스트림 암호(Stream Ciphers)

IT융합공학부 윤세영

유투브 주소: https://youtu.be/pJP1yfeZQ4w

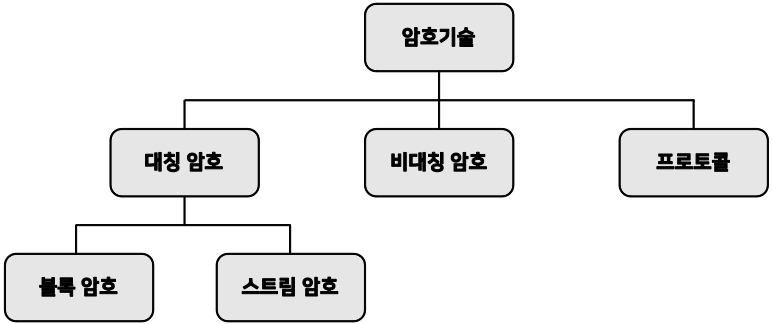
스트림 암호 vs 블록 암호

스트림 암호의 암호화와 복호화

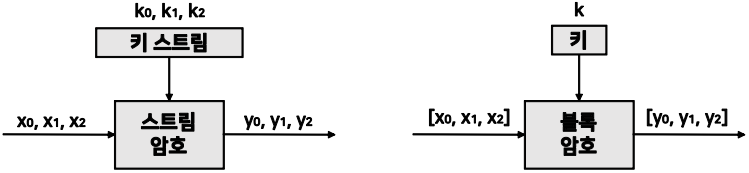
난수 및 의사 난수 생성기

One-Time Pad

암호학에서 스트림 암호란?



스트림 암호 vs 블록 암호



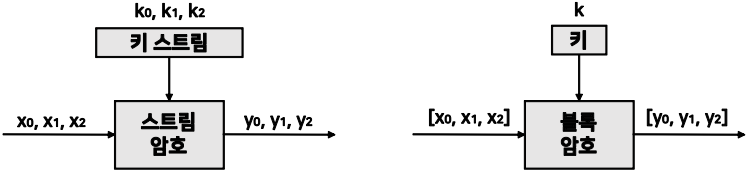
[스트림 암호]

- 비트별로 암호
- 키 스트림의 한 비트와 평문의 한 비트를 가지고 암호화를 수행

[블록 암호]

- 동일한 키로 한 번에 전체 블록의 평문 비트를 암호화

스트림 암호 vs 블록 암호



[스트림 암호]

- 작고 빠르기 때문에 휴대폰이나 작은 임베디드 장치와 같이 컴퓨팅 능력이 적은 응용 분야에 적합
- 대표적인 스트림 암호인 A5/1 암호는 GSM 휴대폰 표준의 일부로 음성 암호화에 사용됨

[블록 암호]

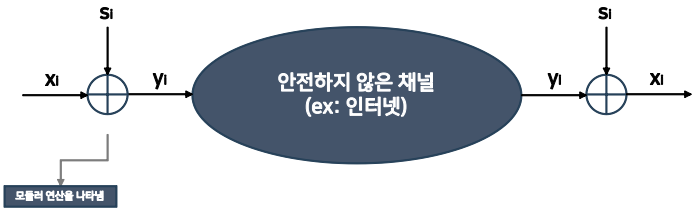
- 인터넷 응용 분야에서 다양하게 활용되고 있음

스트림 암호의 암호화와 복호화

평문(Plaintext) x_i, 암호문(Ciphertext) y_i, 키 스트림(Key Steam) s_i $(x_i, y_i, s_i \in \{0,1\})$에 대하여

암호화(Encryption): $y_i = e_{s_i}(x_i) \equiv x_i + s_i \bmod 2$

복호화(Decryption): $x_i = d_{s_i}(y_i) \equiv y_i + s_i \bmod 2$



스트림 암호의 암호화와 복호화

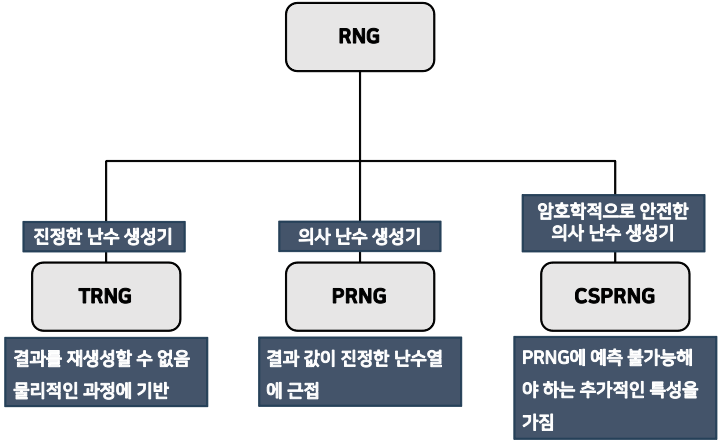
모듈러 2 덧셈이 왜 좋은 암호화 함수인가?
➔ 모듈러 2 덧셈은 XOR 연산과 동일하다. (0⊕0 = 0, 0⊕1 = 1, 1⊕0 = 1, 1⊕1 = 0)
➔ 임의의 입력 값에 대해 0 또는 1의 결과가 될 확률이 정확하게 50%이다.

암호화 함수와 복호화 함수는 동일하다.
➔ $y_i \oplus s_i = (x_i \oplus s_i) \oplus s_i$
➔ $= x_i \oplus (s_i \oplus s_i)$
➔ $= x_i \oplus 0$
➔ $= x_i$

XOR 연산: 자기 자신을 더하면 결과 값은 항상 0

스트림 암호의 안전성은 키 스트림에게 달려 있다.
키 스트림 비트에 대해 가장 중요한 요구조건은 공격자에게 임의의 난수열로 보이는 것이다.
송신자와 수신자 모두 키 스트림을 재생성할 수 있어야 한다.

난수 및 의사 난수 생성기


RNG
진정한 난수 생성기
TRNG
결과를 재생성할 수 없음
물리적인 과정에 기반
의사 난수 생성기
PRNG
결과 값이 진정한 난수열
에 근접
암호학적으로 안전한
의사 난수 생성기
CSPRNG
PRNG에 예측 불가능해
야 하는 추가적인 특성을
가짐

One-Time Pad

다음을 만족하는 스트림 암호를 One-Time Pad라 한다.
One-Time Pad는 무조건적으로 안전하다.

- 키 스트림은 진정한 난수 생성기를 이용하여 생성된다.
- 키 스트림은 합법적인 통신 객체에게만 알려진다.
- 모든 키 스트림 비트는 한번만 사용된다.

무한대의 계산 자원을 가지고도 해독할 수 없는 암호시스템을 무조건적으로 또는 정보 이론적으로 안전하다고 한다.

$$y_0 \equiv x_0 + s_0 \bmod 2$$
$$y_1 \equiv x_1 + s_1 \bmod 2$$
$$\vdots$$

One-Time Pad

- 키 스트림은 진정한 난수 생성기를 이용하여 생성된다.

- TRNG, 진정한 랜덤 비트를 생성하는 물리적인 장치가 필요하다.

- 키 스트림은 합법적인 통신 객체에게만 알려진다

- 송신자가 수신자에게 직접 전달하거나, 신뢰할 수 있는 택배 서비스 등을 이용해야 한다.

- 모든 키 스트림 비트는 한번만 사용된다.

- 키 스트림 비트는 재사용될 수 없으므로 모든 평문 비트에 대해 하나의 키 비트가 필요하다.
- 따라서 키의 길이가 길어진다.

Q & A