GREAU Alexandre

VISSUZAINE Emmanuel

# Android Programming

*<u>Enoncé</u> : 2 utilisateurs veulent échanger des messages de façon synchronisée. Aucun des deux utilisateurs ne peut/doit connaitre le contenu du message de l'autre avant d'avoir envoyé son propre message. 1. Chaque utilisateur envoie son message codé. 2. A la réception d'un message codé, on envoie un "accusé de réception" 3. Lors qu'on a reçu le message et l'autre et l'accusé de réception de notre message, on envoie le code pour décoder le message. 4. A la réception du code, l'application notifie l'utilisateur et affiche le message décodé (ou le met dans la base de SMS).*

## <u>Fonctionnalités implémentées :</u>

- Envoi d'un message crypté
- Réception d'un message crypté et mise dans une base de données jusqu'à réception de la clé de déchiffrage
- Envoi différé de la clé de déchiffrement du message crypté précédemment envoyé
- Affichage du message décrypté à la réception de la clé de déchiffrement

## <u>Fonctionnement :</u>

L'utilisateur envoie un message quelconque à l'un de ses contacts. Le message est crypté à l'aide du chiffré de César et d'une clé aléatoire, que l'application associe au numéro de téléphone du contact.

Le message est ainsi envoyé crypté au contact, qui à son tour envoie un message crypté de manière aléatoire, de façon identique.

Une fois les messages envoyés, les utilisateurs sont libres d'envoyer la clé de déchiffrement du message.

Les clés une fois reçues débloquent pour chaque utilisateur les messages associés et les affichent décryptés sous forme de Toast.

**Base de données :**

La base de données ROOM utilisées par notre application Android et une base de données SQL construites et interrogées via des classes Java et des annotations simples.

Le type de données stocké dans la base de données est un type construit contenant un message, un ID, et un numéro de téléphone associé.

A l'aide de la classe *EncMessManager* qui est associée à l'activité principale, la gestion de l'encryptage/décryptage et les requêtes faites à la base de données sont reléguées à une classe Java pur (non Android).

**Fonctionnalités manquantes :**

La gestion des accusés de réception n'est pas faite, initialement, les clés ne devaient être envoyées qu'après réception par l'interlocuteur du message codé et par l'utilisateur du message opposé.