# Crypto Symétrique
# TD L'échange de clé symétrique

## Contexte

Depuis de la 3ème génération du réseau mobile (3G), le protocole AKA (authentication and key agreement) a été mis en place pour permettre aux utilisateurs mobiles d'établir un canal sécurisé avec le réseau lui donnant accès à des services (SMS, appels, Internet,…).

L'infrastructure mobile est complexe, figurant principalement trois types de composantes :

- Les utilisateurs avec des périphériques qu'on appelle techniquement User Equipment (UE)
- Le réseau mobile, se décomposant en deux sous-parties :
    - Le réseau d'accès radio (Radio Access Network, RAN)
    - Le cœur de réseau (Core Network, CN)

Les communications mobiles d'aujourd'hui permettent un accès ubiquitaire : c'est-à-dire, nous pouvons utiliser les services mobiles partout et toujours. Ceci force une distinction entre le cas d'utilisation du réseau domestique, et le cas dans lequel on utilise un réseau étranger (en roaming). Nous avons notamment trois types d'entités qui jouent un rôle dans les communications :

- Les utilisateurs, équipés de UEs
- Les opérateurs propres (Home Network, HN) des utilisateurs auxquels les utilisateurs font confiance
- Les opérateurs fournisseurs du service mobile (Serving Network, SN), auxquels les utilisateurs ne font pas toujours confiance, mais qui sont censés leurs fournir l'accès au réseau mobile.

Au long de ce TD, notre mission sera de comprendre (avec des simplifications) le fonctionnement et la sécurité du protocole AKA.

## Exercice I

Supposons dans un premier temps que le protocole AKA avait lieu entre un utilisateur (ou plutôt, son UE) et l'opérateur propre de cet utilisateur (son Home Network, HN), sans intermédiaire. Ceci est une simplification (nous allons voir cela plus en détails lors des prochains exercices).

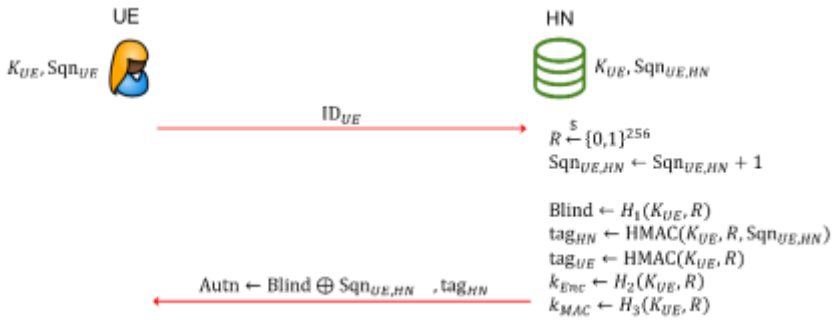
Le protocole AKA est à clé symétrique. Chaque UE partage une clé symétrique $K_{UE,HN}$ avec son HN. Bien-sûr, un seul HN peut avoir des milliards d'utilisateurs. Cette clé est stockée dans un élément sécurisé de l'UE, notamment la carte SIM. En plus de cette clé, lors de la mise en fonctionnement de la carte SIM, un

numéro de séquence $\mathrm{Sqn}_{UE}$ est choisi aléatoirement. Ce numéro de séquence sera modifié à chaque exécution du protocole -- il représente l'état de l'UE.

De son côté, le HN aura également un état, $\mathrm{Sqn}_{UE,HN}$, dont la valeur initiale sera $\mathrm{Sqn}_{UE}$ . La valeur de $\mathrm{Sqn}_{UE,HN}$ évolue à chaque exécution du protocole également et représente l'état du HN par rapport à UE.

Le schéma ci-dessous décrit une partie d'une exécution honnête du protocole AKA, entre un certain UE et son HN. Le protocole AKA a pour but une authentification mutuelle : premièrement du HN vers le UE, et ensuite de l'UE vers le HN. De plus, les deux parties doivent calculer une paire de clés $k_{Enc}, k_{MAC}$.

Analysez bien le schéma et répondez ensuite aux questions ci-dessous.




1. Ce protocole est partiel, montrant comment le $HN$ calcule un nombre de valeurs. Du côté de l'UE, ce dernier doit premièrement comparer le $\mathrm{Sqn}$ du HN à son propre $\mathrm{Sqn}$. Si les deux valeurs coïncident, alors l'UE doit vérifier l'authentification de l'HN, calculer son propre authentification $\mathrm{tag}_{UE}$, et l'envoyer au HN.

   En ayant ces informations, pouvez-vous compléter le protocole ci-dessus ?

2. Expliquez les rôles de chacune des valeurs $\mathrm{Blind}, \mathrm{tag}_{HN}, \mathrm{tag}_{UE}, k_{\mathrm{Enc}}, k_{\mathrm{MAC}}$, et déduisez ensuite les propriétés de sécurité demandées pour chaque valeur.

3. Pourquoi doit-on utiliser 3 fonctions de hachage différentes dans le schéma ci-dessus ? Y-a-t-il moyen de n'en utiliser qu'une ?

4. Disons que chacune de ces trois fonctions de hachage est très forte (remplaçable par un oracle aléatoire). Est-ce que cela suffit pour assurer la sécurité demandée pour les valeurs $\mathrm{Blind}, k_{\mathrm{Enc}}, k_{\mathrm{MAC}}$ ? Sinon, quelle autre propriété doit-on avoir ?

5. Regardons l'authentification dans le protocole ci-dessus. Dans l'absence d'un adversaire actif, ce protocole est-il sécurisé ?

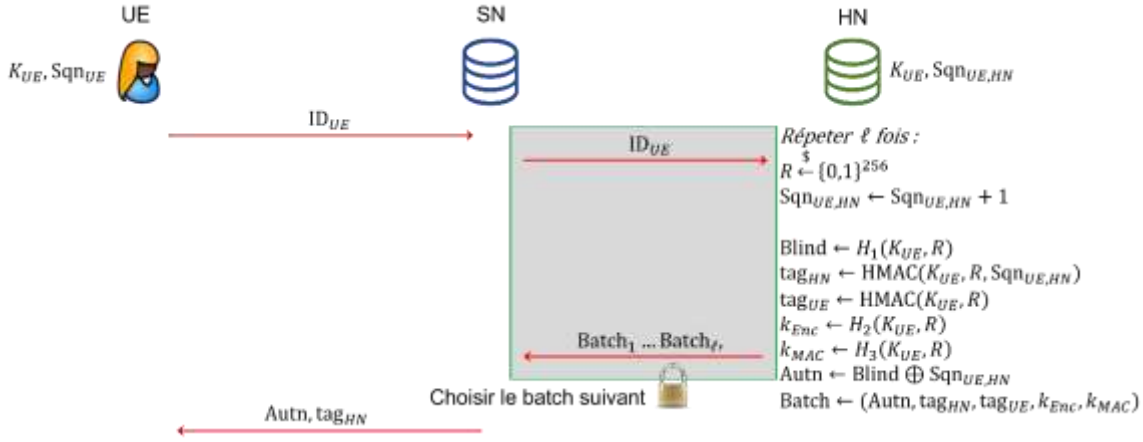
6. Et si l'attaquant est actif ?

# Exercice II

Dans le premier exercice, le protocole est exécuté entre un UE et son HN. Mais, en réalité, le protocole AKA s'exécute à 3 parties, avec un intermédiaire entre le HN et l'UE : notamment un réseau de service (serving network, SN). Le réseau de service n'a pas accès à la clé de l'utilisateur, ni aux numéros de séquence, ni du côté UE, ni du côté HN.

Le protocole AKA doit permettre au SN de s'authentifier auprès de l'UE et à l'UE d'être authentifié par le SN. De plus, un canal sécurisé doit être établi entre le SN et l'UE (donc, les deux entités doivent calculer des clés de session).

Dans ce contexte le protocole incomplet de l'exercice I devient le schéma ci-dessous.




Le système fonctionne notamment par «batch ». Au lieu de devoir demander des données d'authentification et des clés de session à chaque session, le SN demandera un ensemble de plusieurs (dans notre figure, $\ell$) ensembles de valeurs. Le canal entre le SN et le HN est sécurisé et mutuellement authentifié.

Ensuite, le SN peut choisir le prochain batch de valeur, choisir les valeurs $\mathrm{Autn}$ et $\mathrm{tag}_{HN}$ et les envoyer. Le reste du protocole sera le même que celui que vous avez trouvé à l'exercice I.

1. La valeur d'authentification auprès de l'UE utilisé par SN est générée par HN. Alors, cette authentification ne peut pas garantir le fait que SN est le HN propre à l'utilisateur. Qu'est-ce que cette valeur garantit-elle à l'UE ?
2. Les standards mobiles demandent la sécurité des données de l'UE par rapport au SN. Est-ce que cette sécurité est garantie par le protocole ci-dessus ?
    a. Pourquoi ? Donnez un argument intuitif.
    b. Est-ce que cette propriété est incluse dans les propriétés habituelles d'authentification et de sécurité de canal ?
3. Reprenez vos attaques contre un attaquant actif. Est-ce que ces attaques sont aussi efficaces contre ce protocole qu'ils ne le sont contre le protocole de l'exo précédent ?

4. Regardez le dernier exercice du TD précédent. Pouvez-vous utiliser la contre-mesure donnée contre ces attaques ?
5. Est-ce que ce protocole respecte la vie privée de l'UE ?