LISV Laboratoire d'ingénierie des systèmes de Versailles
UVSQ université PARIS-SACLAY

Cartes à puce
TP Noté

Halim Djerroud

révision 0.1

Préambule

Le but de la séance est d'apprendre à développer un projet complet de carte à puce industrielle. On va simuler le fonctionnement d'une carte SIM.

Principe de fonctionnement d'une carte SIM

Lorsqu'on allume un téléphone portable, on est invité à introduire un code PIN (*Personal Identification Number*) :

1. Si le code PIN est correct, la carte est déverrouillée.
2. Si le code PIN est incorrect, il reste 2 essais.
   Si au bout des 2 essais, le code PIN est incorrect, la carte est bloquée et on est invité à entrer un code de déblocage, le code PUK (Personal Unlocking Key) :
   (a) Si on entre le bon code PUK, on est invité à choisir un nouveau code PIN.
   (b) Si au bout de 3 essais le code PUK est incorrect, la carte est bloquée pour de bon et devient inerte.
   Remarque : Dans ce TP, on ne va pas limiter les tentatives de déblocage de la carte.

Quand la carte sort d'usine, elle est dans un état vierge, rien n'est inscrit dedans.

Une fois sortie d'usine elle est transportée chez l'opérateur du téléphone qui la personnalise. Cette personnalisation consiste à introduire des données (nom, prénom, numéro de téléphone,...) mais surtout : les codes PIN (en général, 4 caractères à 0) et PUK (8 caractères) initiaux. La carte se trouve alors dans un état verrouillé.

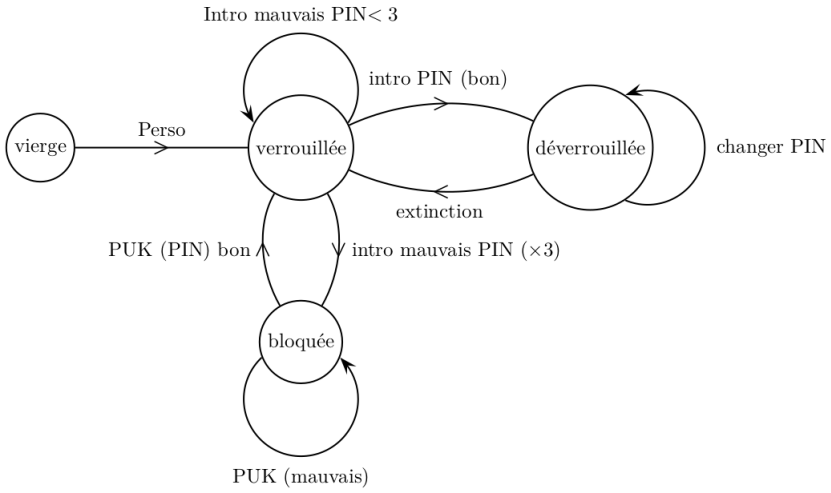
Pour pouvoir téléphoner, il faut déverrouiller la carte et pour se faire, il faut introduire le bon code PIN.
— Si on introduit le bon code PIN la carte est déverrouillée.
— Si on introduit le mauvais code PIN, elle reste verrouillée.

Au bout du 3ème essai, elle se trouve dans un état bloqué.

Pour la débloquer il faut la remettre dans un état verrouillé et pour cela, il faut introduire le code PUK et le nouveau code PIN associé.

La seule commande que l'on va autoriser lorsque la carte est déverrouillée est le changement du code PIN.

Voici l'automate des états de la carte depuis la sortie d'usine jusqu'à son utilisation :



Exercice 1

La seule commande reconnue par la carte en sortant d'usine est la commande d'introduction de la personnalisation. Écrire une fonction d'introduction de la personnalisation qui introduit les codes PUK et PIN dans la carte de commande : `85 20 00 00 0c` k_1 ... k_8 n_1 ... n_4

- k_1 ... k_8 correspond aux 8 caractères du code PUK
- n_1 ... n_4 correspond aux 4 caractères du code PIN

Remarque : Quand on reçoit des données, il ne faut pas effectuer des opérations d'écriture en ***EEPROM*** *en même temps car ces opérations sont lentes et il se peut que l'écriture ne soit pas correcte. La solution est de stocker d'abord les données en* ***RAM*** *pour les écrire après en* ***EEPROM****.*

Exercice 2

Écrire une fonction d'introduction du code `PIN` de commande :
`85 00 00 00 04` n_1 ... n_4. Cette commande renvoie :

- `90 00` si le code `PIN` est correct
- `6c 04` si le code `PIN` n'a pas le bon nombre de caractères
- `98 4x` avec `x` le nombre d'essais restants, si le code `PIN` est incorrect
  - soit `x=0`, la carte est bloquée
  - soit `x=1` ou `x=2`

Lorsque la carte est verrouillée, la seule commande qu'elle accepte est l'introduction du code `PIN`.

Remarque : Dans la norme GSM (Global System for Mobile communications), cette commande se nomme CHV (Card Holder Verification) et la classe correspondante est ***A0****.*

Exercice 3

Écrire une fonction de changement du code PIN de commande :
`85 01 00 00 08` $a_1 \ldots a_4$ $n_1 \ldots n_4$

- k_1 ... k_8 correspond aux 8 caractères du code PUK
- n_1 ... n_4 correspond aux 4 caractères du code PIN

Cette commande renvoie :

- `90 00` si le code `PIN` est correct et le changement est effectué
- `6c 04` si le nombre de paramètre est incorrect
- `98 40` si l'ancien code PIN est incorrect

Exercice 4

Écrire une fonction de déblocage, qui introduit le code PUK et le nouveau code PIN, de commande : `85 02 00 00 0c` $a_1 \ldots a_4$ $n_1 \ldots n_4$

Cette commande renvoie :
- `90 00` si le code PUK est correct et le nouveau code PIN a été introduit
- `6c 0c` si le nombre de paramètre est
- `98 40` si le code PUK est incorrect

Remarque : Dans la norme GSM, la commande de déblocage est la même que la commande CHV.

Script de test

```
1  : 85 20 00 00 0c 10 11 12 13 14 15 16 17 25 26 27 28
2  : 85 00 00 00 04 00 00 00 00
3  : 85 00 00 00 04 00 08 01
4  : 85 02 00 00 0c 85 04 00 00 08 00 00 00 00
5  : 85 00 00 00 04 25 26 27 28
6  : 85 01 00 00 08 25 26 27 28 01 01 01 01
7  : 85 00 00 00 04 25 26 27 28 ef fd ae b1
8  : 85 00 00 00 04 00 00 00 00
9  : 85 00 00 00 04 00 00 00 00
10 : 85 00 00 00 04 00 00 00 00
11 : 85 02 00 00 0c 01 02 03 56 67 87 38 ae 00 00 00 00
12 : 85 02 00 00 0c 10 11 12 13 14 15 16 17 02 02 02 02
13 : 85 20 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00
```

1. Introduction de la personnalisation des codes :
   - `PUK = 10 11 12 13 14 15 16 17`
   - `PIN = 25 26 27 28`
2. On introduit un mauvais PIN = `00 00 00 00`
   On doit avoir l'erreur : `98 42`
3. On introduit un mauvais PIN avec le mauvais nombre d'octets
   On doit avoir l'erreur : `6c 04`
4. On essaie de débloquer le PUK alors que l'état n'est pas à bloqué
   On doit avoir l'erreur : `6d 00`
5. On introduit le bon code PIN, on est à l'état déverrouillé
6. On veut changer le code PIN mais l'ancien est incorrect
   On doit avoir l'erreur : `98 40`
7. On change le code PIN en : `ef fd ae b1`
8. On entre un mauvais PIN
   On doit avoir l'erreur : `98 42`
9. On entre un mauvais PIN
   On doit avoir l'erreur : `98 41`
10. On entre un mauvais PIN
    On doit avoir l'erreur : `98 40` et la carte se bloque
11. On débloque avec le mauvais PUK
    On doit avoir l'erreur : `98 40`
12. On débloque avec le bon PUK
13. On essaie de personnaliser le PUK et PIN
    On doit avoir l'erreur : `6d 00`