암호학 입문

김호중, 이지윤

함께 해볼 활동들

1. 암호학의 역사
2. 암호의 과거와 현재
3. 소프트웨어

암호란 무엇일까요?

비밀을 유지하기 위해서 허락된 사용자만 알 수 있도록 꾸민 약속을 말합니다.

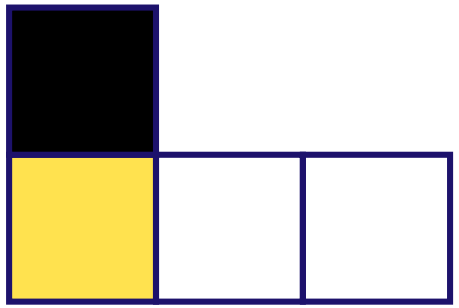
우리의 생일, 주민번호 등 타인이 알았을 때 남용될 수 있는 정보들을 안정하게 보호해 줍니다.

암호(cryptography)는 그리스어로 비밀이라는 뜻 크립토스(kryptos)에서 기원하였습니다.

암호가 없다면 어떤 일이 벌어질까요?

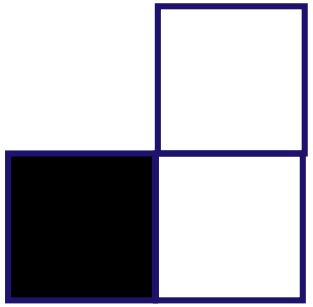
디지털 환경(인터넷)에서 암호가 하는 역할은 무엇이 있을까요?

암호는 어떻게 사용할까요?



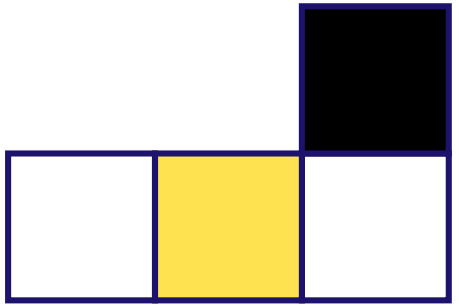
1 단계

보내는 사람이
암호화할 정보 준비



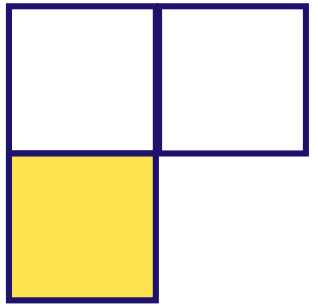
2 단계

암호화
암호 만들기



3 단계

복호화(암호풀기)



4 단계

받는사람이
정보를 사용

1 단계

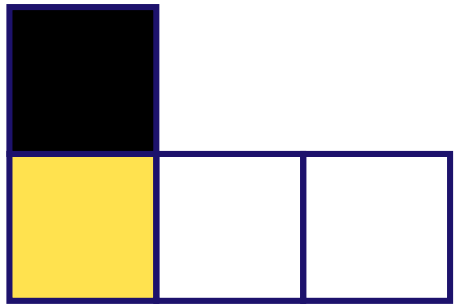
“대한민국 강원도 평창”

“선생님은 사과를 좋아한다”

“연세대학교가 평창을 13시에 공격한다”

암호화할 정보를 준비한다.
(받는 사람의 상황을 고려하여 결정합니다.

정확한 정보를 전달하기 위해서 정보를 정리한다.



2 단계

“연세대학교 평창 13시 공격”

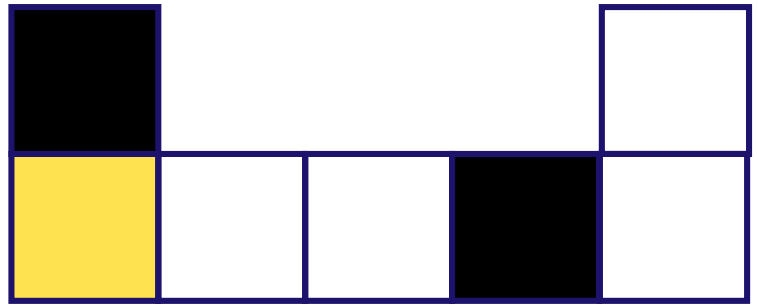
암호화(암호 만들기)

“1224 54 317 0001”

암호화할 정보가 정해졌다면 미리 정한 규칙에 따라 암호화합니다.

암호화된 정보는 암호화방식을 모른다면 해독하기 어려워야 합니다.

암호화된 정보를 해독할 수 있는 키를 가진 사람이 해독하기 쉽도록 암호화 해야 합니다.



3 단계

“1224 54 317 0001”

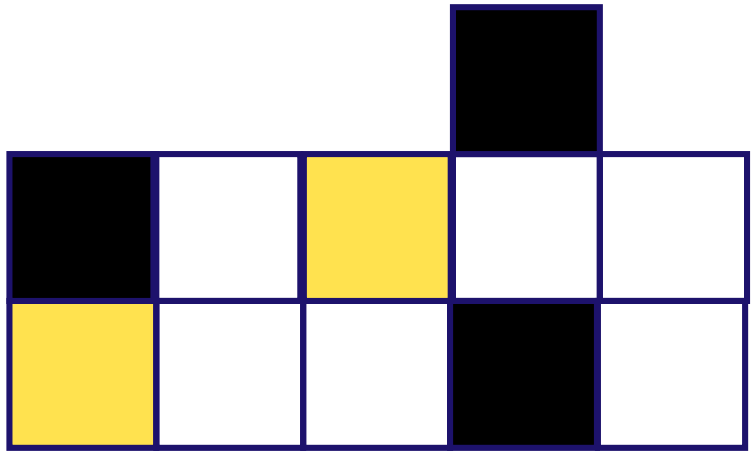
“키를 활용하여 암호풀기”

“연세대학교가 평창을 13시에 공격한다”

미리 정한 암호풀기(키) & 암호화 방식에 따라서 암호문을 해독합니다.

암호를 풀 수 있는 복호화 방식을 “키”라고 부릅니다.

키가 공개된다면 누구든 암호를 쉽게 풀 수 있습니다.



4 단계

“연세대학교가 평창을 13시에 공격한다”

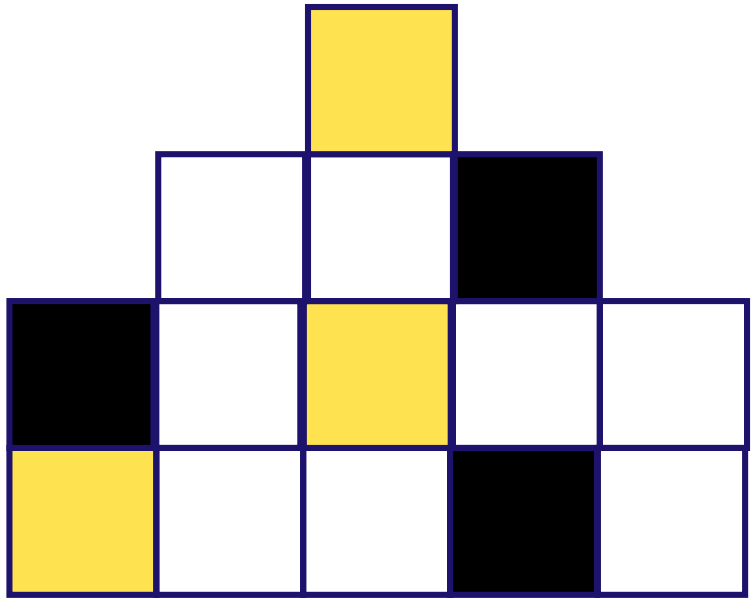
“12시 까지 평창 공격준비를 마친다”

“우리가 먼저 연세대학교를 11시에 공격한다”

정보가 중요한 상황에서 상대방에게 키가 주어진다면 심각한 손해로 이어집니다.

암호화된 정보를 전달받은 후에 행동을 결정합니다.

전쟁 뿐 아니라 정보가 중요해진 현시대에서 암호는 중요한 역할을 수행합니다.



암호화 & 복호화 한번 더 정리해보면

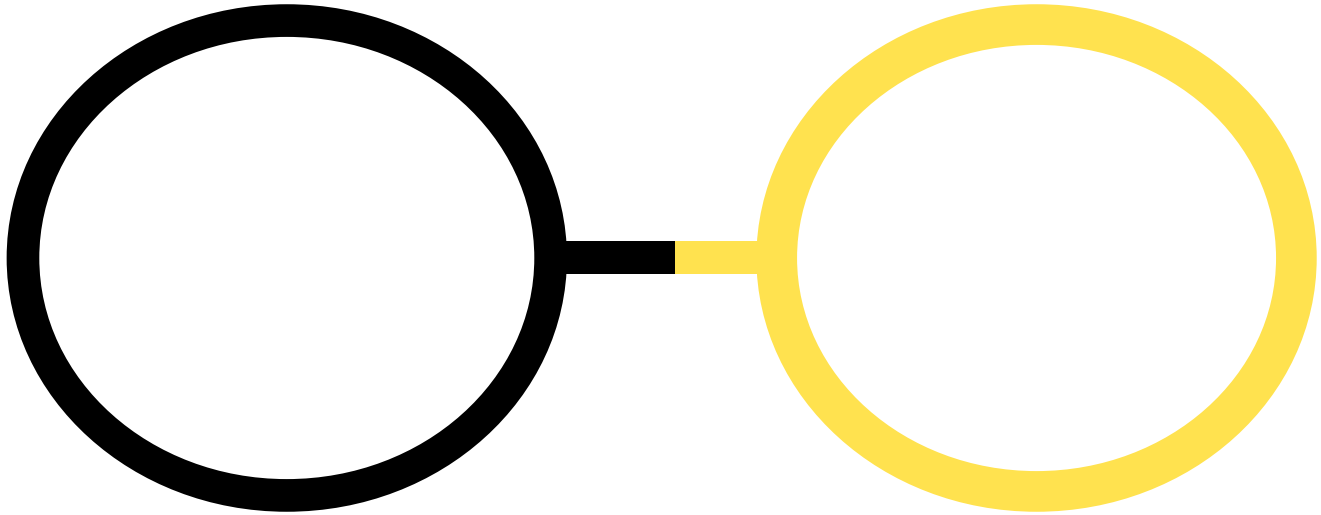
어떤 암호가 좋은 암호일까?

암호화(암호 만들기)

허락된 사용자 즉 키를 가진 사용자만이 정보에 접근할 수 있도록 제어해야 합니다.

정보의 가치가 상승할 때 암호화의 중요성 또한 커진다.

암호화 된 정보는 복호화(암호풀기) 할 수 있어야 가치가 있다. (복호화 할 수 있는 키가 명확하게 정의되어 있어야한다.)



복호화(암호풀기)

복호화 할 수 있는 키가 없다면 복호화가 매우 어려워야 좋은 암호입니다.

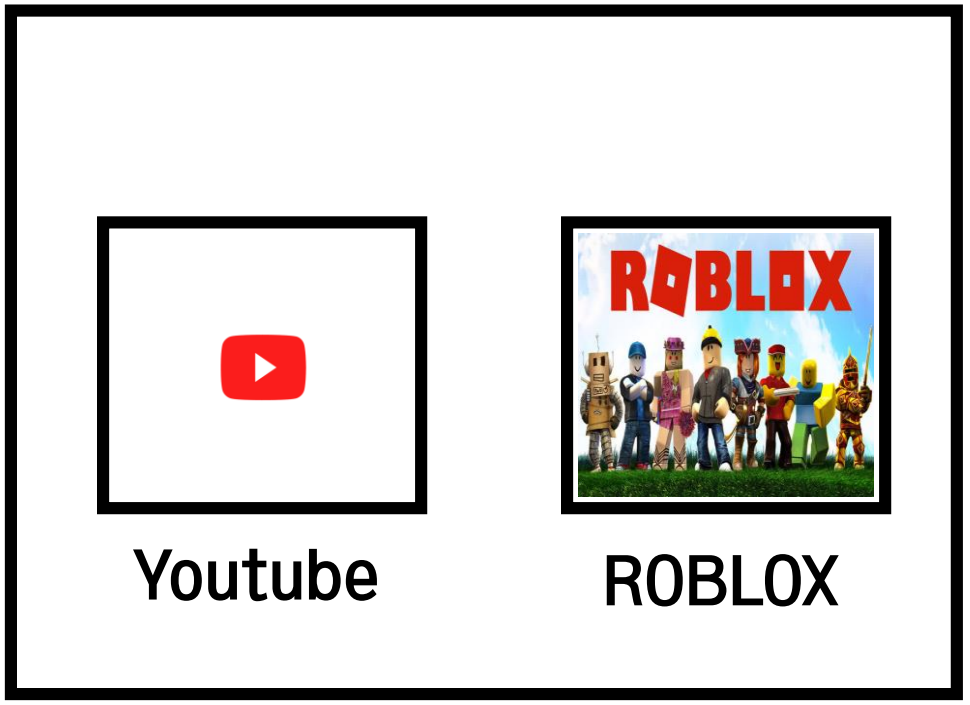
존재할 수 있는 모든 경우의 키 수를 대입해보면 어떤 암호라고 복호화 가능합니다.

암호화와 복호화에는 반드시 “키”라 부르는 규칙이 존재합니다.

암호가 없다면 어떻게 될까?

사용자

서비스 이용을 위해서 로그인을 해야 한다.
유튜브, 로블록스 에게 내가 서비스 이용자임을 알린다.(로그인)



우리가 이용하고자 하는 서비스

사용자의 로그인 정보를 파악하고 로그인을 시켜야 하지만 사용자가 진짜 사용자인지 도둑인지 확인할 수 없다.(로그인 불가능)

암호가 없다면 어떻게 될까?

사용자

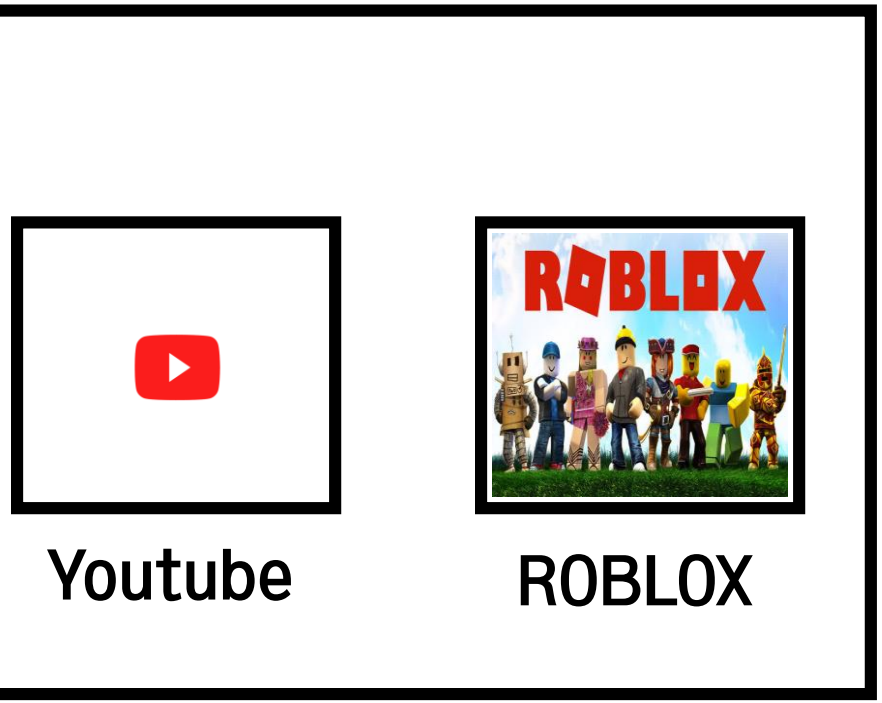
나의 개인정보를 활용하여 서비스에 로그인을 시도한다.

도둑

사용자의 정보를 훔쳐 서비스에 로그인하여 악의적으로 사용한다.

로그인

훔치기



Youtube

ROBLOX

우리가 이용하고자 하는 서비스

암호가 없다면 도둑의 훔치기에 취약해지게 됩니다.

암호는 주로 언제 사용되어 왔을까요?

정보의 전달

주로 전쟁과 함께 발전하였으며 대표적으로 카이사르, 스키테일 암호가 있습니다.

- 복호화 규칙을 알고 있다면 해독이 쉬어야 하며 복호화 규칙을 모른다면 풀기 어렵게 만들어야 합니다.
- 정보의 가치가 상승할 때 함께 암호학(암호를 다루는 학문)의 가치 또한 높아졌습니다.

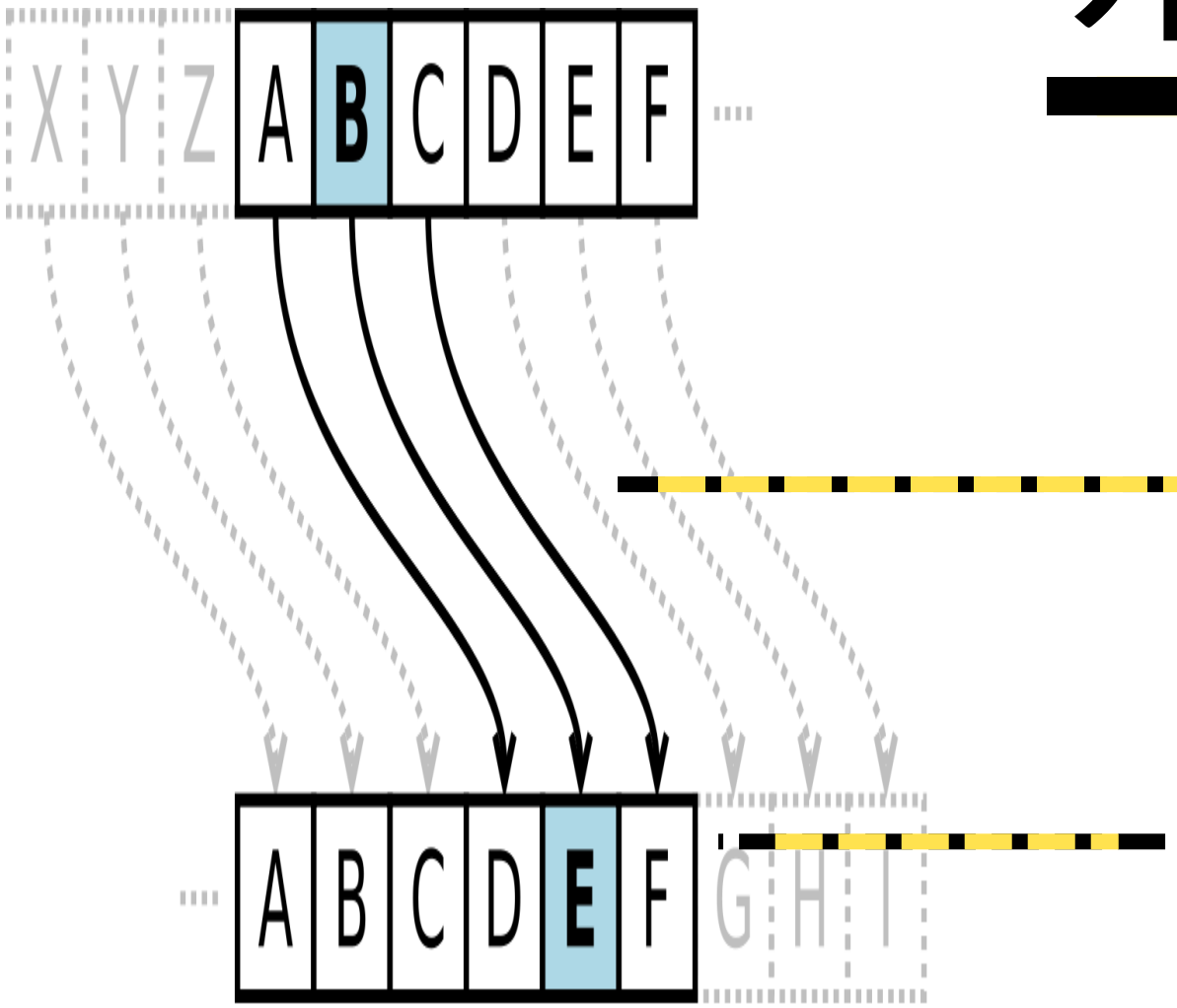
온라인 서비스

은행 등의 금융서비스와 개인정보를 요구하는 인터넷 서비스(유튜브, 로블록스 등) 모두 중요한 정보를 기반으로 동작합니다.

- 개인정보를 다른 사람이 쉽게 악용할 수 있다면 심각한 범죄발생(해킹) 가능성이 높아집니다.
- 우리의 개인정보 악용을 막기 위해서 암호화하여 서비스관리자와 정보를 주고받습니다.

카이사르 암호

영상 시청



로마의 정치가 율리우스 카이사르가 사용한 방식입니다.

암호화 하고자 하는 내용을 알파벳별로 일정한 거리만큼 밀어서 다른 알파벳으로 치환하는 방식입니다.

키가 될 수 있는 모든 경우의 수를 대입하면 암호의 해독이 가능합니다.
(키가 될 수 있는 경우의 수가 많을 수록 해독하기 어렵습니다.)

알파벳의 경우 26개로 구성되어 있으면 키의 개수는 25개 입니다.

“

카이사르 암호 실습시간

학습지를 보고 주어진 암호문을 직접 해독해보아요

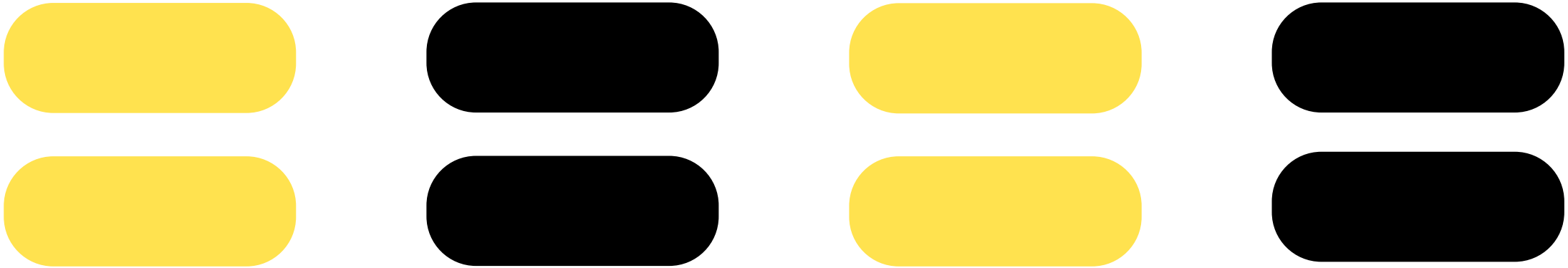
”

카이사르 암호 실습시간

카이사르 암호풀기

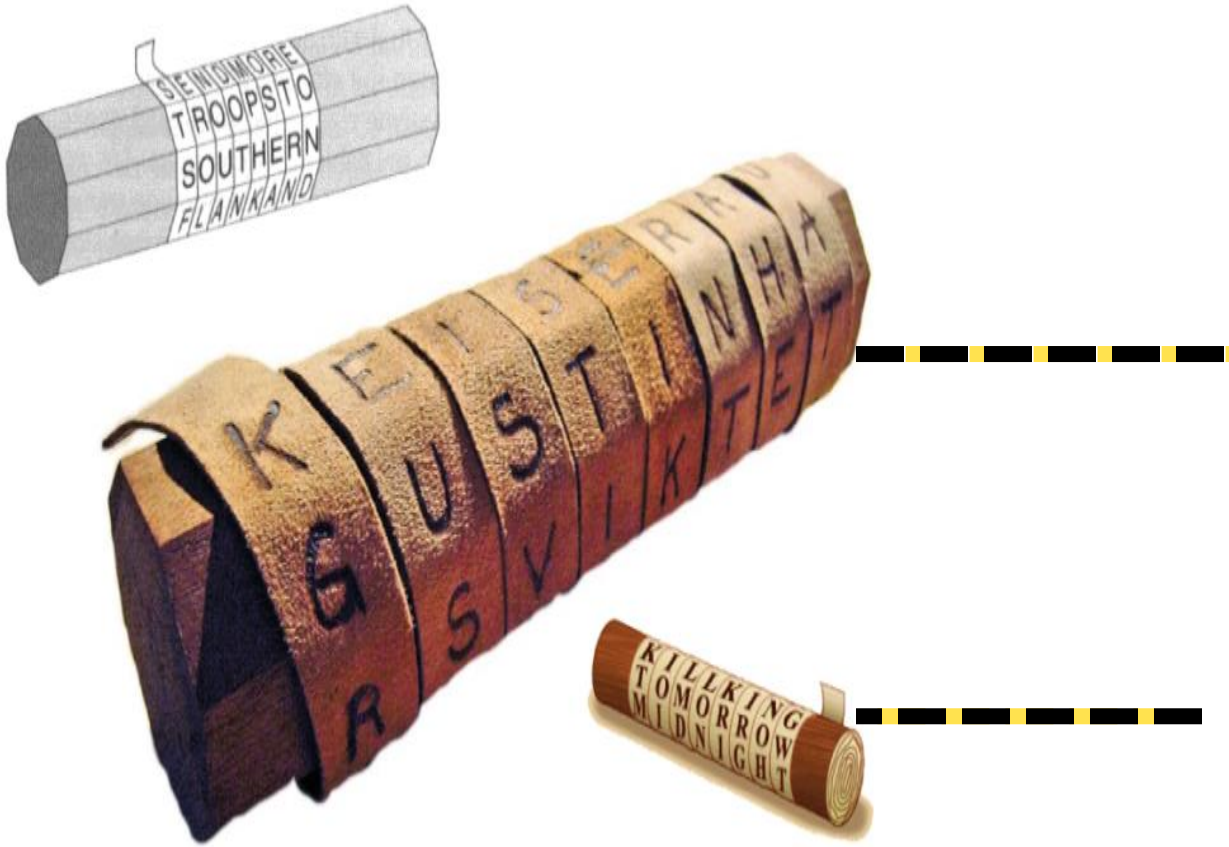
카이사르 암호는 알파벳을 n번만큼 이동시켜 암호화 시킵니다.

- 위 암호학 규칙을 이해하고 응용하여 키를 찾아 암호를 풀어 보아요.
- 아래에 있는 단어 중 마음에 드는 것 부터 암호를 풀기 시작할 게요. 하나라도 푼 사람은 정답을 말해주세요.



스키테일 암호

영상 시청



스파르타에서 전쟁터에 나가 있는 군대에 비밀메시지를 전할 때 사용한 암호입니다.

비밀리에 전달 해야 하는 메시지를 그림과 같이 감아서 암호문을 작성합니다.

원통형막대의 굵기에 따라서 보여주는 단어가 달라지며 이는 곧 키가 됩니다. (특정한 원통형 막대를 사용하여 암호화 & 복호화 합니다.)

그 당시 굉장히 비싼 값을 자랑했던 양피지를 사용했기에 긴 문장을 전달하는 것이 부담되었으며, 막대의 굵기를 유추해서 암호를 해독할 수 있었습니다.

“

스키테일 암호 실습시간

학습지를 보고 주어진 암호문을 직접 해독해보아요

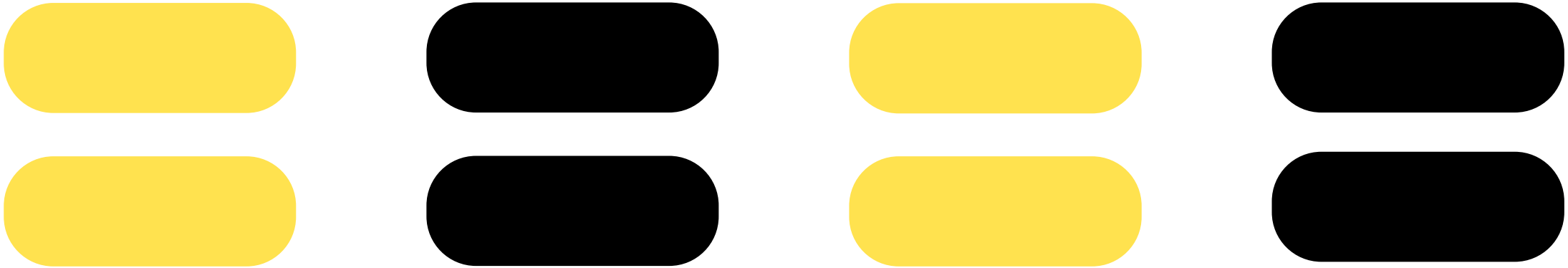
”

스키테일 암호 실습시간

스키테일 암호풀기

스키테일 암호는 종이를 원통형막대에 감아 암호화 시킵니다.

- 스키테일 암호의 키(원통형 막대)를 찾고 정보를 추측해보아요.
- 암호를 모두 푼 학생은 손을 들고 선생님을 불러주세요.



“

숨겨진 과제

친구에게 전달하고 싶은 말을 직접 암호화해보아요

”

숨겨진 과제

암호 만들기

암호화 하고 싶은 문장, 친구에게 전하고 싶은 문장을 정하고 본인이 선택한 규칙에 따라 암호화 해봐요.

- 친구에게 전달하고 싶은 문장을 정하고 암호화를 시작해요. 암호화 규칙을 설명할 수 있어야해요.
- 친구에게 이상한 말하기 나쁜 말 하기 금지.

암호 풀기

친구가 전해준 암호를 풀어보아요. 앞에서 해본 것 처럼 키를 찾아보아요.

- 먼저 암호를 해결한 학생은 손을 들고 선생님을 불러주세요.
- 빠르게 그리고 정확하게 암호를 풀어보아요.

암호란 무엇일까요?

암호 란 풀 수 없는 정보가 아니라 풀기 어려운 정보입니다.
(암호의 복잡성은 대응되는 키의 경우의 수와 연결됩니다.)

소프트웨어, 컴퓨터를 사용한다면 더 빨리 암호를 풀 수 있을까요?

풀 수 있다면 어떤 원리로 해결될까요?

알아보기

SW의 힘을 통해 암호를 풀어볼게요.

키가 없다면 암호를 풀 수 없을까?

키를 유추할 수 있는 방법에는 무엇이 있을까요?

Thank You