2017 국가암호기술 공모전

형태보존암호화를 이용한 랜섬웨어 방지 및 스테가노그라피 보안강화기술

형태보존암호화 정의

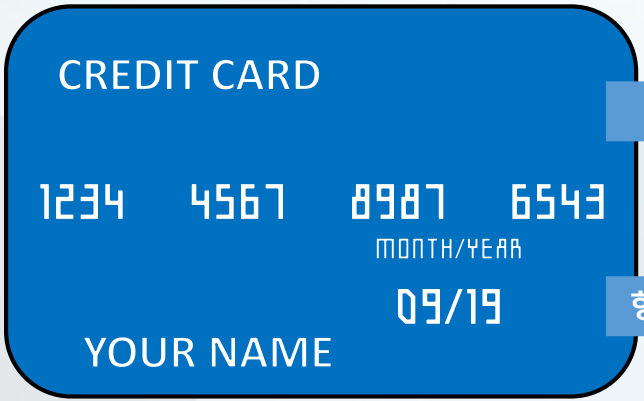
- 원문의 형태와 암호문의 **형태가 동일함**을 보장하는 암호화 기술

형태보존암호화 특징

- **15바이트 이하의 정보**에 대한 암호화에 효율적임
- **데이터베이스의 구조 변경**을 최소화할 수 있음

형태보존암호화 예시

- 신용카드와 같이 숫자로 구성되는 평문에 대한 암호문은 숫자로 결정됨



블록암호화

기존 블록암호를 통한 암호문

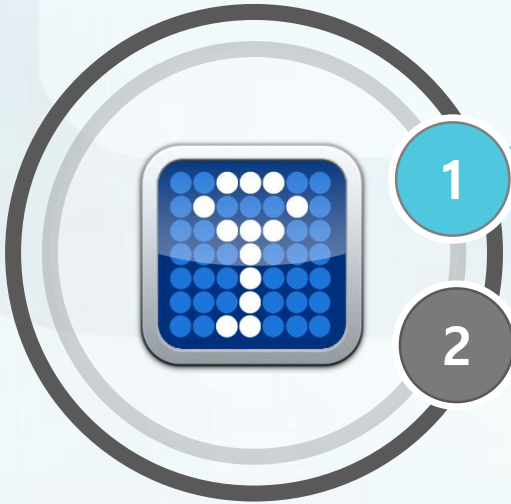
BusiN3427tlleaDV7NA=
(Base64 인 코딩 적용, 기존형태와 다름)

형태보존암호화

형태보존암호를 통한 암호문

7483127865309458
(기존형태와 동일함)

차례



랜섬웨어

- 데이터를 암호화하고 이를 **인질로 금전을 요구**하는 악성 프로그램

랜섬웨어의 종류

- 크립트, 케르베르, 세이지, 록키

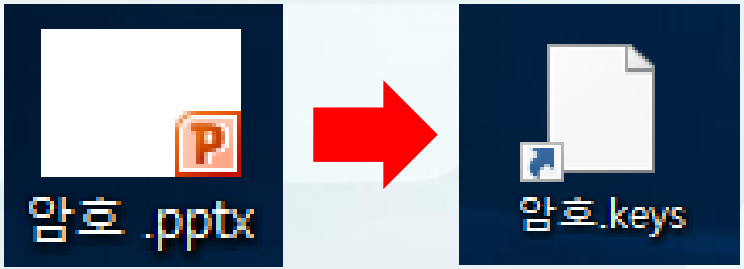
랜섬웨어의 동작원리

- 랜섬웨어는 **특정한 확장자 (중요 파일)**를 검색한 후 이를 **암호화**

랜섬웨어 방지 기법 #1

- 랜섬웨어에서 검색하는 **특정한 확장자**를 형태보존암호화시키는 시스템 구축

※ 예시) OO대학교 학생이 타 대학교 외투를 입고 있으면 OO대학교 학생으로 유추 불가능



실제 컴퓨터 시스템 적용 화면

랜섬웨어 방지 기법 #2

- 파일 확장자와 함께 파일 내부의 **시그니처**에 대한 형태보존 필요
- 파일 내부의 시그니처는 파일 상에서 **일정한 크기만을 활용** 가능
- 형태보존암호화 시 **시그니처 저장공간의 변경없이 암호화** 가능

확장자	시그니처(16진수)	오프셋	설명
AVI	52 49 46 46 XX XX XX XX 41 56 49 20 4C 49 53 54	0	동영상 파일
BMP	42 4D	0	이미지 파일
GIF	47 49 46 38 39 61	0	이미지 파일
HWP	D0 CF 11 E0 A1 B1 1A E1	0	한글 파일

시스템 동작 메커니즘

1) 확장자/시그니처 암호화 과정

- 확장자와 시그니처를 형태보존암호화 후 해당 파일에 대한 정보를 **서버에 저장**

2) 실행 과정

- 시스템에 적법한 **사용자 인증을 거친 후 로그인**
- 실행하고자 하는 파일을 클릭하면 해당 파일에 대한 정보를 서버에서 검색
- 해당 파일에 대한 정보에 따라 **복호화없이 바로 적합한 연산 실행**

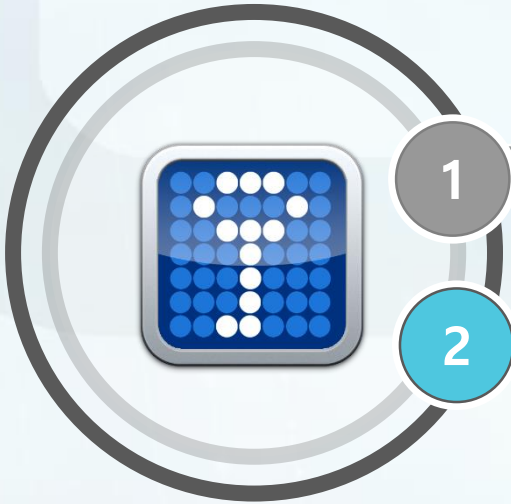
- 예시) 해당 파일이 HWP 확장자를 형태보존암호화한 파일인 경우 확장자 및 시그니처에 대한 복호화 없이 한글 프로그램을 실행시킴
  → 파일 확장자명과 시그니처는 프로그램 실행에 영향을 미치지 않음,
  따라서 복호화는 필요하지 않음

보안성 및 성능 평가

- **보안성**: 특정 확장자 및 시그니처에 대한 랜섬웨어 공격 기법 방지

- **성능**: 약간의 연산이 추가적으로 필요
  초기에 형태보존암호로 확장자 및 시그니처 암호화 1회 필요
  프로그램 실행 시 파일 정보 검색 필요 → 복호화가 필요 없음

차례



스테가노그래피의 정의

- 사진 음악 동영상 등의 일반적인 파일 안에 데이터를 숨기는 기술

목적

1. 은밀한 의사소통
2. 일급 비밀문서의 수송

특징

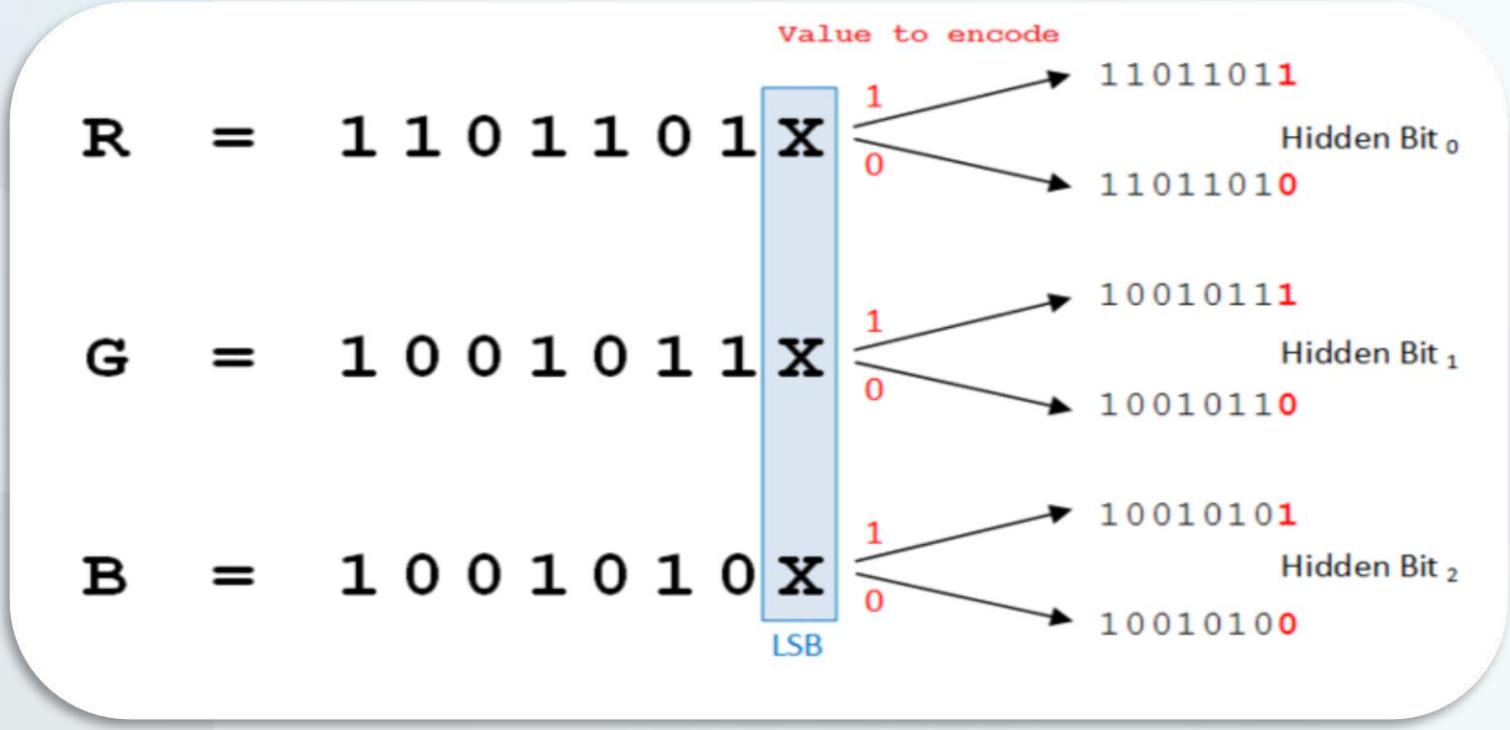
1. 보안수준을 높이는 게 목표
2. 다량의 데이터는 숨기기 힘듦

데이터 삽입

육안으로 확인 불가능

스테가노그래피 정보 삽입법

- 가장 기본적인 방법으로써 최하위 비트에 비밀정보를 삽입
- 진보된 기법으로는 주파수 도메인에 비밀정보를 삽입하는 기술이 있음
- 스테가노그라피 정보 노출 시 보안성 강화를 위해 삽입 정보에 대한 암호화 적용



스테가노그래피 정보 삽입법의 문제점

- 많은 정보를 숨기게 될 경우 원본에 대한 **변경이 많이 일어남**
  → **탐지가 보다 쉽게 가능한 문제점**
- 예시) 사진을 포토샵으로 많은 정보를 수정 시 쉽게 확인 가능
  → 아래와 같이 눈 수정을 많이 한 경우 **쉽게 확인 가능**

스테가노그라피 상에 안전한 암호문 삽입법

- 기존 블록암호화로 **15 바이트 이하 정보 암호화 시 16 바이트로 정보가 확장됨**
- 스테가노그라피의 경우 **최소한의 정보만을 암호화 후** 삽입 가능

- 예시) 8 바이트 암호화 시

기존 블록 암호화

8 바이트 평문 → 16 바이트 암호문

형태보존암호화

8 바이트 평문 → 8 바이트 암호문

보안성 및 성능 평가

- **보안성**: 스테가노그라피 탐지를 보다 어렵게 함
- **성능**:
  오히려 연산 속도가 개선됨
  → 스테가노그라피를 적용해야 하는 정보의 양이 줄어들기 때문

Q & A

감사합니다