형태 보존 암호에 대하여

Made by 양유진 공승화 전다형

학습목표

학생

선생님 오늘 저희가 배울 내용이 무엇인가요?

오전 11:31

오늘은 형태 보존 암호에 대해 수업 할거야~

왜 그러니?

오전 11:34

학생

아 그냥 오늘 수업시간에 뭘 배울까 궁금해서요..ㅋㅋㅎ

오전 11:36

오늘 수업을 통해서 형태보존암호의 표준에 대한 내용과 형태 보존 암호의 암호화 과정에 대해서 알 수가 있어

또 이 암호 기법이 실생활에서 어떻게 쓰이는지도 알아볼거야~!

오전 11:40

학생

으....어려워 보이네요.. 감사합니다

오전 11:36

들어가기

두 비밀번호 중 무엇이 더 관리에 용이해 보이나요?

A	B
aE7Buxsk90o4weksdlm	1720

기본 다지기

- '암호'란?

-비밀 인증 데이터의 한 형식
-중요한 정보나 물건을 보호하기 위하여 사용

- '평문'이란?

-일상적으로 사용하는 문장
-암호화하기 전 또는 암호문을 해독한 문장

- '암호문'이란?

-평문을 암호처리하여 특정인만 이용할 수 있도록 암호화한 문서

- '**암호화**'란?

-암호 + 화(化, 되다)

평문 → 암호문

- '**복호화**'란?

-복(復, 돌아오다) + 암호 + 화(化, 되다)

-암호화의 반대 과정

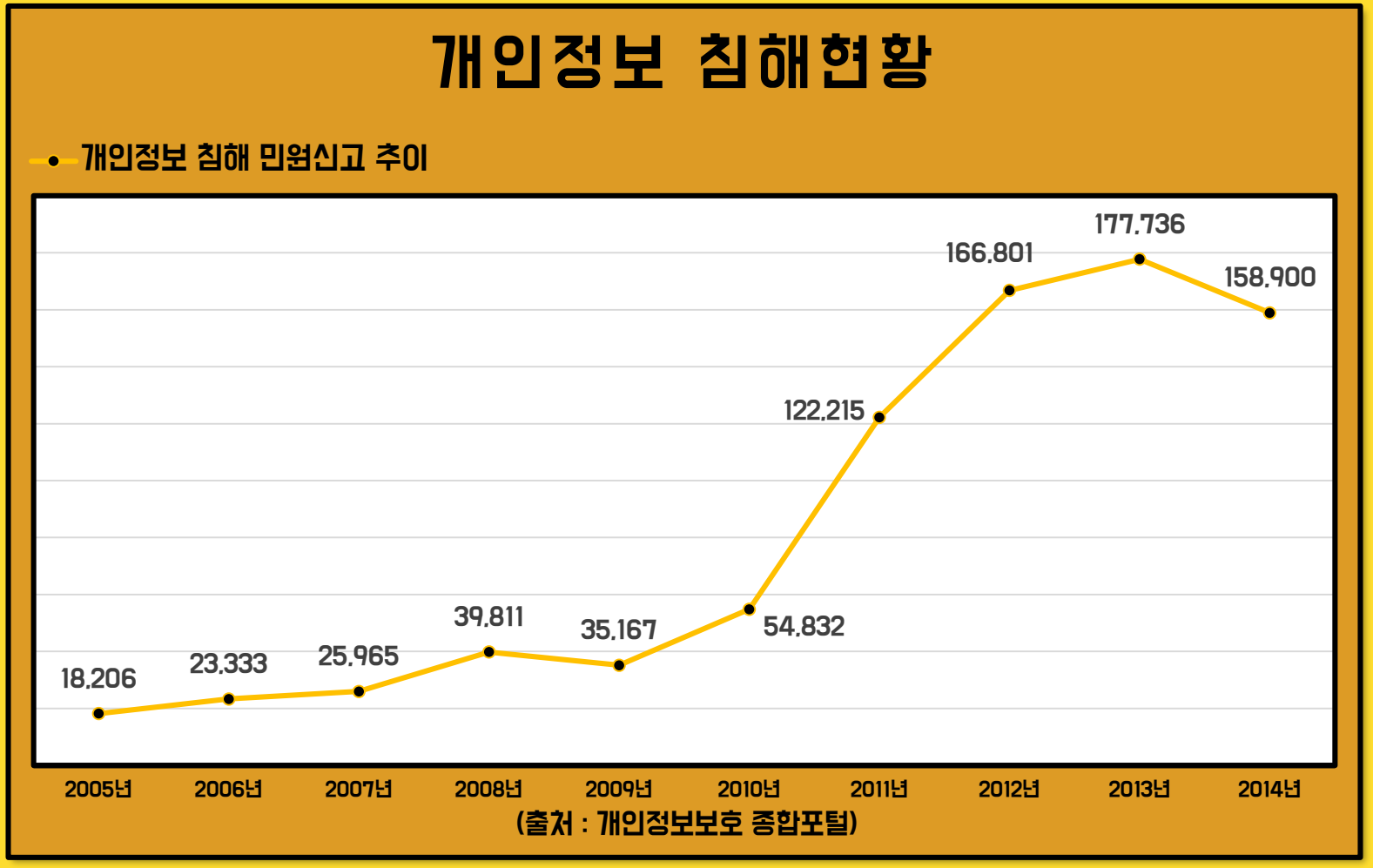
암호문 → 평문

• '알고리즘'이란?
-문제를 해결하기 위한 단계적인 절차
-컴퓨터 프로그램=정교한 알고리즘들의 집합

• '비트'란?
-데이터를 나타내는 최소단위
-0과 1만 사용

암호화의 필요성

- 개인정보 침해



- # 개인정보 유출 피해

https://www.youtube.com/watch?v=xEBMpKvYhxs(앱)
https://www.youtube.com/watch?v=5kKKLj3L5is (카드)

암호화 방식

DES (Data Encryption Standard)

키길이 : 56비트

해킹 쉬움

너무 짧음

보완

AES (Advanced Encryption Standard)

-고급 암호화 표준
-키길이 : 128, 192, 256비트
-해킹 하기 어려움

AES

① hi_hellohi_hello (16글자) → 78F jlop5Ui12ki9e

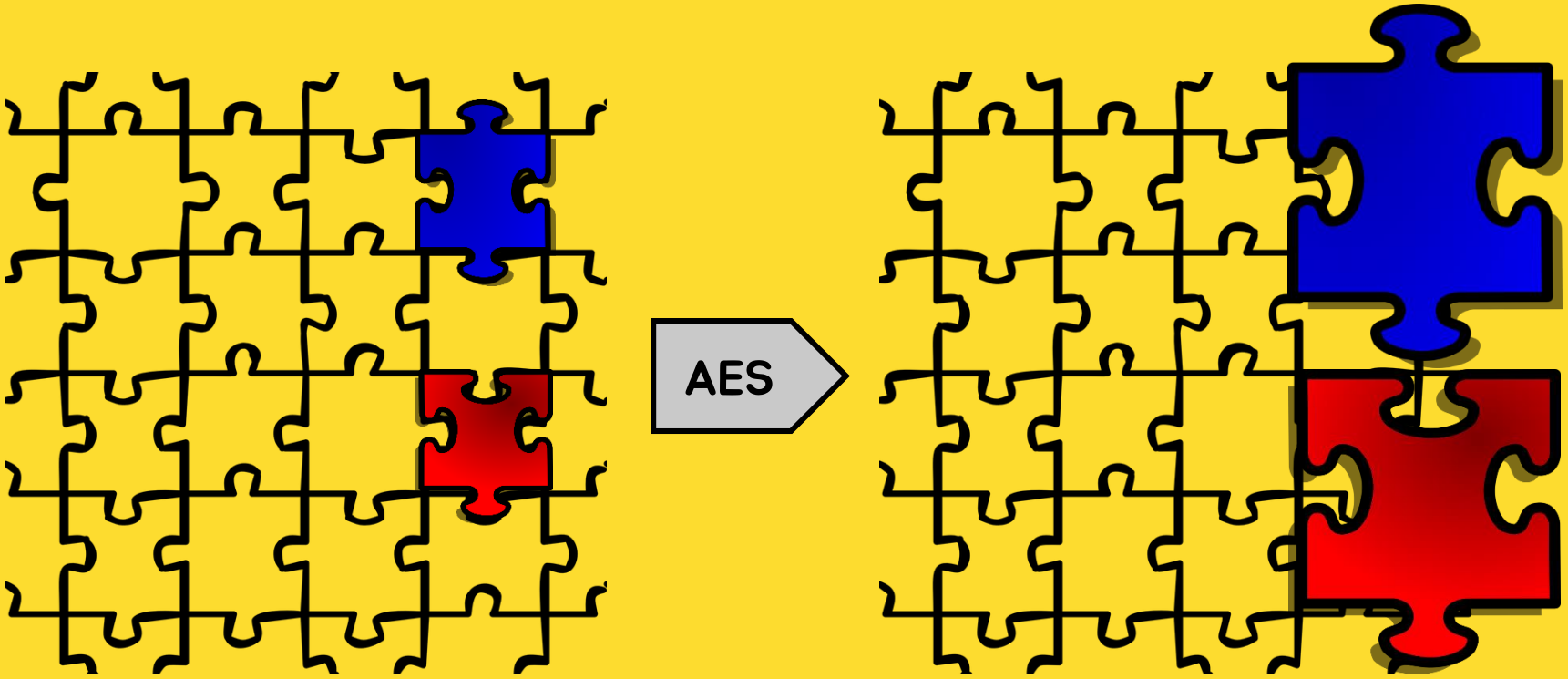
예) 2바이트 → 16글자 (바이트)

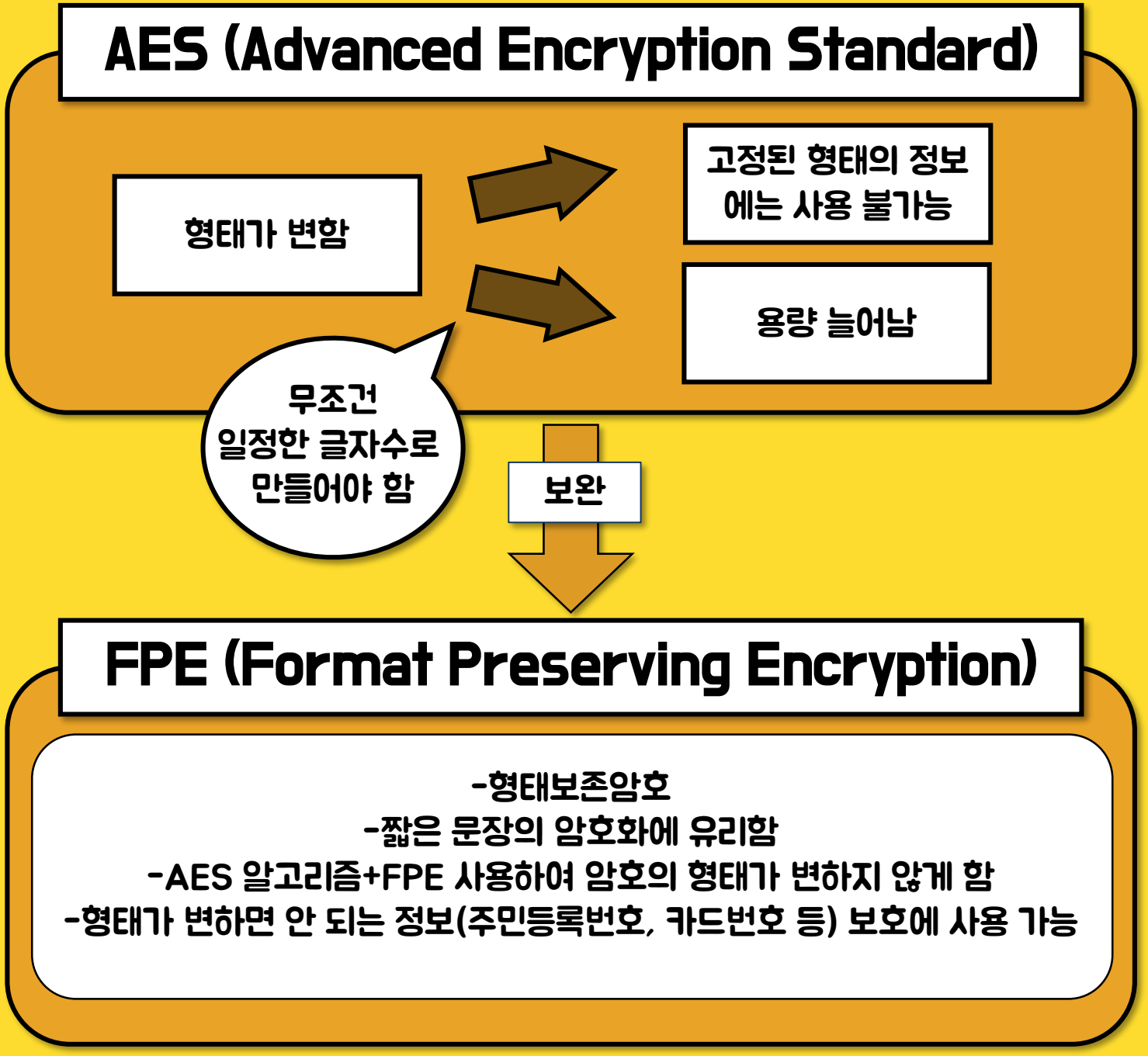
② hi (2글자) 확장 → h4lf5pge1o3pqkeo

- 용량 증가
- 형태 변함

-2바이트라면 글자를 무조건 16바이트로 확장한 다음 암호화해야함

-AES는 128, 192, 256비트가 있음 → 단문(4~8글자 등)은 용량이 아주 많이 증가


AES


AES (Advanced Encryption Standard)
형태가 변함
고정된 형태의 정보
에는 사용 불가능
용량 늘어남
무조건
일정한 글자수로
만들어야 함
보완
FPE (Format Preserving Encryption)
-형태보존암호
-짧은 문장의 암호화에 유리함
-AES 알고리즘+FPE 사용하여 암호의 형태가 변하지 않게 함
-형태가 변하면 안 되는 정보(주민등록번호, 카드번호 등) 보호에 사용 가능

형태가 변하면 안 되는 정보가 있다고?

주민등록번호 ○○○○○○ — ○○○○○○○

카드번호 ○○○○ — ○○○○ — ○○○○ — ○○○○

이메일주소 [ ] @ [.]

Abcdefg157 @ naver.com

형태보존암호 암호화 구조

1단계 평문 → [랭킹함수]

1-1단계 StrToNum

1-2단계 NumToBits

2단계 TBC 암호화

3단계 [역랭킹함수] → 암호문

3-1단계 BitsToNum

3-2단계 NumToStr

1단계 평문→랭킹함수

랭킹함수란?

-형 변환 함수 (문자 → 숫자 → 비트)

-평문과 암호문이 동일한 형태를 가지도록 함.

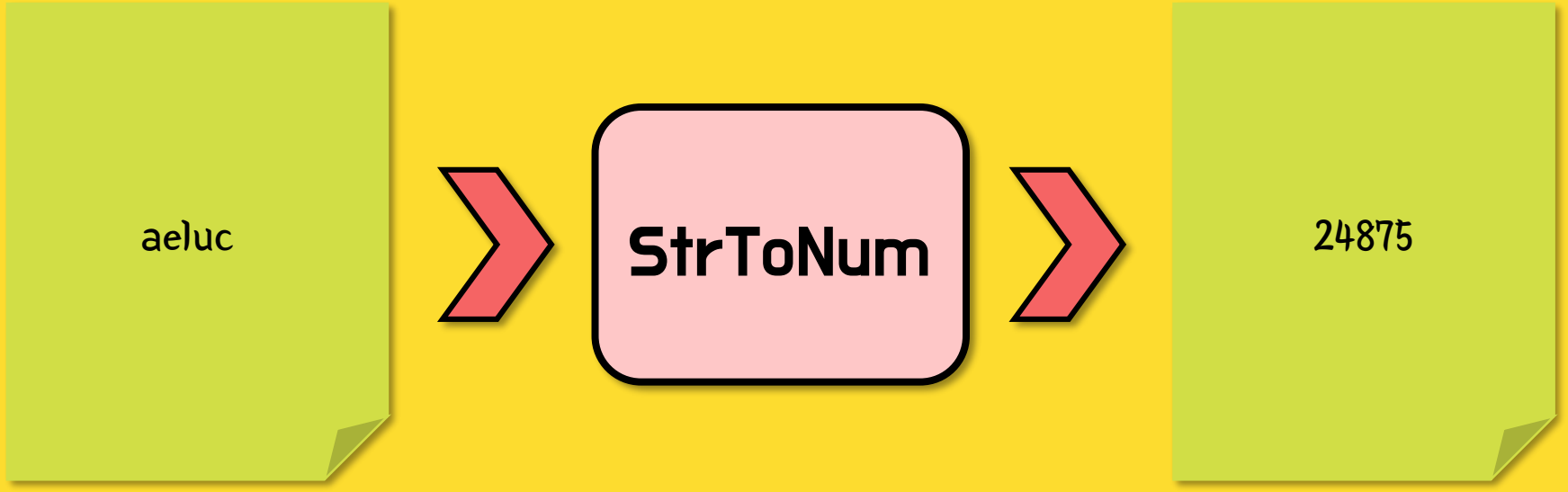
1. StrToNum

2. NumToBits

1-1 단계 StrToNum

StrToNum란?

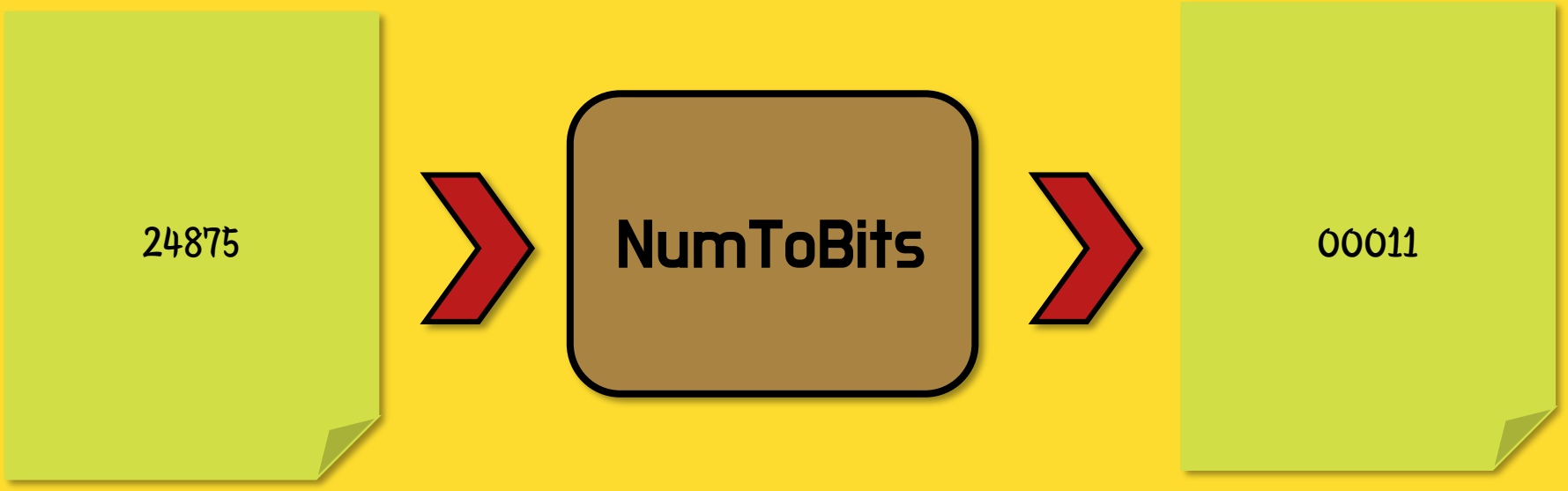
-문자(String)를 숫자(Number, 0~9)로 바꾸는 함수 (형 변환 함수)



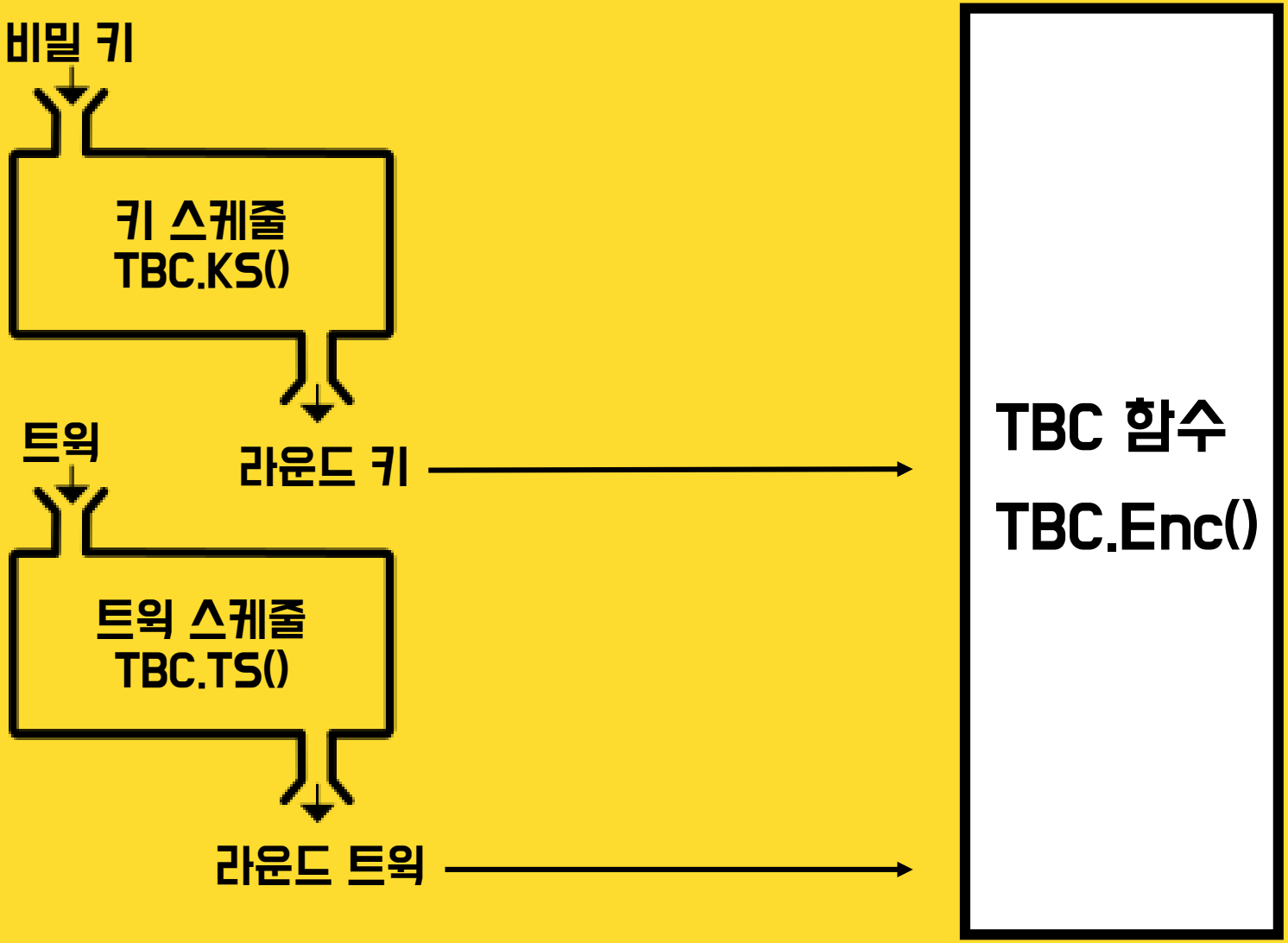
1-2 단계 NumToBits

NumToBits란?

-숫자(Number)를 비트(Bits)로 바꾸는 함수 (형 변환 함수)



2단계 TBC 암호화



비밀 키(Secret Key)란?

-암호화&복호화에 사용되는 비밀 정보

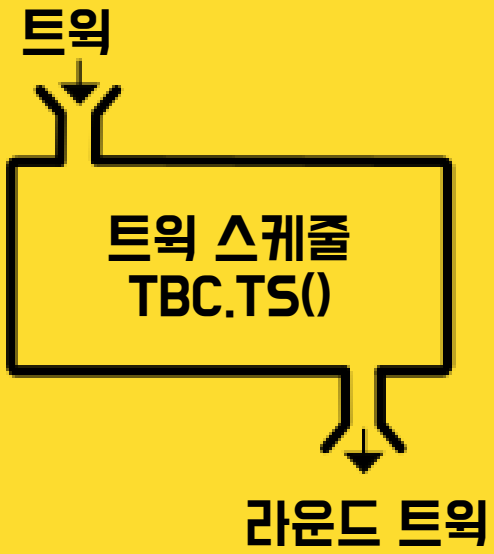
키 스케줄(Key Schedule)이란?

-비밀 키를 입력 받아 라운드 키를 생성하는 과정

-TBC.KS() 함수

라운드 키(Round Key)란?

-키 스케줄을 통하여 생성되는 값



트윅(Tweak)이란?

-암호 키(비밀 키)와 달리 비밀일 필요가 없음

-암호화&복호화에 사용되는 보조입력(부가정보)

-트윅이 바뀌면 암호문도 바뀜 →보안문제점 제거 가능

(평문이 짧을 때 암호문으로 평문을 유추할 수 있음)

트윅 스케줄(Tweak Schedule)이란?

-트윅을 입력받아 라운드 트윅을 생성하는 과정

-TBC.TS() 함수

라운드 트윅(Round Tweak)이란?

-트윅으로부터 트윅 스케줄을 통하여 생성되는 값

TBC 함수

TBC.Enc()

TBC 함수란?

- 암호화 과정에서 사용되는 함수
- 평문을 다른 사람들이 알 수 없는 패턴으로 바꿔주는 암호화 함수
- 라운드 트윅(Round Tweak) 과 라운드 키(Round Key)가 재료로 사용됨

3단계 역랭킹함수→암호문

역랭킹함수란?

-랭킹함수 과정을 반대로 진행하는 함수 (랭킹함수와 역함수 관계)

-형 변환 함수 (비트 → 숫자 → 문자)

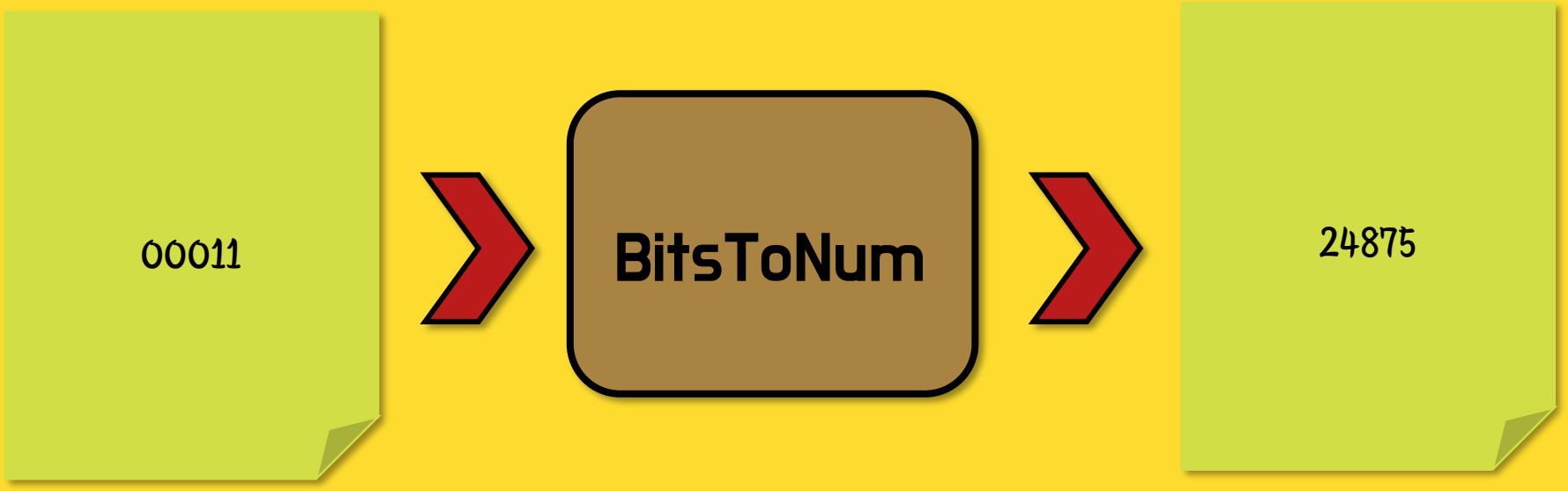
1. BitsToNum

2. NumToStr

3-1 단계 BitsToNum

BitsToNum이란?

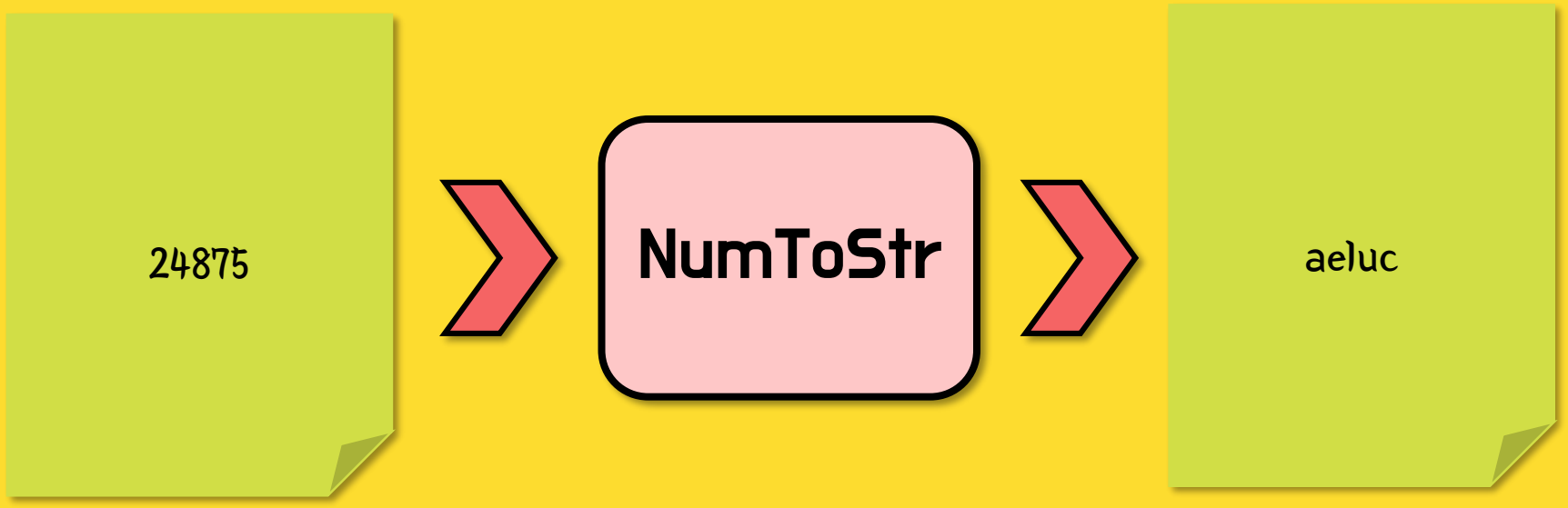
- 비트(Bits)를 숫자(Number)로 바꾸는 함수 (형 변환 함수)



3-1 단계 NumToStr

NumToStr란?

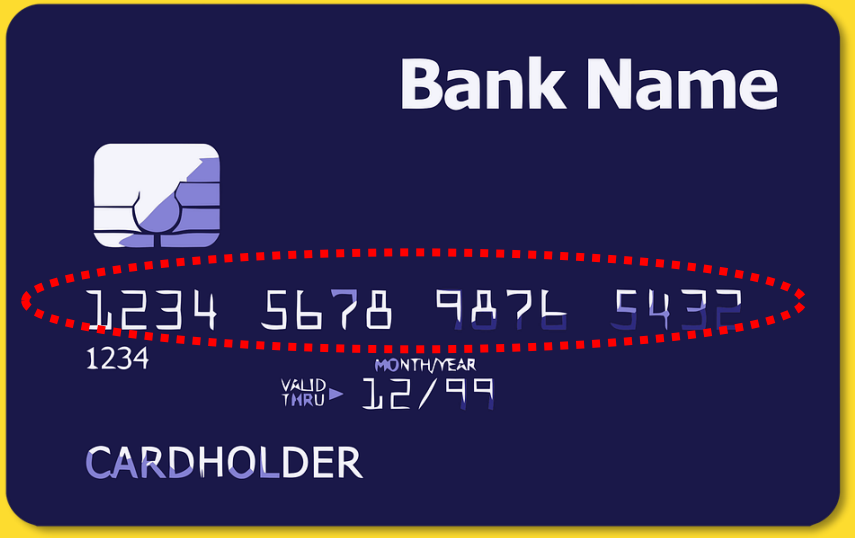
- 숫자(Number)를 문자(String)로 바꾸는 함수 (형 변환 함수)



형태보존암호 응용

① 주민등록번호

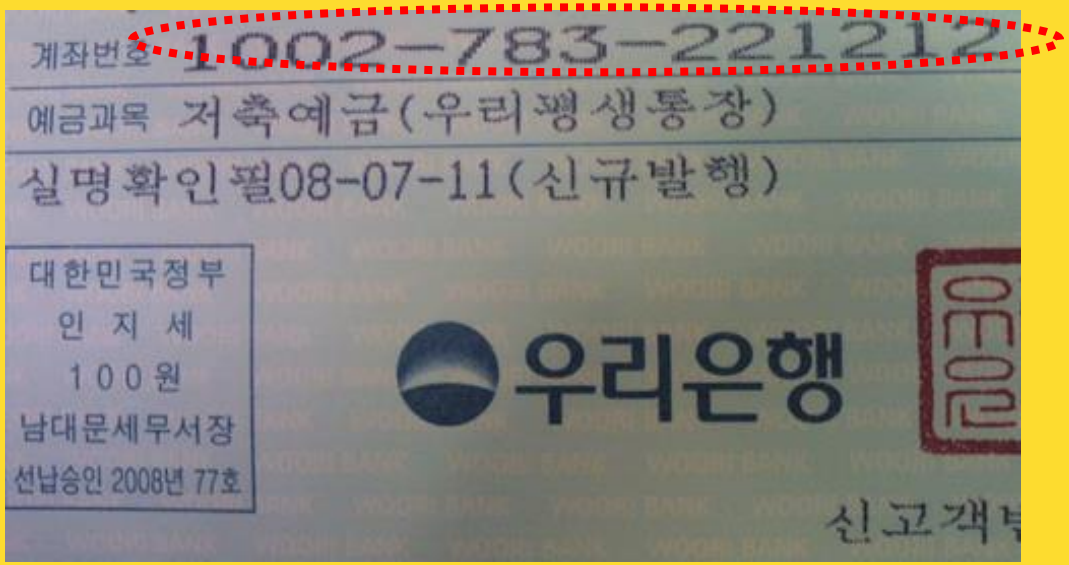
② 카드번호



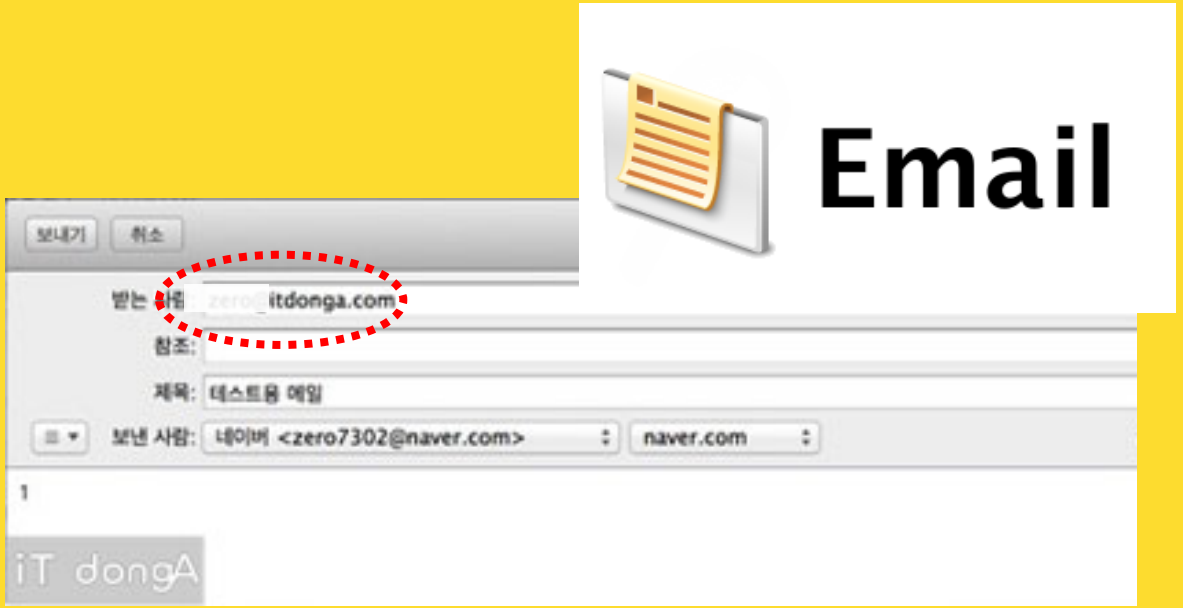
③ 여권번호


대 한 민 국
REPUBLIC OF KOREA
여 권
PASSPORT
대 한 민 국 REPUBLIC OF KOREA
여권 PASSPORT
2
타입/ Type
PD
발행국/ Issuing country
KOR
1
여권번호/ Passport No.
D12345678
성/ Surname
HONG
이름/ Given names
KIL DONG
국적/ Nationality
REPUBLIC OF KOREA
생년월일/ Date of birth
01 JAN 1975
주민등록번호/ Personal No.
1234567
성별/ Sex
M
발급일/ Date of issue
10 MAR 2008
발행관청/ Authority
MINISTRY OF FOREIGN AFFAIRS AND TRADE
기간만료일/ Date of expiry
10 MAR 2013
한글성명
홍길동
3
PDKORHONG<<KIL<DONG<<<<<<<<<<<<<<<<<<<<<<<<
D123456785KOR7501012M1303100123456 7V15788666
ČESKÁ REPUBLIKA/CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
TYP/TYPE/TYPE
P
KÓD/CODE/CODE
CZE
ČÍSLO PASU/PASSPORT NO./PASSEPORT NO
99009054
01 PŘÍJMENÍ/SURNAME/NOM
SPECIMEN
02 JMÉNO/GIVEN NAMES/PRÉNOM
VZOR
03 STÁTNÍ OBČANSTVÍ/NATIONALITY/NATIONALITÉ
ČESKÁ REPUBLIKA / CZECH REPUBLIC
04 DATUM NAROZENÍ/DATE OF BIRTH/DATE DE NAISSANCE
22.06.1969
11 RODNÉ ČÍSLO/PERSONAL NO./NO PERSONNEL
695622/0612
06 MÍSTO NAROZENÍ/PLACE OF BIRTH/LIEU DE NAISSANCE
PRAHA 1
05 POHLAVÍ/SEX/SEXE
F
07 DATUM VYDÁNÍ/DATE OF ISSUE/DATE DE DÉLIVRANCE
29.07.2006
08 PLATNOST DO/DATE OF EXPIRY/DATE D'EXPIRATION
29.07.2016
10 PODPIS DRŽITELE
HOLDER'S SIGNATURE
SIGNATURE DU TITULAIRE
SPECIMEN
P<CZESPECIMEN<<VZOR<<<<<<<<<<<<<<<<<<<<<<<<
99009054<4CZE6906229F1607299695622061 2<<<<74

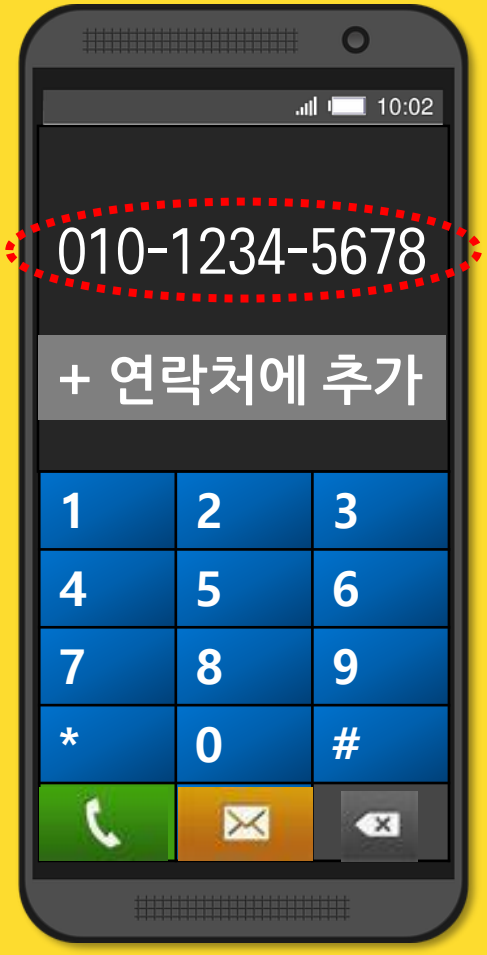
④ 계좌번호


계좌번호 1002-783-221212
예금과목 저축예금(우리평생통장)
실명확인필08-07-11(신규발행)
대한민국정부
인 지 세
100원
남대문세무서장
선납승인 2008년 77호
우리은행
신고객

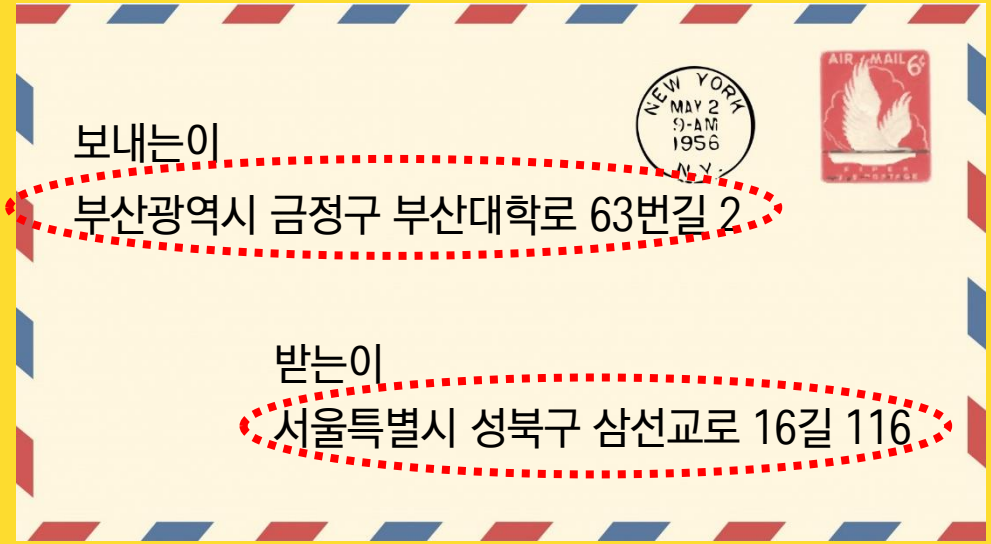
⑤ 이메일


Email
보내기
취소
받는 사람
itdonga.com
참조:
제목: 테스트용 메일
보낸 사람: 네이버 <zero7302@naver.com>
naver.com
1
iT dongA

⑥ 전화번호


10:02
010-1234-5678
+ 연락처에 추가
1
2
3
4
5
6
7
8
9
*
0
#

⑦ 주 소


NEW YORK
MAY 2
9-AM
1956
AIR MAIL 6
보내는이
부산광역시 금정구 부산대학로 63번길 2
받는이
서울특별시 성북구 삼선교로 16길 116

QUIZ TIME

QUIZ TIME

1. 일상적으로 사용하는 문장을 뜻하는 이것은 무엇일까요?

(Hint)
암호화하기 전 또는 암호문을 해독한 문장을 뜻합니다.

Answer

평문

QUIZ TIME

2. 비트는 1과 2만 사용한다. [O/X]

Answer

X

〈해설〉

비트는 데이터를 나타내는 최소단위로
0과 1만 사용한다.

QUIZ TIME

3. DES는 AES의 키길이가 너무 짧아 보안에 취약하다는 단점을 보완하기 위해 등장하였다. [O/X]

Answer

X

〈해설〉

DES의 키길이는 56비트로 너무 짧아 보안에 취약했기 때문에 이를 보완하기 위해 AES가 등장하였다.

QUIZ TIME

4. 형태가 변한다는 AES의 단점을 보완하기 위해 등장한 암호화 알고리즘은?

(Hint)
형태가 변하면 안 되는 정보 보호에 사용이 가능하다.

Answer

형태보존암호 or FPE

QUIZ TIME

5. 형태보존암호 과정 중 숫자를 비트로 변환시켜주는 함수의 이름은 무엇일까요?

(Hint)
-숫자는 영어로 Number이다.

Answer

NumToBits

QUIZ TIME

6. 트윅(Tweak)은 평문 길이가 짧을 때, 암호문을 통해 평문을 유추할 수 있다는 문제점을 제거해준다. [OX]

Answer

O

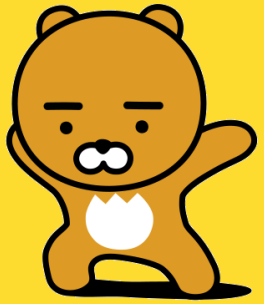
〈해설〉

보조입력으로 사용되는 트윅(Tweak)은 변경 될 때마다 암호문이 달라진다.

이로 인해 문제점(암호문을 통해 평문을 유추)을 제거할 수 있다.

QUIZ TIME

7. 카드번호, 주민등록번호 등은 형태가 변하면 안 되는 정보에 속한다. [O/X]



Answer

O

〈해설〉

카드번호, 주민등록번호 등은 형태가 고정되어 있기 때문에, 형태가 변해 용량&길이가 늘어날 경우 문제가 발생할 수도 있다.

QUIZ TIME

8. 실생활에서 형태보존암호가 쓰인 사례 3가지를 말해보세요.

Answer

카드번호, 주민등록번호, 여권번호
이메일, 주소, 전화번호, 계좌번호
中 3개

더 알아보기 +

형태 보존 암호화 관련 오픈 소스 라이브러리

python, C/C++, Java, .net 등 다양한 플랫폼 기반의 FPE 오픈 소스 라이브러리 존재 (<표 1>참조)

라이브러리	설명	라이선스
LibFTE	Python 기반의 FFX(FF1) 라이브러리	MIT
Libffx	Python 기반의 FFX(FF1) 라이브러리	GPL
Botan(FPE)	C++ 기반의 FE1 라이브러리	BSD2
Miracl	C/C++ 기반의 BPS 라이브러리	상업 라이선스 및 AGPL
DotFPE	.net 기반의 FE1 라이브러리	NewBSD
JavaFPE	Java 기반의 FE1 라이브러리	NewBSD

<표1> FPE 관련 오픈 소스 라이브러리

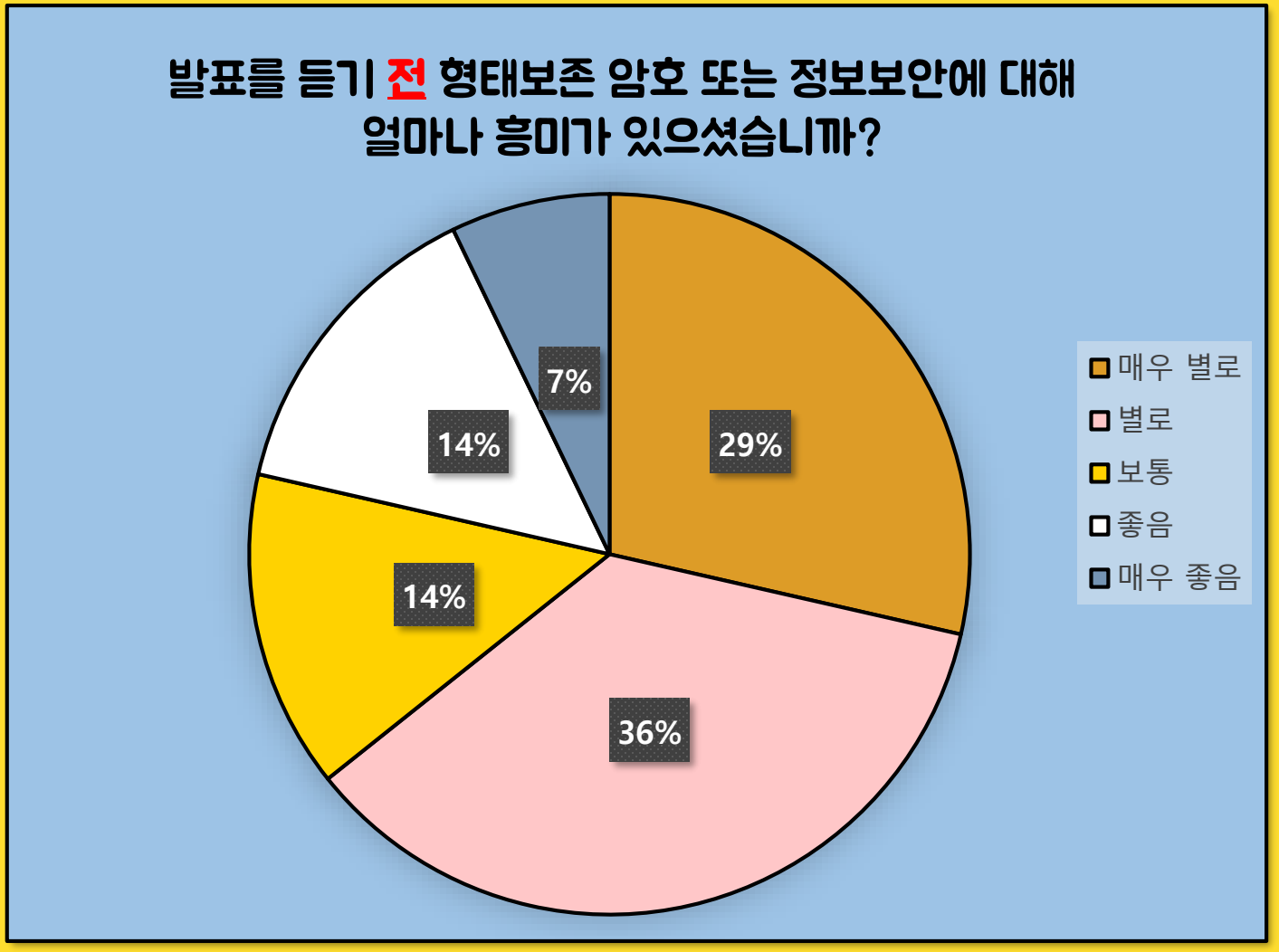
Bye

수고하셨습니다

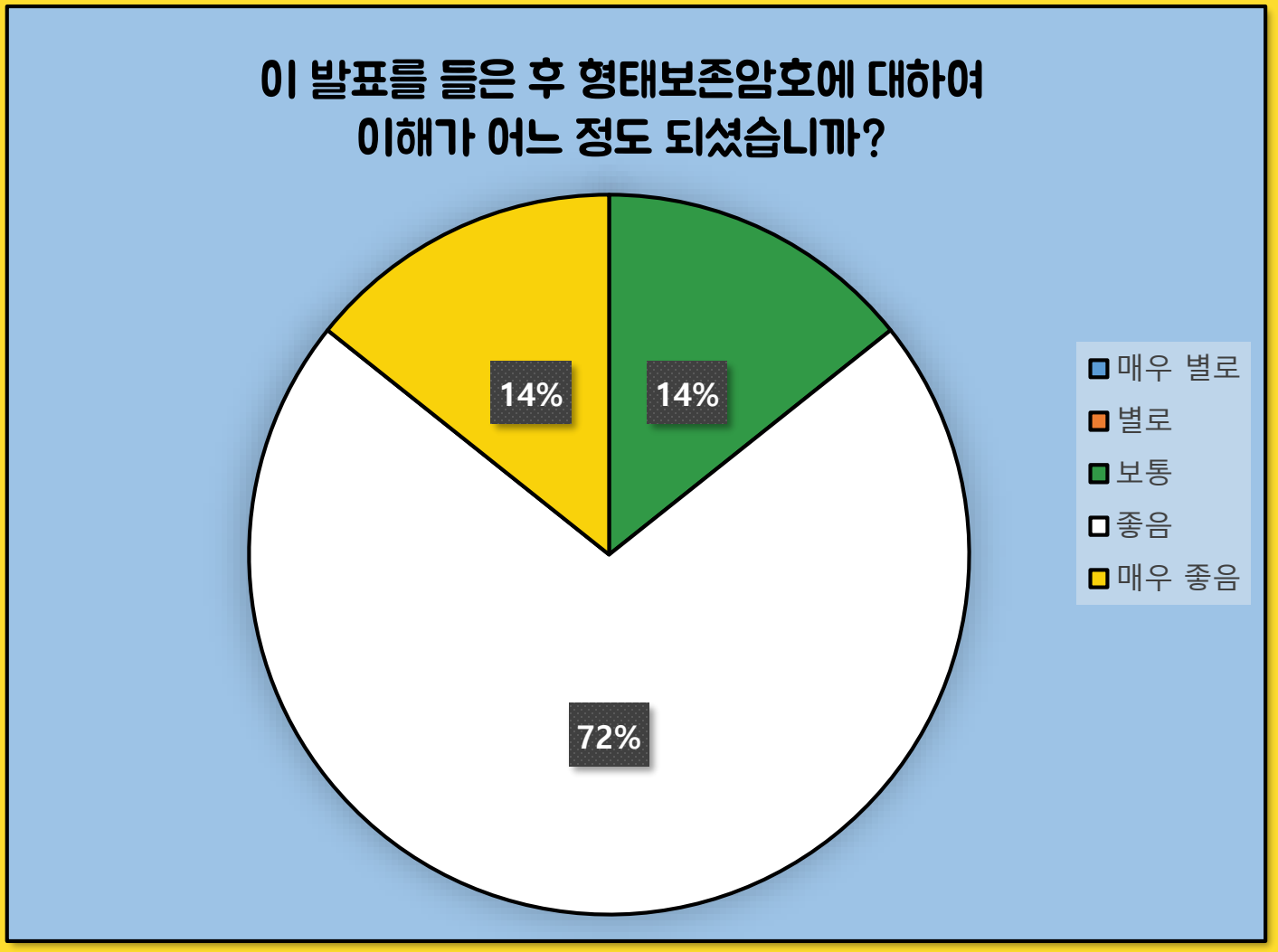
발표

〈 사진 〉 중고등학생 14명 앞에서 발표하는 모습

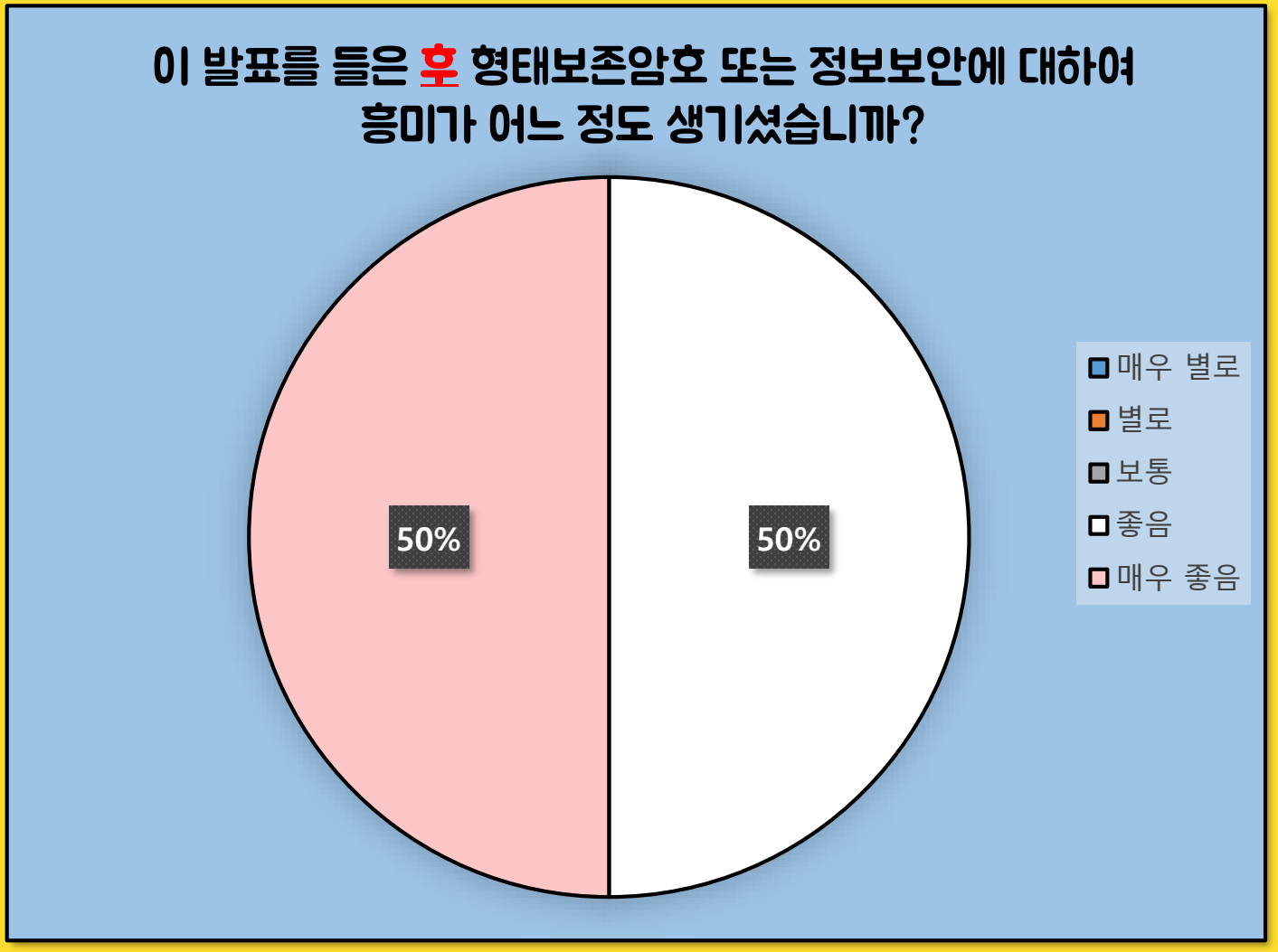
결과



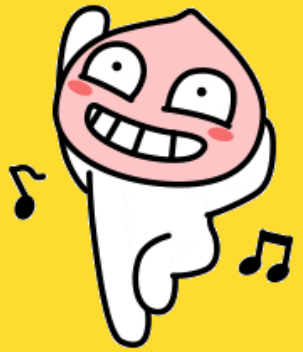
발표 이전에는 형태보존암호 또는 정보보안에
보통을 제외하고 61% 가량이 관심이 없다고 답변.

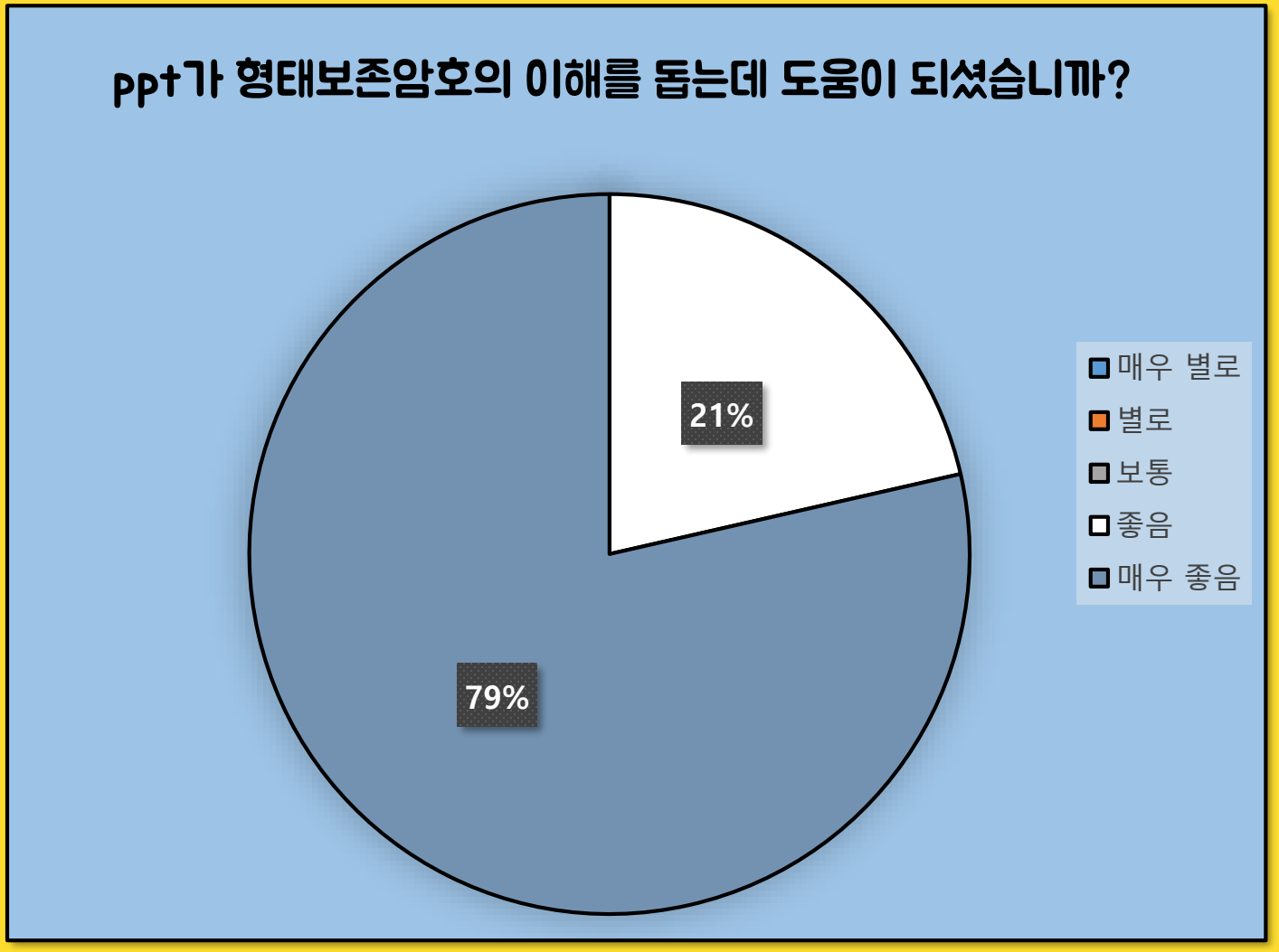


발표 후 대부분의 학생들이 이해를 했다고 답변.

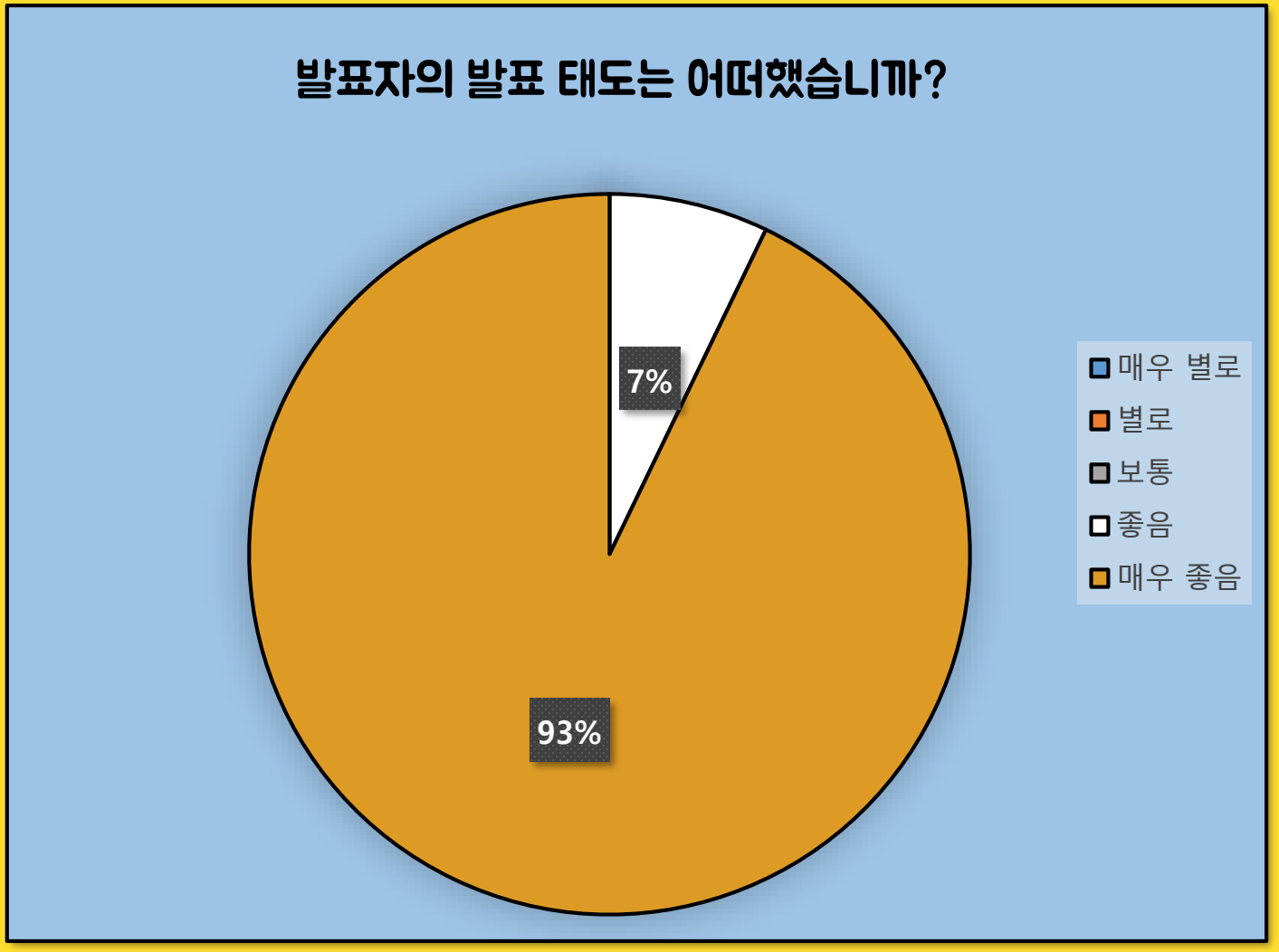


발표 후 대부분의 학생들이
형태보존암호 또는 정보보안에 관심이 생겼다고 답변.





발표 후 대부분의 학생들이
ppt가 형태보존암호 이해에 도움이 되었다고 답변.



대부분의 학생들이 발표자의
발표 태도에 만족한다고 답변.

Bye

들어주셔서 감사합니다!