Group 4 - PadLock Messaging

Hexi Huang, Weishen Liu,
Andrew Samuelson, Saarah Kothawala

Introduction

Due to the fact that ID can be fake, people can change how they look and messages can be stolen, **nothing is absolute safe**. But on the other hand, there are still **tasks** we need to do **privately**, such as messaging and duties. We need a safe way to **confirm the object is the right person**, therefore, we try to develop the **One Time Pad communication and identification tool** in order to make it as save as possible.

Solution

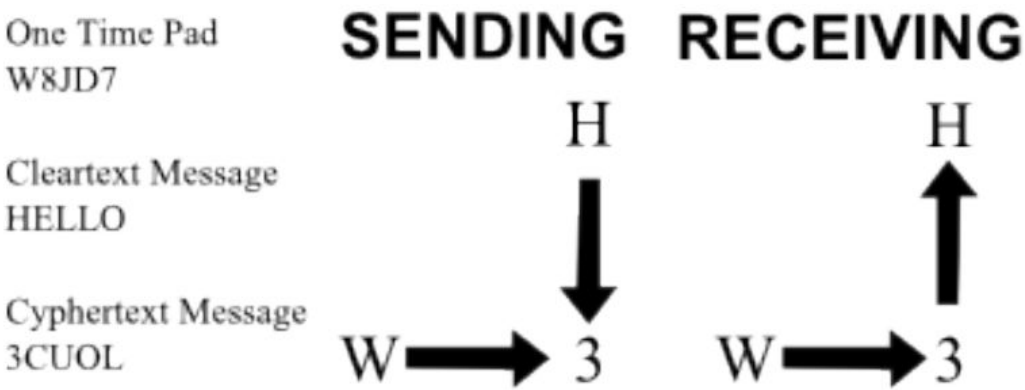
We are trying to build a tool to help two sides to confirm their identity. We are using **One Time Pad** for the tool (ex. Matching the ID number / secret word that both sides agree on).

1. Security officers take term
2. Bankers and transferring money
3. Police officers confirming each other's identities

One Time Pad

One Time Pad is an symmetric encryption method, and One Time Pad is very secure because in order to get the right message, it requires the same one time pad key and one time pad table.

	A	B	C	D	E	F	G	H
A	A	B	C	D	E	F	G	H
B	B	C	D	E	F	G	H	I
C	C	D	E	F	G	H	I	J
D	D	E	F	G	H	I	J	K
E	E	F	G	H	I	J	K	L
F	F	G	H	I	J	K	L	M
G	G	H	I	J	K	L	M	N
H	H	I	J	K	L	M	N	O



Modes

1. Identification Mode: Use the message in the QR code with decryption to see is the message is reasonable
2. Chat Room Mode: Let people can talk to one to one privately with encryption / decryption in One Time Pad (future development)

Processes - Identification Mode

There are 3 inputs and 1 output:

1. Inputting One Time Pad table elements
2. Inputting One Time Pad key
3. Inputting message
4. Outputting message / QR code

Expectation - Identification Mode

We are expecting the products will have the five features:

1. Generate the One Time Pad table
2. Generate the One Time Pad key randomly
3. Store / Reused the previous One Time Pad table
4. Encryption message
5. Decryption message
6. Covert message to QR code

Demo - Identification Mode

https://drive.google.com/file/d/1d4AabEHo820x7nAK5A5caaHx0p3ROKgN/view?usp=sharing

Feature Steps

- Chat Room Mode: contain chat room, message back and forth
- Random One Time Pad key generation
- UI Design on iOS, Android or Web platform for the users into Chat Room Mode and Identification Mode

Chat Room Mode Demo ->

https://drive.google.com/file/d/1XkLljvGqIoVWIoLdfFaI8Nr2ro3pOjSi/view?usp=sharing

Thank you so much for your time!