20202430671 김태현

차량에 설치된 장비(라즈베리파이)가
MQTT 프로토콜을 통해 서버로
데이터를 전송한다.

이 과정에서 송수신을 가로채거나
데이터를 위·변조할 수 있기에
각 말단에 암호화는 빼질수없다

이에 혼돈신호라는 것을 사용하게 된다.

↳ 예측불가한 신호

XOR연산
- 서로 다르면 1, 같으면 0으로 출력

메시지 이니셜

혼돈신호 11001101
XOR 01111011

- MQTT에서의 혼돈 XOR 암호화 시스템의 활용
  1. 발신자 : 센서 데이터 생성후 혼돈신호 XOR 암호화
  2. 혼돈신호 생성기
  3. 암호화 알고리즘 : 메시지와 혼돈신호를 XOR 연산
  4. MQTT Broker : 암호화된 메시지 중계(전송)
  5. 수신자 : 동일한 혼돈신호를 동기화하여 XOR 복호화

*유의사항
- 송신자와 수신자가 서로 동일한 시드를 부여하여 혼돈시퀀스 동기화
- 고급공격에는 취약할 수 있으나

훔친 수정의 공격은 괜찮을것

- MQTT에 직접적으로 활용하는 것이 아니라 MQTT에 전달하기 전에 활용하는 것이다.

XOR혼돈은

↳ 외부에서는 무질서해 보이지만 내부에서는 규칙에 따라 움직이는 시스템

↳ 변화가 적지만 시간이 지남에 따라 큰 차이를 만들 수 있다.

[초기민감성]

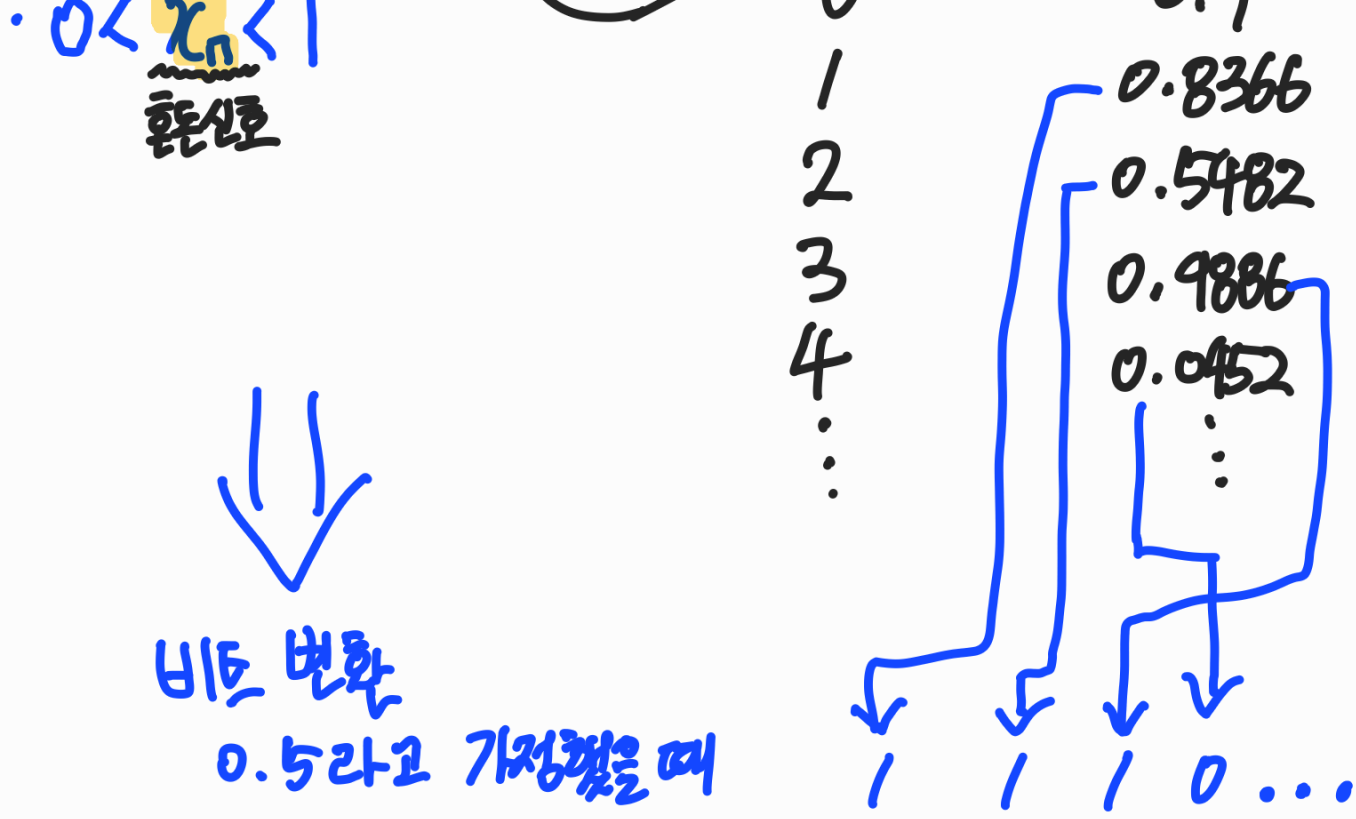
- 예시로 알아본 암호화 (Logistic Map)

$[x_{n+1} = r \times x_n \times (1 - x_n)]$

- x_0 : 초기값
- r : 제어 파라미터

0.7
3.99

n	x_n
0	0.7



↳ 변환된 값을 XOR 암호화에 사용한다.

3번 과정

이 과정을 역으로 하여 복호화 시켜 데이터를 확인한다.