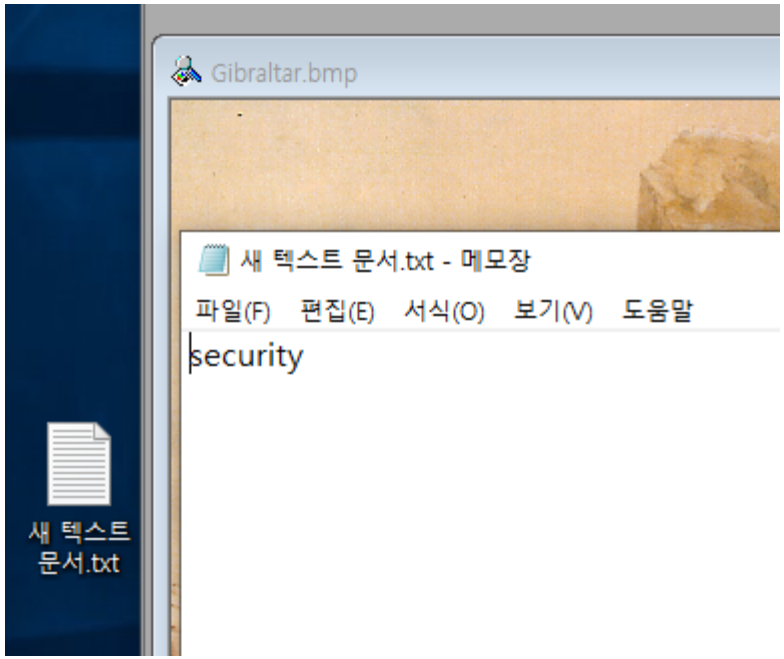
911테러, 왕재산 사건에 사용

2. 기밀성 - 스테가노그래피



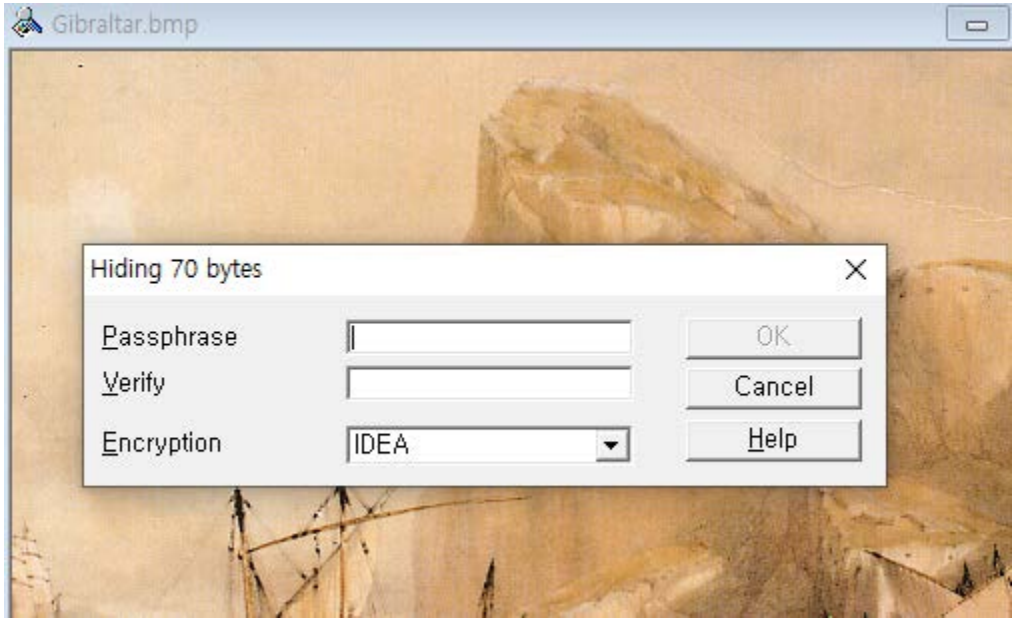
1. 준비한 사진파일을 S-tool4에 Drag & Drop

2. 기밀성 - 스테가노그래피



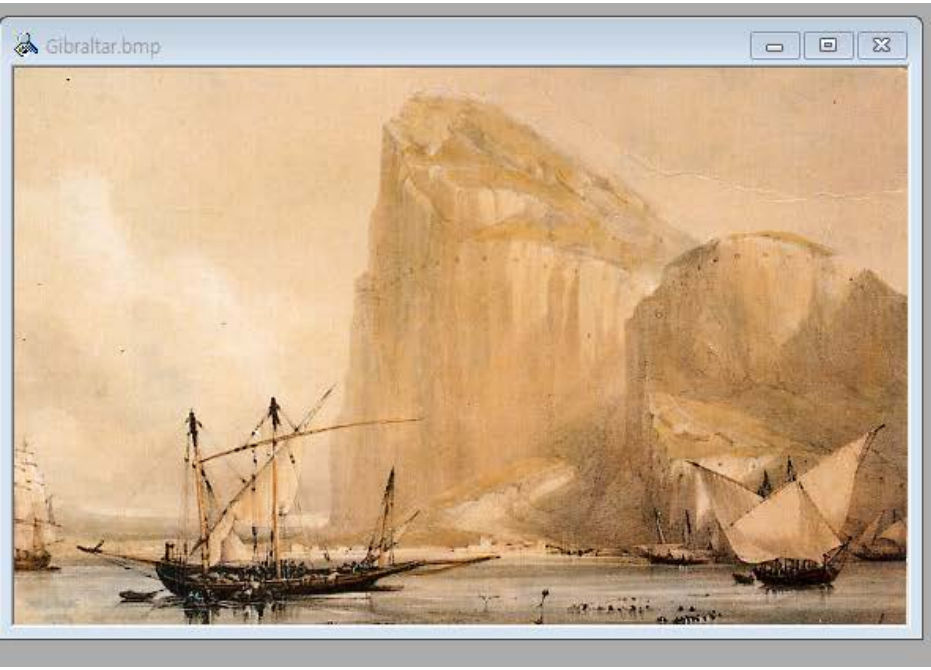
2. Notepad에 입력한 숫자 및 글자를 저장하고 txt파일을 그림에 Drag & Drop

2. 기밀성 - 스테가노그래피



3. 암호키와 암호방식을 선택한 후 OK

2. 기밀성 – 스테가노그래피

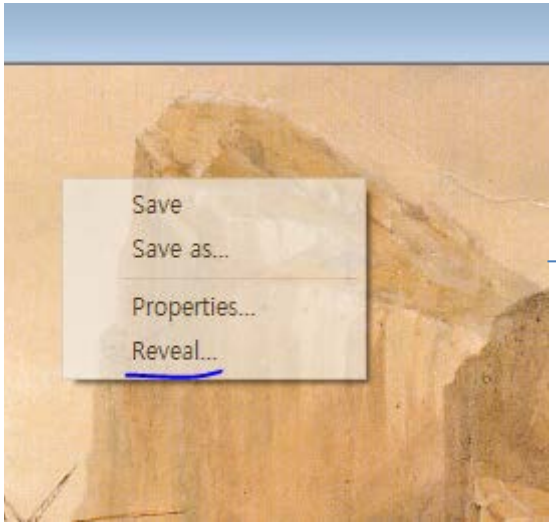


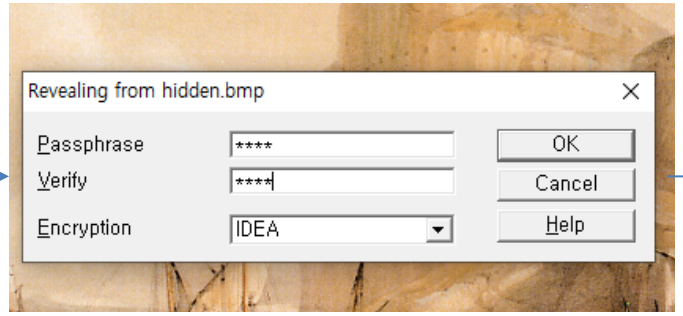
원본 그림

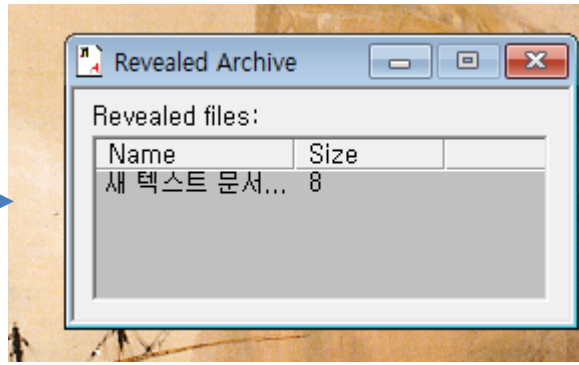
스테가노그래피 적용 그림

실습 2번 : 스테가노그래피 적용 그림파일 첨부

2. 기밀성 – 스테가노그래피







4. 숨겨진 텍스트 파일 확인을 위해 Reavealing, 암호화 방식 선택 후 비밀번호 입력
Revealed Archive 창에서 숨겨진 파일 확인할 수 있으며, 다른 이름으로 저장하여 파일 출력 가능

3. 해쉬함수 – 무결성

해쉬함수란?

- 임의의 크기를 가진 데이터를 고정된 데이터의 크기로 변환시키는 것
- 자료구조에서는 해쉬 테이블을 이용하여 데이터 검색에 활용
- 암호용 해시 함수는 해쉬값을 가지고 원래 입력값을 알아내기 힘들다는 것에 착안, 무결성 검증에 사용
- 해쉬 함수의 요구사항 : 임의 길이 메시지가 고정 길이의 해쉬값을 계산해낼 것
  쉽게 계산이 가능해야 함

3. 해쉬함수 – 무결성

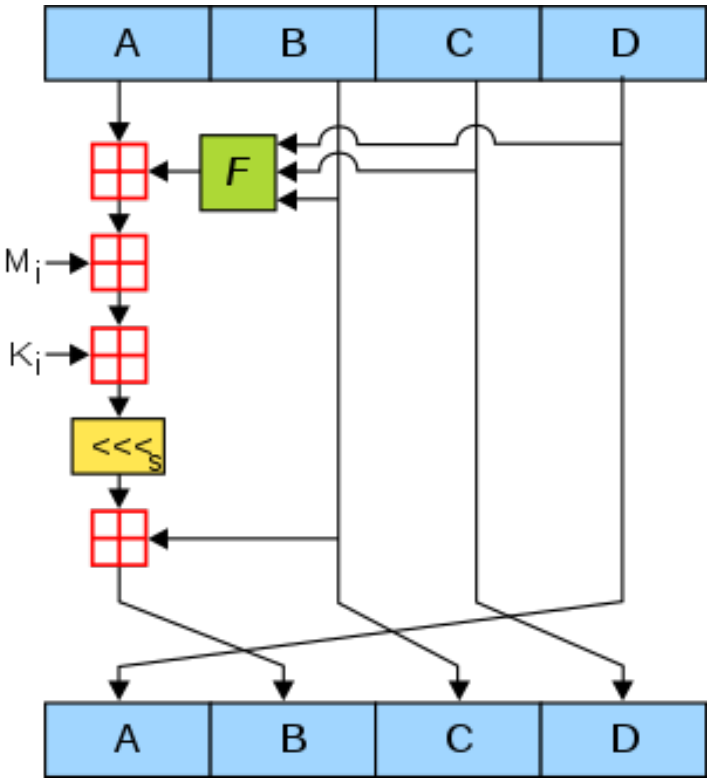
[세번째] Integrity, 무결성 (실습, http://www.convertstring.com/ko/Hash/MD5)

- 해쉬함수(실습하는 MD5 Sum 외에도 수 많은 Hash function 프로그램이 존재) 는 역산, 충돌에 안전해야 한다.

실습 3번 : computersecurity 의 MD5 해쉬값 제출

3. 해쉬함수 – 무결성

- MD5의 취약성 발견 사례



1996년 : 설계상 결함 발견, SHA-1 대체 사용 권장

2004년 : 해쉬값 충돌 발견(다른값 대입, 같은 해쉬값)

2006년 : 컴퓨터 한 대의 계산 능력으로 1분 내 충돌 발견

2008년 : MD5 결함 이용한 SSL 인증서 변조 가능성

충돌이 발생하게 된다면?

실습문제 정리

- **실습 1번 : 춤추는 그림 암호 문장 전체를 완성**
- **실습 2번 : 스테가노그래피 적용 그림파일 첨부**
- **실습 3번 : computersecurity 의 MD5 해쉬값 제출**

- **실습 후 제출**

- **제출 메일 주소 : movestok@seoultech.ac.kr**
- **제출 제목 양식 : 이름_학번_1주차**

참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8

Q & A