Livrable 4 : Strongbox 3000

Equipe 10 : BAL Aboubacry, RAKOTONIRINA Tony, MARTIN Léo, VAUDRY Garance, LESSUEUR Enzo, GERVILLIERS Maxence.

Sommaire :

1. Contexte :

À la suite de la création des niveaux d'authentifications de sécurité de notre sur flowgorithm, nous allons maintenant transcrire ces algorigrammes en code Arduino.

2. Code Arduino :

Circuit design Livrable 4 equipe 10 | Tinkercad

3. Quelques notions à savoir :

`encrypt()` : Fonction pour chiffrer un message.

`setup()` : Cette fonction est utilisée pour configurer les broches de la carte Arduino et initialiser la communication série.
`loop()` : C'est la boucle principale du programme. Elle attend l'entrée d'un code et, en fonction de celui-ci, appelle différentes fonctions de vérification d'authentification pour ouvrir le coffre-fort en plusieurs étapes, activant les différentes couches de sécurité (LEDs représentant les niveaux de sécurité).

4. Explications :

A. Initialisation des variables :

```
void setup()
```

Cette fonction est exécutée une seule fois au démarrage du programme. Elle est utilisée pour effectuer les initialisations nécessaires. Dans ce cas :

```
Serial.begin(9600)
```

Initialise la communication série à une vitesse de 9600 bauds.

```
randomSeed(analogRead(0))
```

Initialise le générateur de nombres aléatoires avec une valeur basée sur la lecture analogique de la broche 0.

```
void loop()
```

La fonction loop() est la boucle principale qui s'exécute en continu après l'exécution de la fonction setup(). Elle déclare les variables carte (pour la carte saisie par l'utilisateur), niveau (le niveau requis pour cette carte) et validation (un indicateur d'authentification réussie ou non).

```
false,
```

Définit les niveaux requis pour chaque carte dans un tableau niveauxCartes. Puis on attend de la saisie de la carte par l'utilisateur via la communication série.

Utilise la fonction Serial.parseInt () pour lire le numéro de la carte et détermine le niveau requis à partir du tableau niveauxCartes.

On effectue une authentification en appelant différentes fonctions (mA1(), mA2(), mA3(), mA4(), mA5()) en fonction du niveau requis.

Si toutes les conditions sont remplies, la variable validation est définie sur true.

On affiche le résultat de l'authentification via la communication série.

Ensuite on ajoute un délai de 1000 millisecondes (1 seconde) pour la lisibilité.

B. Explication des différents niveaux de sécurité :

Fonction MA1() :

La fonction MA1() est responsable de la première étape de vérification de sécurité du coffre-fort. Elle pose des questions à l'utilisateur et vérifie les réponses pour autoriser ou non l'accès. Voici un aperçu de son fonctionnement :

1. Elle pose des questions à l'utilisateur, comme la capitale de la France, le résultat de l'addition 4+2 et le diamètre de la Terre.
2. L'utilisateur répond à chaque question via la communication série.
3. Les réponses sont vérifiées :
   - Si toutes les réponses sont correctes, elle affiche "Excellent" et autorise l'accès.
   - Si une réponse est fausse, elle affiche "Faux, accès refusé" et bloque l'accès.

Fonction MA2() :

La fonction MA2() est une autre étape de vérification d'authentification. Elle utilise un système d'identification basé sur des noms d'agents et un chiffrement/déchiffrement pour valider l'accès. Voici comment elle fonctionne :

1. Elle demande à l'utilisateur d'entrer un nom d'agent.
2. Elle compare ce nom d'agent à une liste préétablie.
3. Si le nom d'agent est valide, elle chiffre un nombre aléatoire et le présente à l'utilisateur.
4. L'utilisateur doit déchiffrer ce nombre avec une clé privée et entrer le résultat.
5. Si le résultat correspond au nombre aléatoire initial, l'accès est accordé ; sinon, l'accès est refusé.

Fonction MA3() :

La fonction MA3() est chargée de l'authentification à l'aide de la reconnaissance de la rétine. Voici comment elle fonctionne :

1. Elle demande à l'utilisateur de placer son œil devant le lecteur.
2. Elle attend une réponse de l'utilisateur via la communication série.

3. Si la réponse est correcte, elle autorise l'accès.
4. Si la réponse est incorrecte, elle refuse l'accès et bloque l'exécution.

Fonction MA4() :

La fonction MA4() gère l'authentification à l'aide de la reconnaissance de l'empreinte digitale. Son fonctionnement est le suivant :

1. Elle demande à l'utilisateur de placer son doigt sur le capteur digital.
2. Elle attend une réponse de l'utilisateur via la communication série.
3. Si la réponse est correcte, elle autorise l'accès.
4. Si la réponse est incorrecte, elle refuse l'accès et bloque l'exécution.

Fonction MA5() :

La fonction MA5() effectue une autre vérification basée sur un système d'identifiants d'agents et de chiffrement. Voici comment elle fonctionne :

1. Elle demande à l'utilisateur de fournir une lettre d'agent.
2. Elle vérifie cette lettre parmi une liste d'identifiants.
3. Si la lettre d'agent est valide, elle chiffre un nombre aléatoire et l'affiche à l'utilisateur.
4. L'utilisateur doit déchiffrer ce nombre avec une clé privée et entrer le résultat.
5. Si le résultat correspond au nombre aléatoire initial, l'accès est accordé ; sinon, l'accès est refusé.

Ces fonctions représentent différentes couches de sécurité utilisées pour authentifier l'utilisateur avant d'accorder l'accès au coffre-fort. Chaque fonction implémente une méthode d'authentification différente, comme des quiz, des vérifications d'identifiants, des données biométriques, ou des systèmes de chiffrement/déchiffrement pour assurer un niveau de sécurité accru.