

Conclusion et perspectives

Dans ce mémoire nous avons présenté les notions de base de la cryptographie et on a présenté une application très importante dans notre vie moderne. Les systèmes d'identification par radiofréquence sont appliqués dans plusieurs domaines tels que, la santé, la chaîne de production, le contrôle d'accès. Ces utilisent dans l'étape d'authentification un protocole d'authentification RFID. Il y a plusieurs catégories des protocoles d'authentification, nous avons choisi cinq protocoles exigeant les fonctions de hachage et les générateurs des nombres pseudo-aléatoires (PRNG).

Au long de notre travail, nous avons concentré notre étude sur la conception et l'implémentation d'un simulateur. Dans la phase de conception, on a utilisé la simulation des événements, on a modélisé notre simulateur avec le langage de modélisation UML utilisant le diagramme de classe, le diagramme de cas d'utilisation et le diagramme de séquence pour chaque protocole.

La dernière étape est d'implémenter le simulateur. On a utilisé l'environnement de développement EDI NetBeans qui est basé sur le langage de programmation *Java*. Parmi les extensions de *Java* largement utilisés, on cite *Java Cryptography Extension (JCE)*. JCE fournit un cadre et la mise en œuvre pour le cryptage, la génération de clés, et calculer les différents types de fonction de hachage (e.g. SHA-1, MD5,...etc.).

Dans notre simulateur en essayer d'atteindre les objectifs suivantes :

- Assure le fonctionnement des protocoles d'authentification des systèmes d'identification par radiofréquence, et en particulier assurer l'authentification du tag et l'authentification du lecteur.
- Faire une comparaison entre les différents protocoles d'authentification étudiés en termes de performance.

Cependant, il existe encore des choses à améliorer. La simulation sera en entier si on peut ajouter certains graphiques de relations tels que longueur de la clef ou l'identificateur et la mise à jour dans le cas l'identifiant est dynamique. Autre perspective, la simulation des protocoles d'authentification de type « avec collision » dont le protocole utilise le service dans le cas le serveur est activé seulement et le service n'attend pas finaliser du protocole.