암호화

1) NN 활용한 암호화 논문 서칭

Neural Network Based Cryptography (2014)

Pseudo Random Number Generator에서 NN 활용

Symmetric Cryptography (1 secret key)

A symmetric key cryptography using genetic algorithm and error back propagation neural network (2015)

Encryption 시 Genetic algorithm 사용/ Decryption 시 NN 활용

Symmetric Cryptography (1 secret key)

Encryption Algorithm Based on Neural Network (2019)

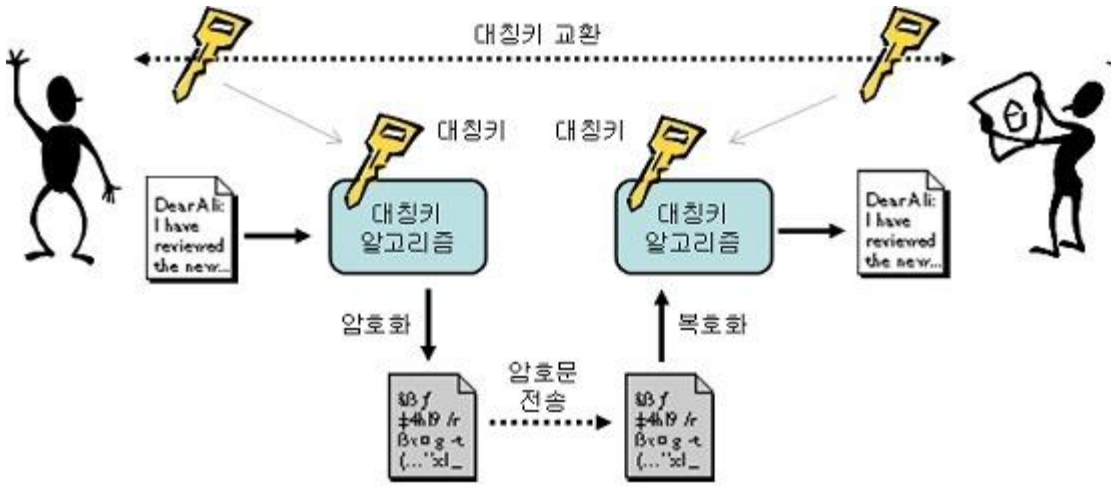
Auto-associative neural network를 이용한 암호화

Symmetric Cryptography (1 secret key)

2) 암호화 사용 상황 비교 (대칭키 암호화)

(1) 기존

발신자와 수신자가 명확히 존재하여 서로 정해진 대칭키를 교환해 암호화 및 복호화



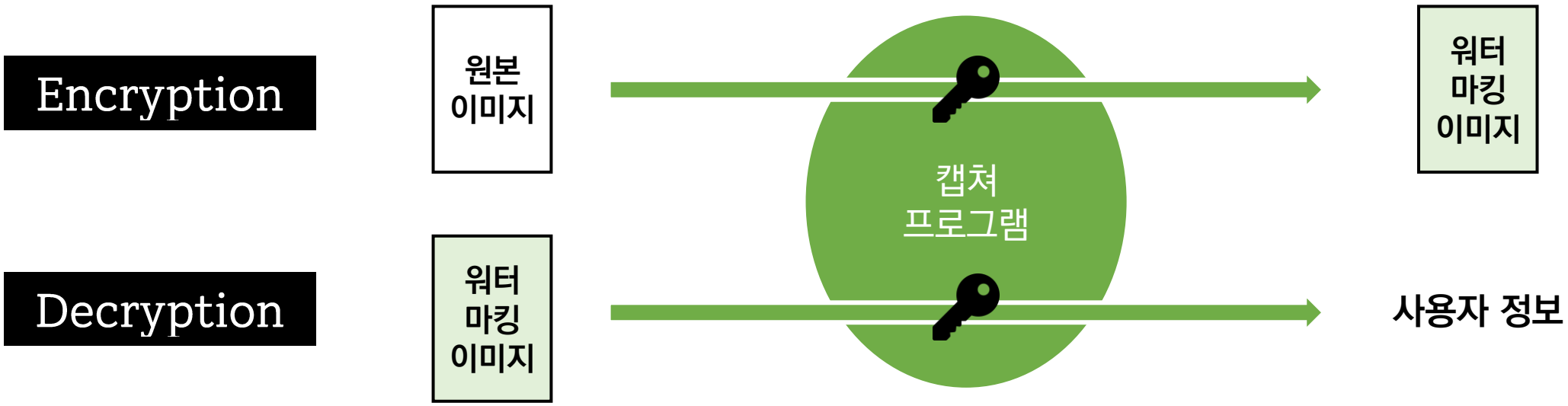
(2) 캡쳐 시스템

(기존 시스템 도입 시) 사람마다 다른 대칭키를 적용하면 어떤 대칭키를 사용했는지 모르는 상태에서 복호화 해야함

389(*$(#)

불법 유출된 이미지에서 추출한
복호화가 필요한 암호문

3) 캡쳐 프로그램 특이점



1. 사람마다 다른 대칭키를 사용하면 복호화 시 brute force 방식으로 모든 키를 적용해서 찾아야 함
2. 캡쳐 프로그램은 사용자 간 대칭 키 교환이 불필요 (암호화 및 복호화 시 자체 중재자 역할 수행)

→ 동일한 대칭 키 사용해 암호화 및 복호화

장점 : 속도가 빠름
단점 : 키 교환하면서 대칭키가 노출될 수 있음

4) 암호화 방식 구상

암호화한 사용자 정보를 직접 이미지에 삽입

변경

사용자 정보 해시 테이블의 Index 값 + @를 이미지에 삽입

EX) 해시 테이블은 캡쳐 프로그램의 DB에 위치

Index	(대칭키 사용) 암호화된 사용자 정보
12235	394)$()%(#_$)%#*$^)
12236	4(#%*^#)495396#)$5
…	…

장점

1. 이미지에서 워터마크를 추출해도 사용자 정보를 알 수 없음
2. 공통된 대칭키를 사용하여 어떤 암호문도 복호화 가능
3. 작은 크기의 정보(index)만을 이미지에 삽입하여 효율적

캡쳐 시 수집하는 사용자 정보(예상)

1. 디바이스 정보
2. 기기 식별번호
3. IP 주소
4. 캡쳐 일시

EX) D522fHD!bbbbb!123.5.2.66!202004081829333

5) 암호화 계획(다음주 수요일까지 코딩)

Neural Network Based Cryptography (2014)의 암호화 방식 참조

1. Neural Network를 이용해 PRNG 생성
2. 생성된 난수를 이용해 Secret Key 생성
3. (AES 또는 DES) 알고리즘 채택해 Secret key와 함께 이용
4. Plane text를 암호화 및 복호화