# Capstone Design 2조

Enhanced Security Delivery Algorithm

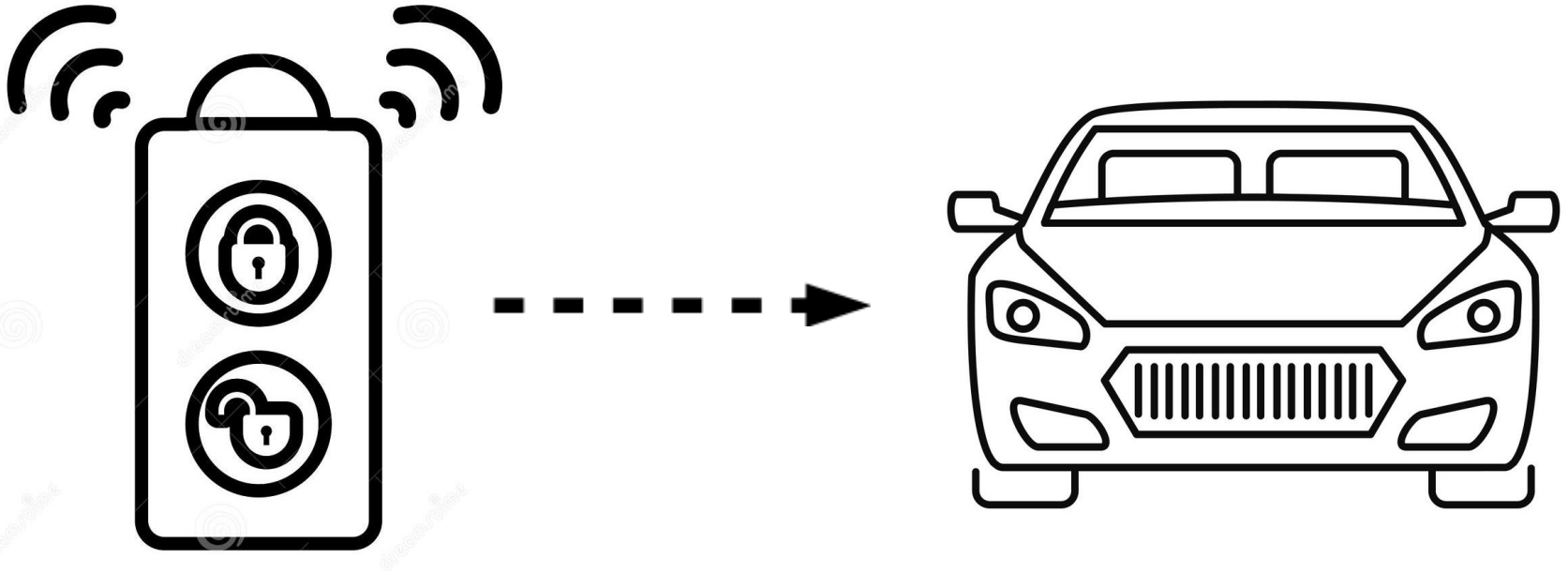
20125502 김계홍
20164293 송서연
20165050 이새벽
20165060 임지민
20165048 허유나

# Task Overview

**Create encryption programs using public keys and symmetric keys for more reliable security**

# Motivation of task

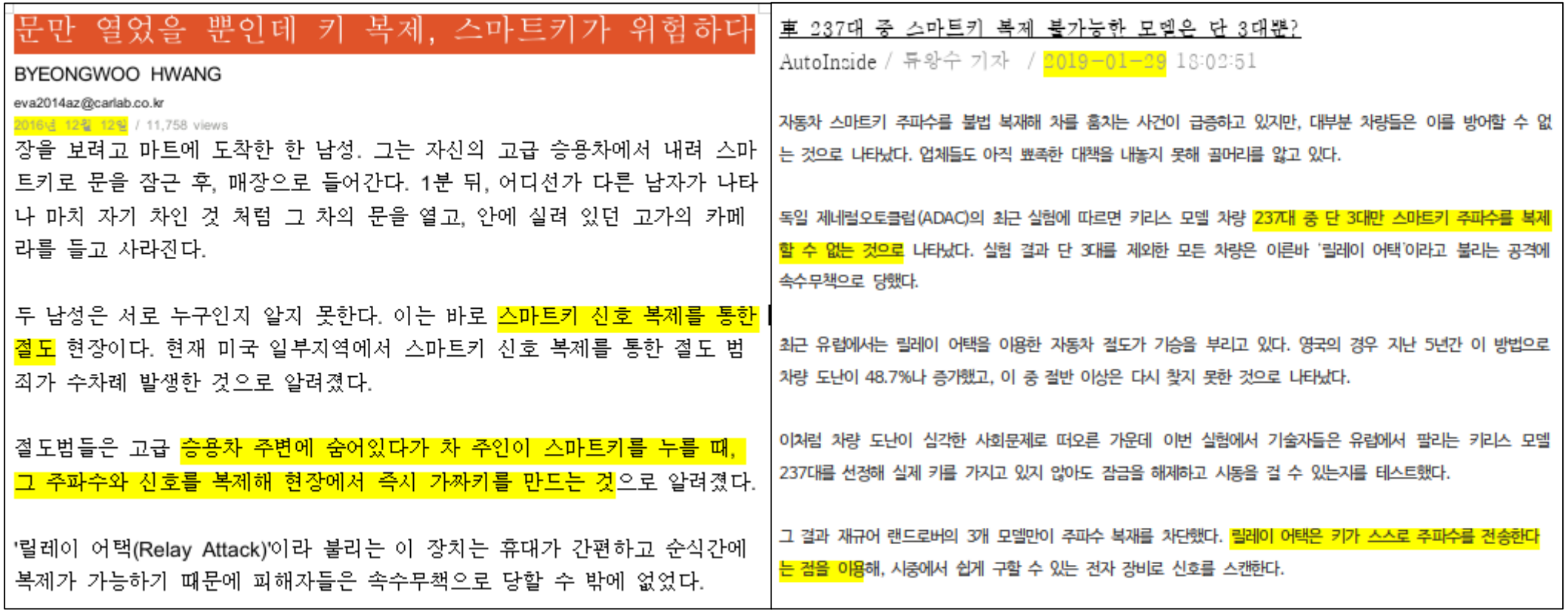
❖Immobilizer



- Each vehicle has its own unique information.
- Radio wave recognition Through communication between antennas.
- Known to ensure high security.

# Motivation of task

* Constant threat from hacking



## 문만 열었을 뿐인데 키 복제, 스마트키가 위험하다

BYEONGWOO HWANG

eva2014az@carlab.co.kr

2016년 12월 12일 / 11,758 views

장을 보려고 마트에 도착한 한 남성. 그는 자신의 고급 승용차에서 내려 스마트키로 문을 잠근 후, 매장으로 들어간다. 1분 뒤, 어디선가 다른 남자가 나타나 마치 자기 차인 것 처럼 그 차의 문을 열고, 안에 실려 있던 고가의 카메라를 들고 사라진다.

두 남성은 서로 누구인지 알지 못한다. 이는 바로 스마트키 신호 복제를 통한 절도 현장이다. 현재 미국 일부지역에서 스마트키 신호 복제를 통한 절도 범죄가 수차례 발생한 것으로 알려졌다.

절도범들은 고급 승용차 주변에 숨어있다가 차 주인이 스마트키를 누를 때, 그 주파수와 신호를 복제해 현장에서 즉시 가짜키를 만드는 것으로 알려졌다.

'릴레이 어택(Relay Attack)'이라 불리는 이 장치는 휴대가 간편하고 순식간에 복제가 가능하기 때문에 피해자들은 속수무책으로 당할 수 밖에 없었다.

## 車 237대 중 스마트키 복제 불가능한 모델은 단 3대뿐?

AutoInside / 듀왕수 기자 / 2019-01-29 18:02:51

자동차 스마트키 주파수를 불법 복재해 차를 훔치는 사건이 급증하고 있지만, 대부분 차량들은 이를 방어할 수 없는 것으로 나타났다. 업체들도 아직 뾰족한 대책을 내놓지 못해 골머리를 앓고 있다.

독일 제네럴오토클럽(ADAC)의 최근 실험에 따르면 키리스 모델 차량 237대 중 단 3대만 스마트키 주파수를 복제할 수 없는 것으로 나타났다. 실험 결과 단 3대를 제외한 모든 차량은 이른바 '릴레이 어택'이라고 불리는 공격에 속수무책으로 당했다.

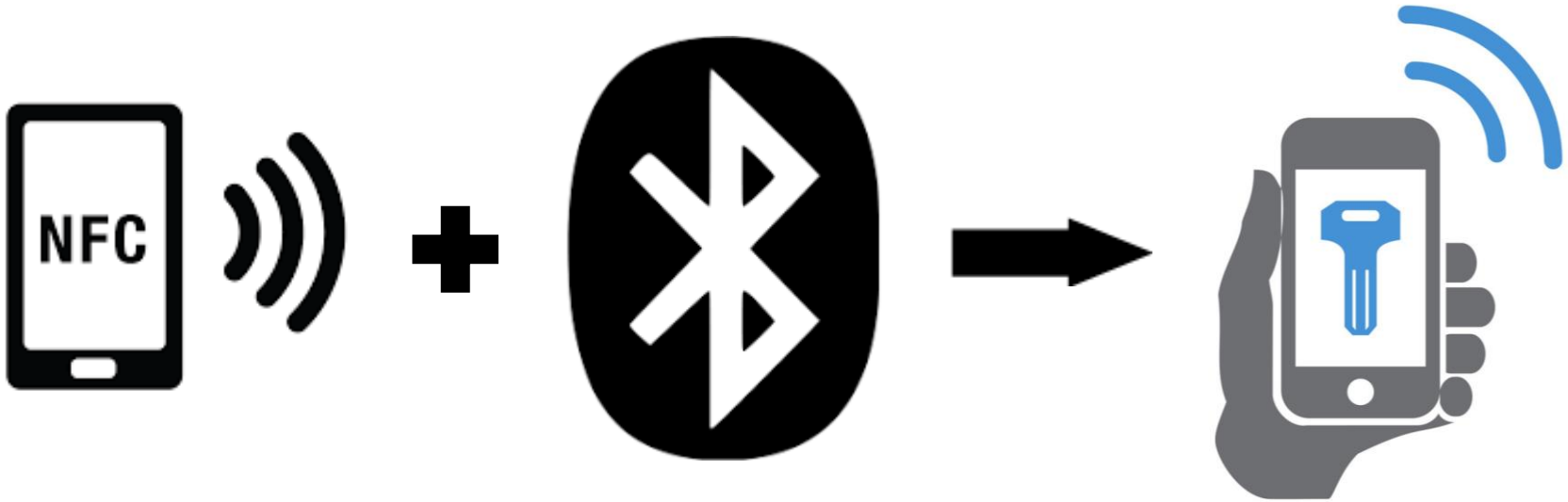
최근 유럽에서는 릴레이 어택을 이용한 자동차 절도가 기승을 부리고 있다. 영국의 경우 지난 5년간 이 방법으로 차량 도난이 48.7%나 증가했고, 이 중 절반 이상은 다시 찾지 못한 것으로 나타났다.

이처럼 차량 도난이 심각한 사회문제로 떠오른 가운데 이번 실험에서 기술자들은 유럽에서 팔리는 키리스 모델 237대를 선정해 실제 키를 가지고 있지 않아도 잠금을 해제하고 시동을 걸 수 있는지를 테스트했다.

그 결과 재규어 랜드로버의 3개 모델만이 주파수 복재를 차단했다. 릴레이 어택은 키가 스스로 주파수를 전송한다는 점을 이용해, 시중에서 쉽게 구할 수 있는 전자 장비로 신호를 스캔한다.

# Motivation of task

❖SmartPhone key




- Provide the same functionality as existing smart keys
- Eliminate the inconvenience of carrying keys
- Can share keys with others

# Motivation of task

## 속속 드러나는 자동차 모바일 앱의 해킹 취약성

카가이 취재팀 | 승인 2017.04.26 18:00 | 댓글 0

지난 25일, 캐나다 보안회사 래피드7(Rapid7)는 현대자동차 블루링크의 보안 취약성을 이용해 원격으로 차량 시동을 거는 데 성공했다고 발표했다. 이 취약성을 이용, 사용자이름·비밀번호·PIN번호·GPS위치기록 등 민감한 정보의 탈취도 가능하다고 한다. 래피드7는 '지난해 12월 8일 자 업데이트 파일에 포함된 버그(bug)를 이용했다'라고 덧붙였다.

현대자동차는 '3월 초, 패치를 통해 이 문제를 해결했다'고 밝혔다. 또 이와 관련해 '도난 사고 등이 보고된 것은 없다'라고 말했다.

최근 스마트폰 해킹, 스마트키 신호 조작 등 첨단 기술을 이용한 자동차 범죄에 대한 논의가 활발하다. 2015년 피아트 크라이슬러의 리콜은 이것이 충분히 가능한 일이고 심각할 수 있다는 것을 보여줬다. 당시 미국에서 140만 대 이상 회수돼 소프트웨어 패치를 받았다. 이것은 미국의 한 보안업체가 지프 체로키의 유 커넥트 인포테인먼트 시스템을 해킹해 10마일 이상 떨어진 곳에서 차량을 제어한 이후의 일이다. 같은 해 GM은 해킹 가능성이 있다며 차량용 OnStar 통신 시스템에서 유사한 버그를 수정했다.

# Task goals

- Integrate new code into existing methods of comparing communication between one key or the antennas attached to each device to provide safer and more reliable security than traditional products.

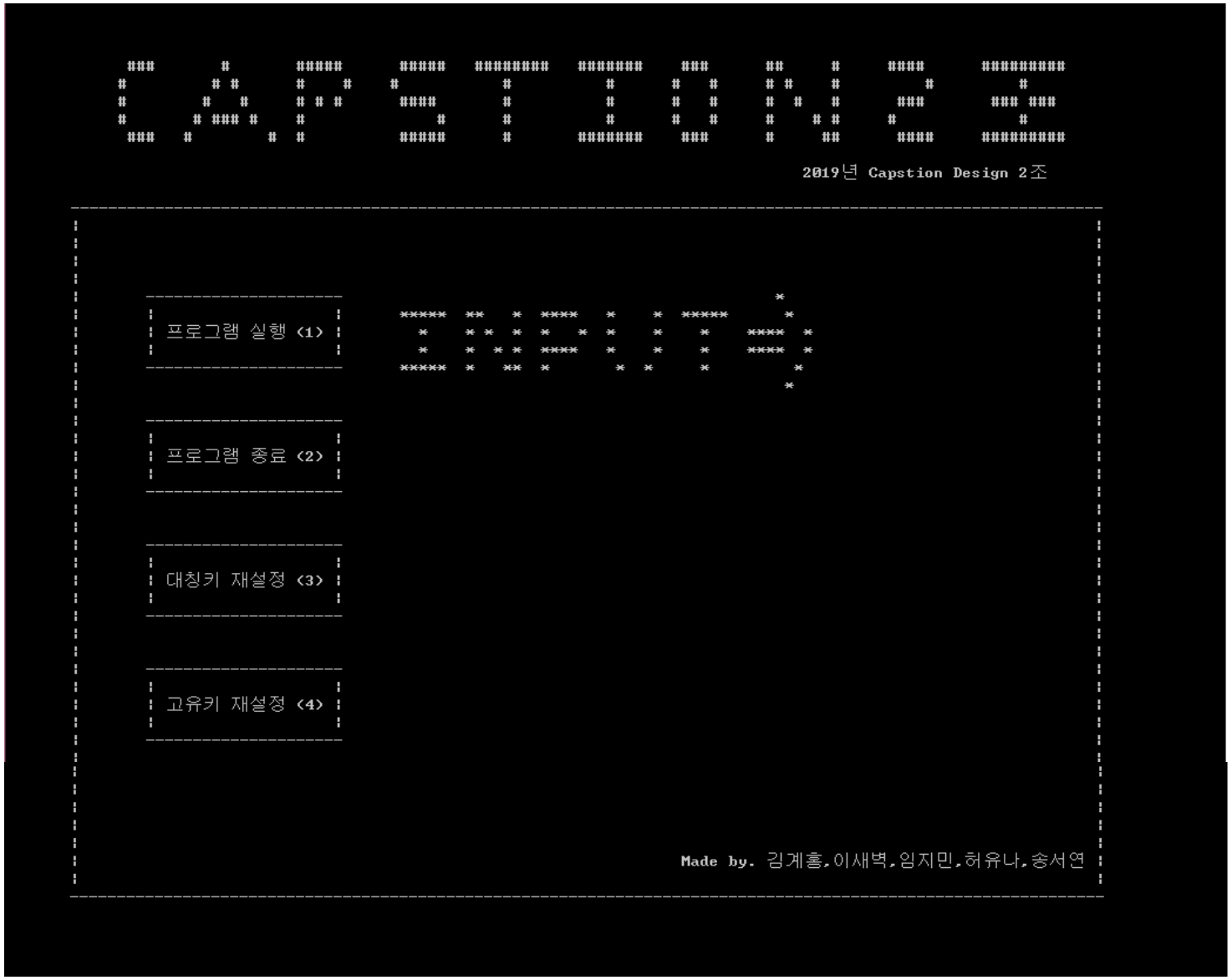
- Allow only authorized persons to obtain authority.

- Team members perform their roles through collaboration to suit their learning objectives of ‘Analyzing Vulnerabilities in Different Domains, Designing Security Technologies and Analyzing Security’.

# Task schedule

<table>
<tr><th></th><th colspan="2">April</th><th colspan="2">May</th><th>Juen</th></tr>
<tr><td>김계홍</td><td colspan="2">Design program</td><td colspan="2">Project license management</td><td>Program combine and management,<br>Add modifications</td><td>Vulnerability analysis</td></tr>
<tr><td>송서연</td><td colspan="3">Create and publish proposals</td><td colspan="3">Git Project Management and Program Documentation Operations</td></tr>
<tr><td>이새벽</td><td rowspan="3" colspan="2">Create symmetric key</td><td colspan="2">Creating an arbitrary value-creating program</td><td>Create symmetric key cryptographic document generation program</td><td rowspan="3">Code modification and Vulnerability analysis</td></tr>
<tr><td>임지민</td><td colspan="2">Creating an random key-reading program</td><td>Adjust text file output position</td></tr>
<tr><td>허유나</td><td colspan="2">Create random key symmetric key insertor</td><td>Adjust text file input position</td></tr>
</table>

# Task result - Task contents



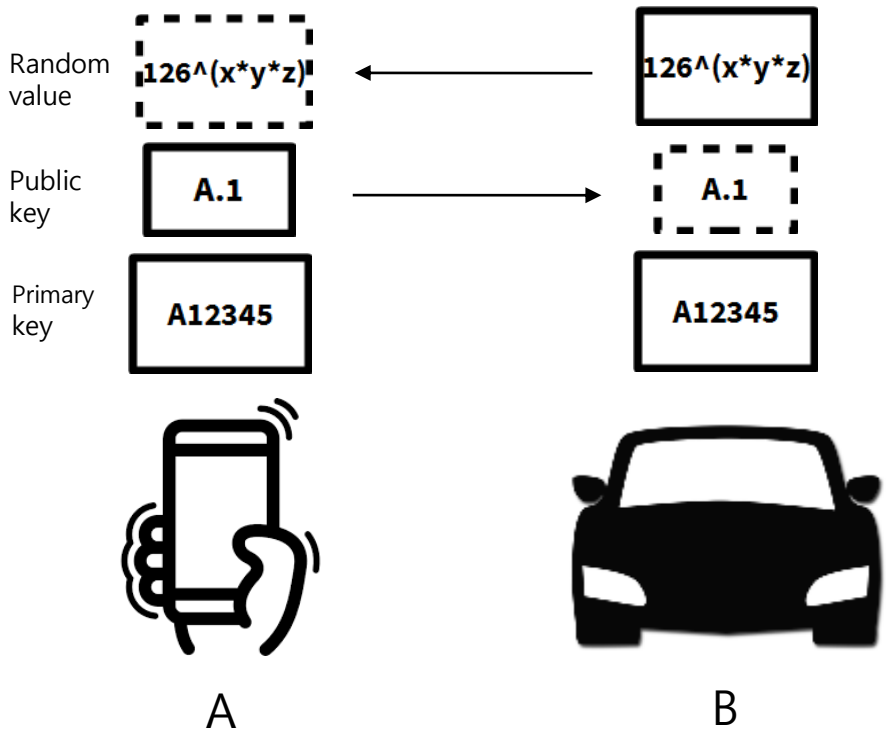
# Task result - Process

- In this document, the sender is referred to as A and the receiver is referred to as B.
- Because A and B are symmetric key structures, internal keys are assumed to be symmetrical already.

1. A uses the public key using digital signature to certify users to B.
   (The digital signature method is not described as A relationship that is not significantly related to this algorithm method)

2. When B is user-certified in A, it generates an random value of 126^(x*y*z), stores it inside B, and sends it to A.
   The random value is expressed as the ASCII value with a range of 1 to 127.
   0 is excluded from random value generation because 0 refers to NULL value.

3. Symmetric keys internally consist of the Unique Key(Array[a]), 3D arrangement(Array[z][y][x]), and arraystarting points ( Array_starting_point[z][y][x] * a ).



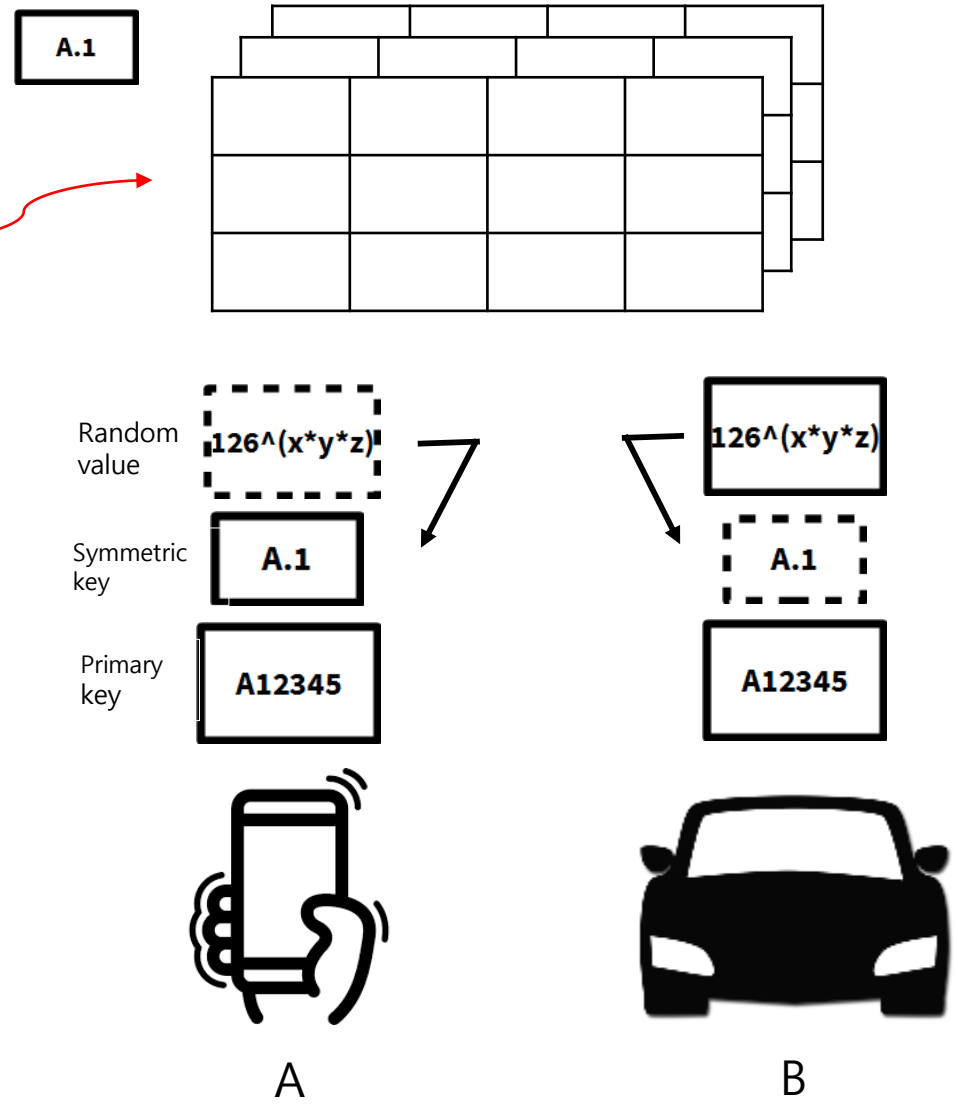
# Task result - Process

4. A and B substitute the inputted random value(126^x*y*z) for the 3D arrangement (Array[z][y][x]).

5. Only x-coordinates of the array_starting_point ( Array_starting_point[z][y][x] * a ) are x++ and random values applied to the 3D arrangement are compared with the unique key.

6. If the x-coordinate of the array starting point ( Array_starting_point[z][y][x] * a ) is x > 9, x, y, and z are switched and repeated a total of three times.

7. Internally there is a safety_counter when compares each array starting point (array_starting_point[z] [y] * a ) with a unique key (Array[a]).
(Switching order is 1,2,3 -> 3,1,2 -> 2,3,1.)

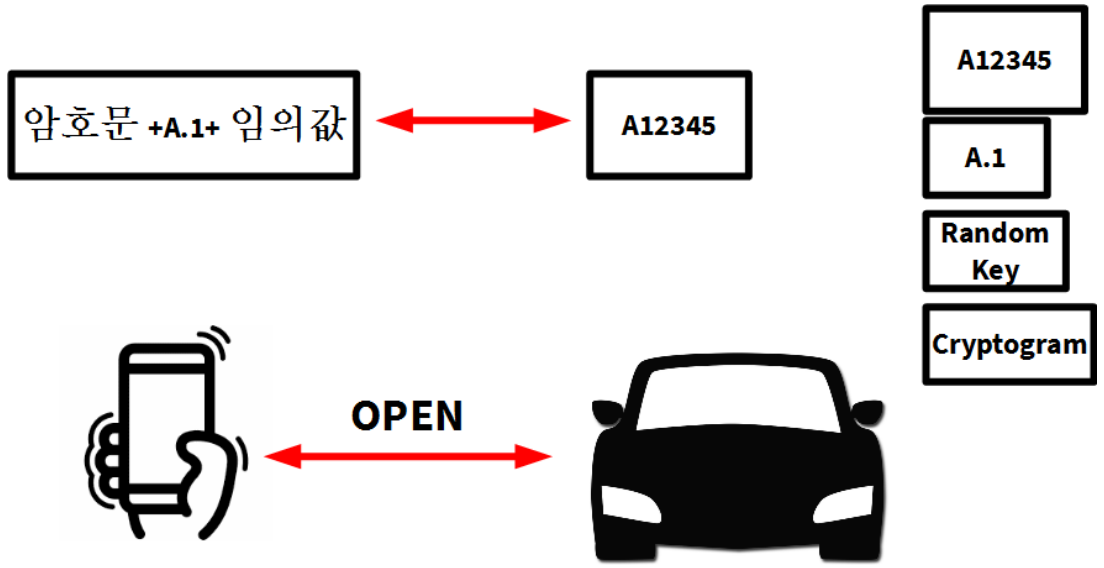


# Task result - Process

8. ArrayStarting points (Array_starting_point[z][y][x] * a ) are each matched to the address of unique keys.
   And ArrayStarting points (Array_starting_point[z][y][x] * a ) outputs '1' if it matches and '0' if it doesn't when it compared to 3D array.

9. A transmits the created cryptogram to B.

10. B compares the cryptogram of B with the cryptogram received from A and returns 1 if it matches and 0 if it does not.



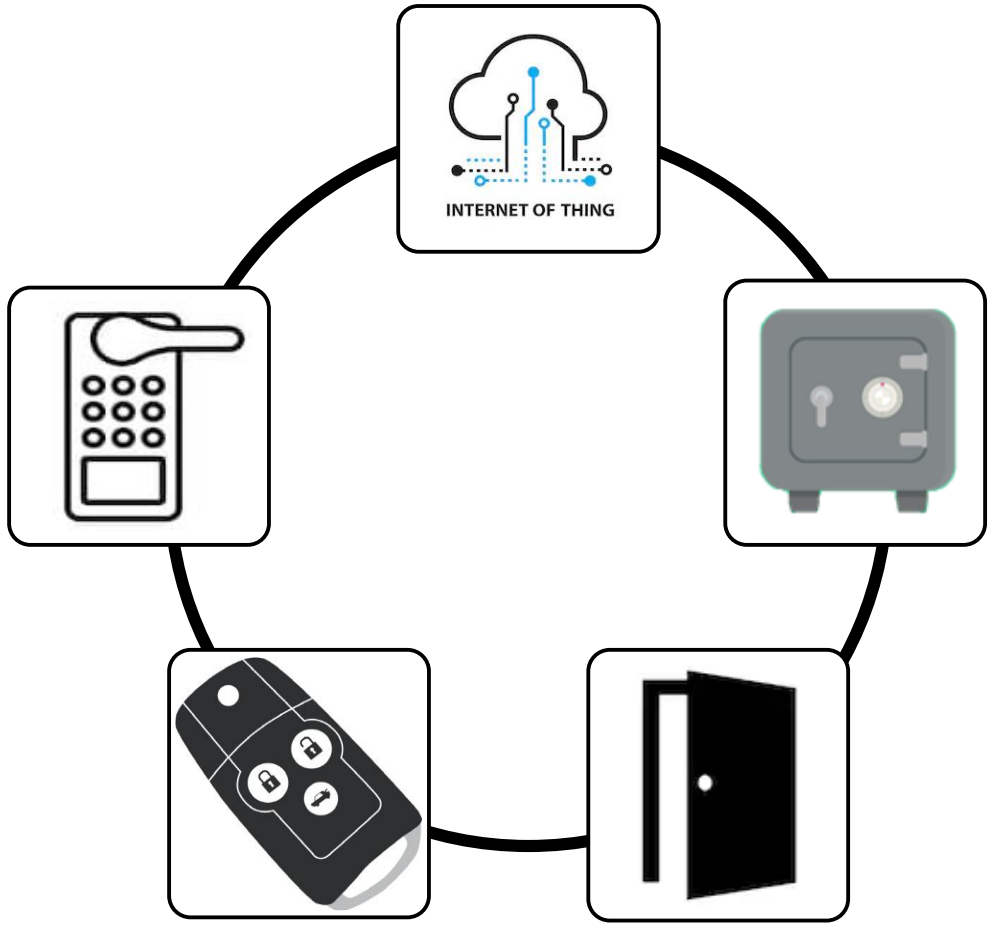
# Task result - Task contents

# Task result - Task contents

# Task result - Task contents

# Task result - Task contents

# Task result - Expected effects




If the program's stability through the algorithm is guaranteed, it applies to all areas that act as smart keys.

So far our group's goal is to use encryption program as a key application of car keys.

Convenience remote control key application that protects personal information and provides.

# Q&A