형태보존암호와 딥러닝 기반의 신경망 구별자

https://youtu.be/t5HhN0XC810

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

형태 보존 암호란?

형태보존 암호의 다양한 알고리즘

형태보존 암호 FF1, FF3-1

차분 특성 및 신경망 구별자

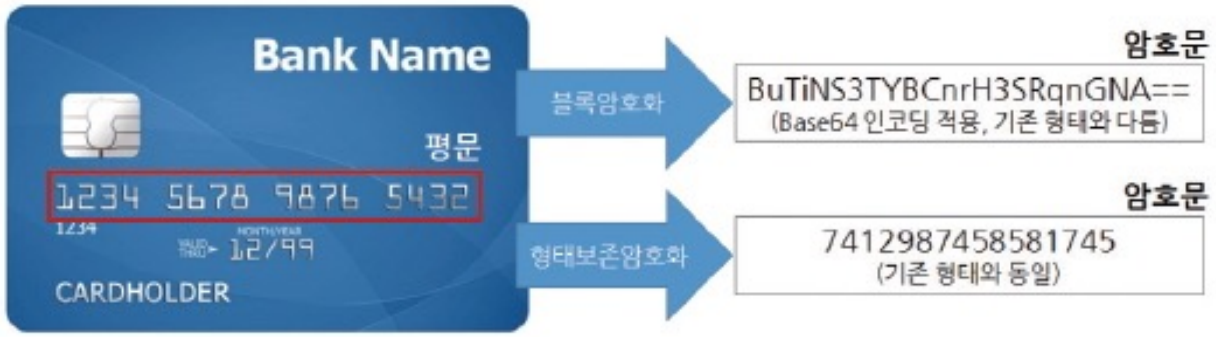
형태 보존 암호란?

형태보존(Format-Preserving Encryption)

암호란?

형태보존암호란 기존 블록암호와 다르게 암호화를 거쳐도 평문이 가진 형태를 온전하게 유지한 채로 길이가 동일하게 생성되는 암호화 기술

형태 보존 암호 기본 개념 설명



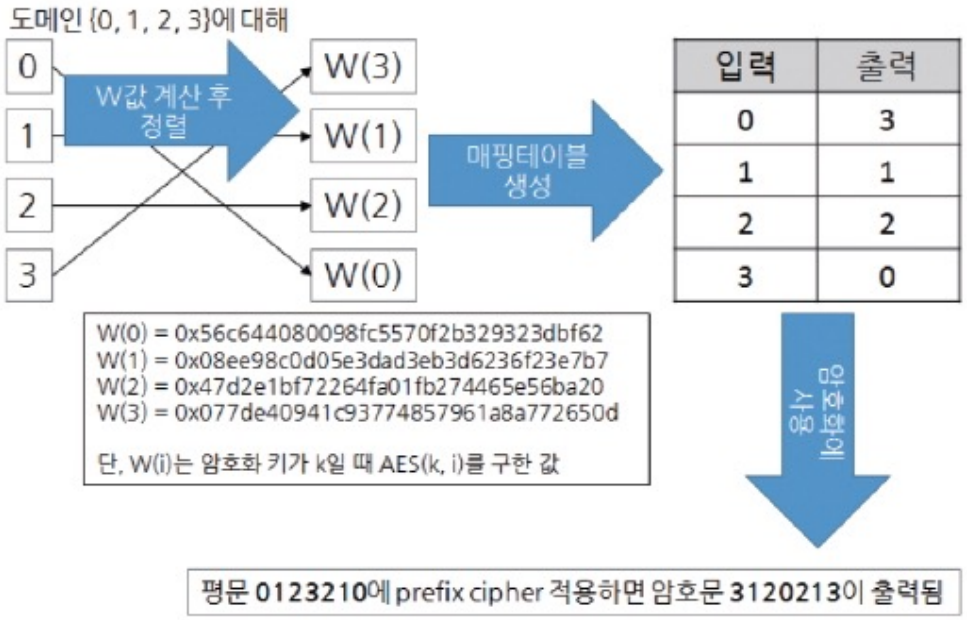
[신용카드 번호의 일반 블록암호화와 형태보존암호화]

카드 번호를 블록암호로 암호화할 경우 입력값의 길이와 형태가 다르지만, 형태보존 암호의 경우 입력값과 길이와 형태가 동일하게 보존된다.

형태보존 암호의 다양한 알고리즘

Prefix Cipher, Cycle – Walking Cipher, Generalized – Feistel Cipher

형태보존 암호의 다양한 알고리즘



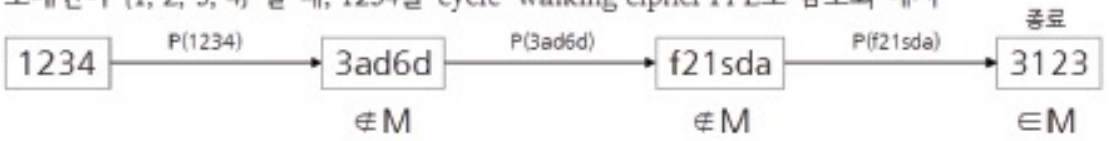
Prefix Cipher 알고리즘

형태보존 암호의 다양한 알고리즘

```
CycleWalkingFPE(x) {
   if P(x)가 M의 원소이면
      return P(x)
   else
      return CycleWalkingFPE(P(x))
}
```

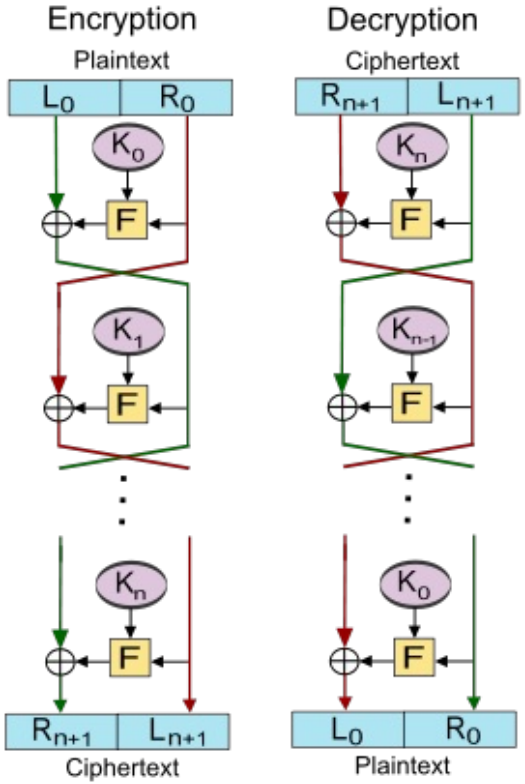
x : 평문
P : AES 등과 같은 블록암호화 알고리즘
M : 도메인 원소들로 부터 순열 조합 가능한 집합

도메인이 {1, 2, 3, 4} 일 때, 1234를 cycle-walking cipher FPE로 암호화 예시



Cycle – Walking Cipher 알고리즘

형태보존 암호의 다양한 알고리즘



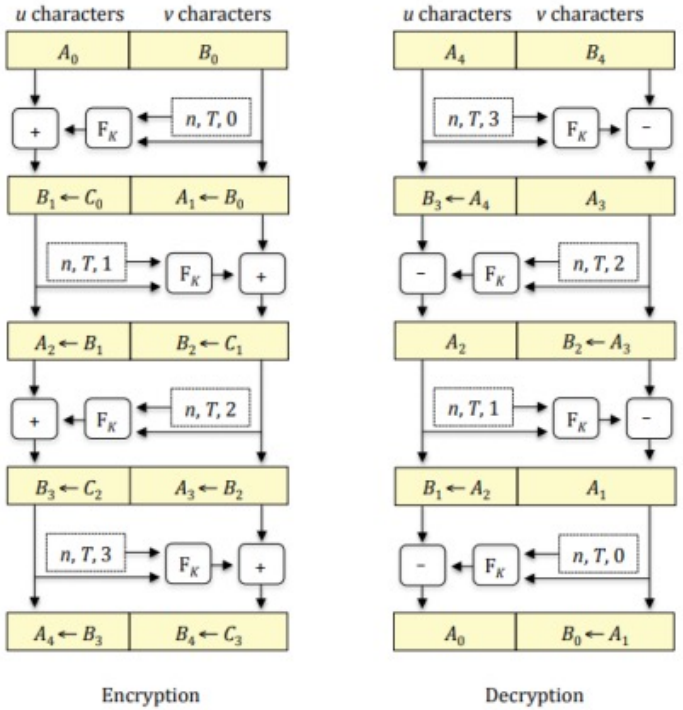
Feistel Cipher 알고리즘

형태보존 암호 FF1,FF3-1

형태보존 암호 FF1, FF3-1

NIST에서 **형태보존암호**에 대한 표준을 진행하였으며 그 결과 FF1, FF3-1가 대표적으로 선정되었다.

형태보존 암호 FF1,FF3



FF1, FF3 Feistel 구조

형태보존 암호 FF1,FF3

radix	$[2 \ldots 2^{16}]$
$radix^{minlen}$	more than 1,000,000
minlen	2
maxlen	2^{32}
round	10

Requirements of FF1

radix	$[2 \ldots 2^{16}]$
$radix^{minlen}$	more than 1,000,000
minlen	2
maxlen	$2 \times \lfloor \log_{radix}(2^{96}) \rfloor$
round	8

Requirements of FF3

FF1은 FF3에 비하여 더 높은 라운드와 길이를 제공하기 때문에 상대적으로 더 안전하며 FF3는 FF1에 비하여 라운드가 적은 대신 더 높은 데이터 처리량을 보인다.

차분 특성 및 신경망 구별자

- 차분 특성
  - 데이터의 변화를 측정하거나 분석하는 과정에서 사용되는 특성
- 차분
  - 서로 다른 평문과 암호문을 XOR한 값
    - 평문 $P_0 \oplus P_1 = P_2$, 암호문 $C_0 \oplus C_1 = C_2$

      → **차분 = (P_2, C_2)**
- 차분 분석
  - 암호 분석 기법 중 하나로, 암호화 알고리즘 또는 키를 해독하기 위해 사용되는 기법

    → 차분 특성을 활용하여 암호화에 사용된 키 일부 정보를 도출하는 방법
- 딥러닝 기반의 신경망 구별자
  - 기존의 암호문에 나타나는 차분 특성을 신경망을 통해 학습
  - 차분을 갖는 암호문과 랜덤 데이터를 구별

    ➔ 차분 특성을 갖는 데이터 수집 → 딥러닝 모델 구축 → 학습 → 차분을 갖는 데이터 구별

Q & A