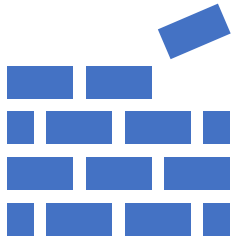
암호학의 과거, 현재, 미래

이지훈

목차

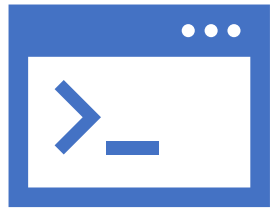


암호학이란?

고대, 근대, 현대의 암호

단방향 암호화

양방향 암호화



양자 암호

양자 암호와 암호학의 미래

암호학이란?

암호 : 특정한 정보를 남들이 이해할 수 없도록 변형하거나 감추는 일련의 단계

컴퓨터에서의 암호 : 원본을 알아보지 못하도록 비화하는데 쓰이는 알고리즘

-> 사용자(송, 수신자)는 쉽고 간편하게, 외부인은 어렵게 하는 것이 Point
-> 이러한 암호에 대해 연구하는 학문이 바로 암호학

암호학이란?

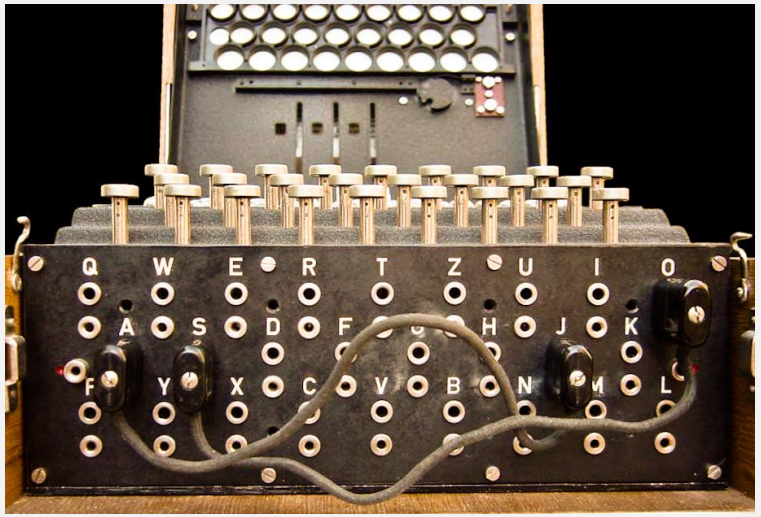
고대의 암호, 스키테일

기원전 400년경 고대 그리스의 군사들이 사용하던 암호

특정 지름을 갖는 막대에 종이를 감고 평문을 횡으로 쓴 다음,
종이를 풀어 문자를 재배치하는 방식

막대의 지름 = 송,수신자 사이에 공유된 비밀키

암호학이란?

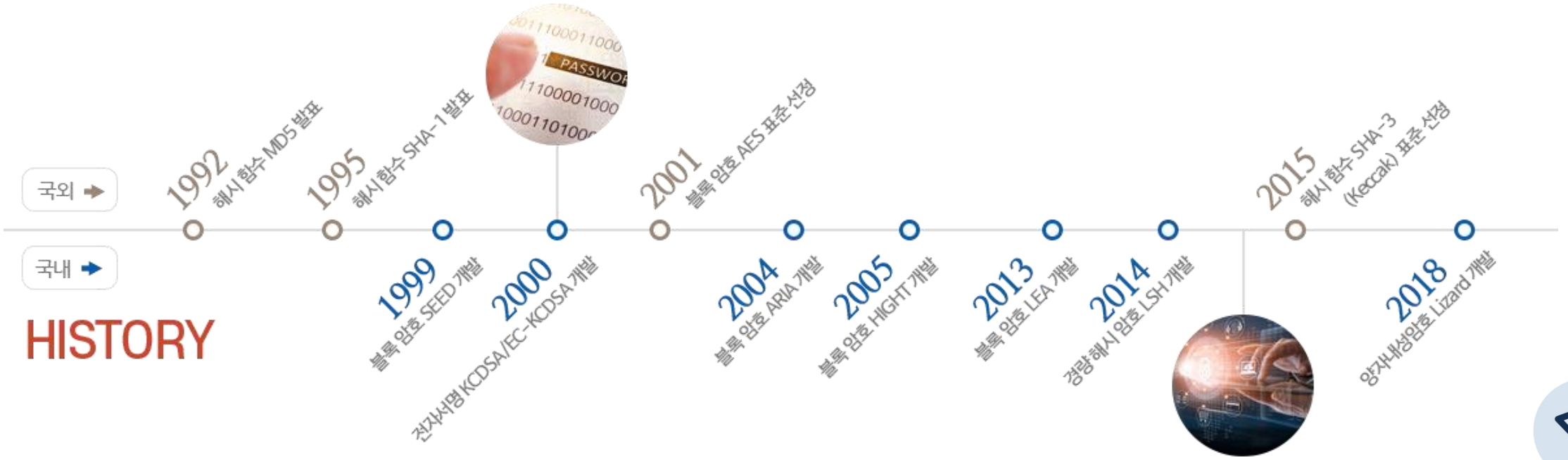


근대의 암호, 에니그마

20세기에 들어서 통신 기술의 발전과 두 차례의 세계대전으로 암호의 연구가 활발히 진행

2차 세계 대전에서 독일군이 사용했던 암호기 - 앨런 튜링을 비롯한 영국의 암호해독부가 암호해독을 성공하였다

현대의 암호학


국외
국내
HISTORY
1992 해시 함수 MD5 발표
1995 해시 함수 SHA-1 발표
1999 블록 암호 SEED 개발
2000 전자서명 KCDSA/EC-KCDSA 개발
2001 블록 암호 AES 표준 선정
2004 블록 암호 ARIA 개발
2005 블록 암호 HIGHT 개발
2013 블록 암호 LEA 개발
2014 경량 해시 암호 LSH 개발
2015 해시 함수 SHA-3 (Keccak) 표준 선정
2018 양자내성암호 Lizard 개발

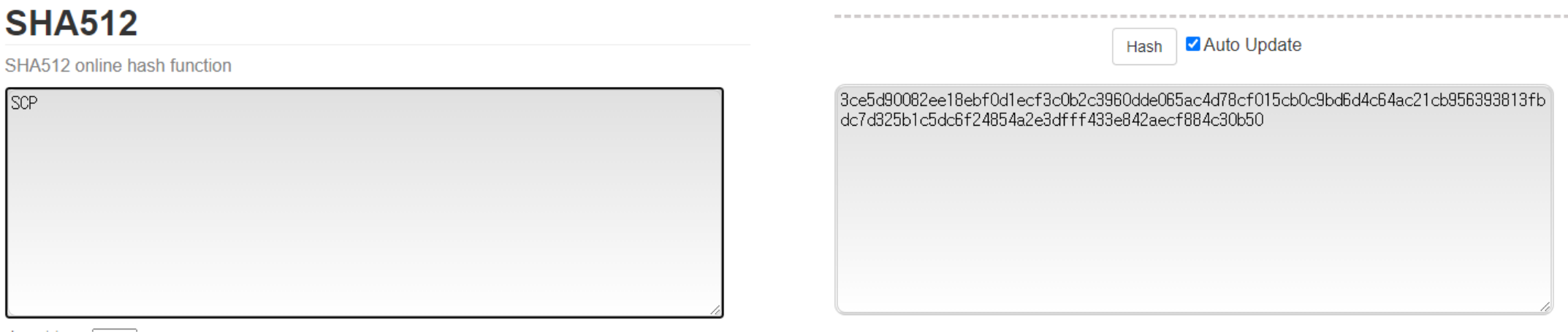
단방향 암호화 : 해시 함수

단방향 암호화 : 암호화는 가능하지만 복호화는 불가능한 암호화 방식.
-> 무결성에 초점을 둔 암호화 방식

비밀번호를 저장 -> 암호화 -> 암호문을 저장 -> 비밀번호를 입력 -> 저장된 암호문과 비교

MD5, SHA 1, SHA 256, SHA 512 등이 대표적인 해시 함수

단방향 암호화 : 해시 함수



https://emn178.github.io/online-tools/

양방향 암호화 : 대칭키

양방향 암호화 : 암호화와 복호화 모두 가능한 암호화 방식
-> 원래 데이터를 얻을 수 있다는 특징을 가지고 있음

대칭키 암호화 방식 : 암호화할 때 사용한 키를 복호화 할 때도 동일하게 사용.
-> 전달 과정 중에 누군가 암호문과 대칭 키를 탈취할 경우, 정보를 얻어낼 수 있는 취약점 발생

양방향 암호화 : 비대칭키

비대칭 키 암호화 방식(공개키 암호화 방식) : 대칭 키 암호화 방식의 단점을 보완한 방식.

A가 B에게 정보를 전달할 경우
공개키와 비공개키라는 키 쌍을 만듦 -> 공개키를 이용해 암호화 -> 비공개키를 이용해 복호화

양방향 암호화 : 비대칭키

https://www.devglan.com/online-tools/rsa-encryption-decryption

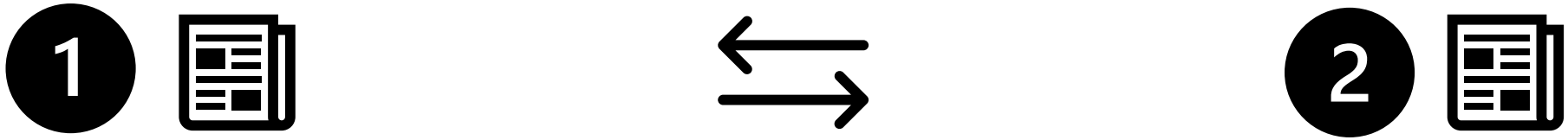
양자 암호

현재의 슈퍼 컴퓨터가 1만년 걸리는 암호를 양자 컴퓨터는 200초면 풀어낼 수 있다.
-> 양자 컴퓨터가 제대로 완성되는 순간에 현존하는 모든 암호는 무의미 해진다

만약 더 복잡하게 암호를 만든다? -> 그만큼 암호화, 복호화 하는데 시간이 오래 걸리므로 비효율적이다.

그래서 현재 연구중인 새로운 암호화 방식인 '양자암호'

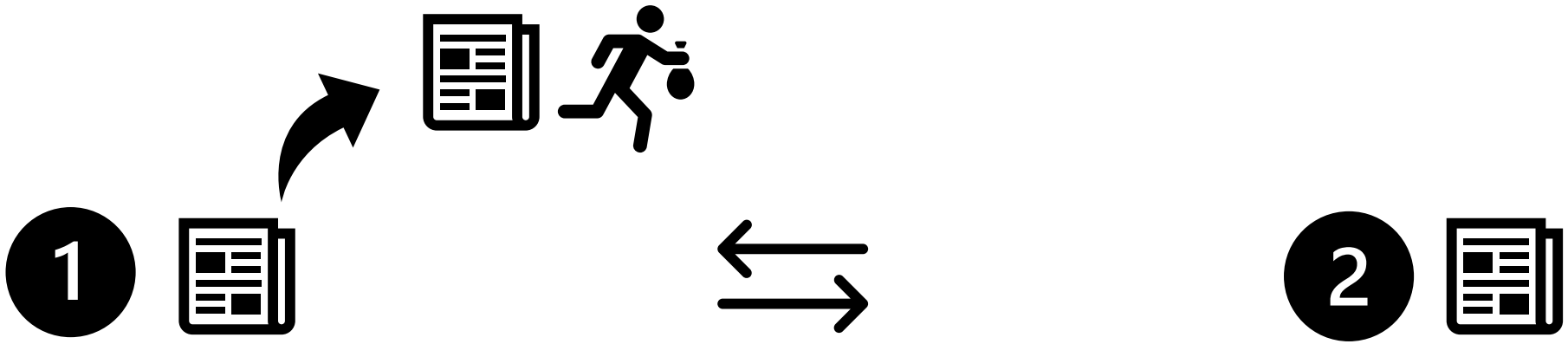
양자역학 ?



양자역학 ?

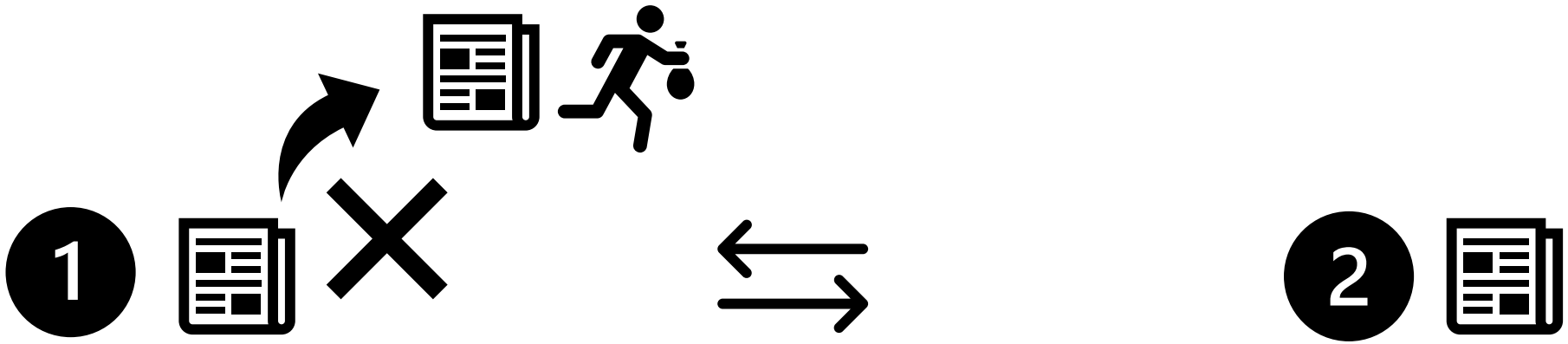
양자역학 ?

양자역학 ?



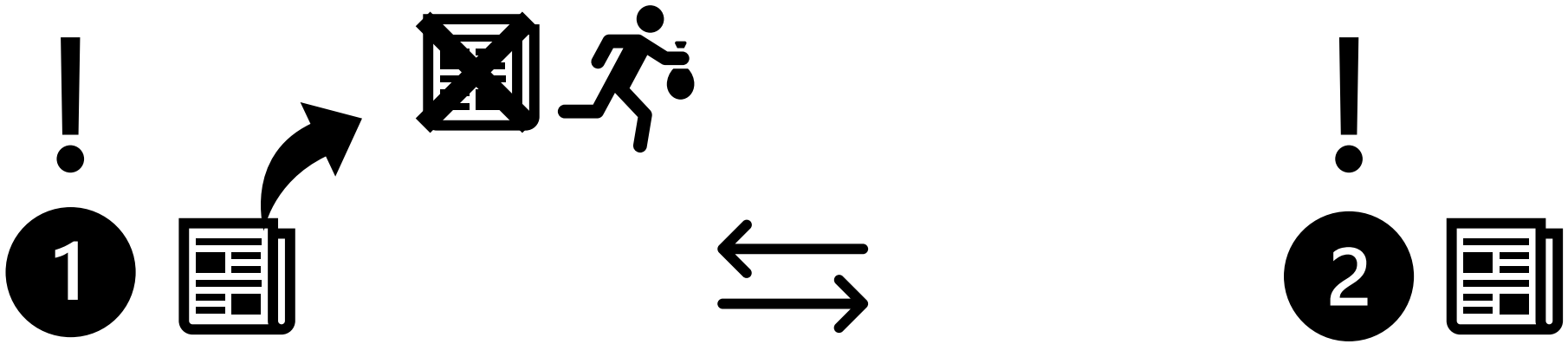
복제 불가 이론

양자역학 ?



복제 불가 이론

양자역학 ?



불확정성의 원리, 슈뢰딩거의 고양이(중첩상태)

Q & A