NOM : CHARED
Prénom : Marouen

UVSQ - Master SeCReTS
Contrôle de connaissances du 17 mars 2017
Partie 1 (3 pages) : cours sur la cryptographie dans les systèmes radiomobiles

NB : les feuilles d'énoncé seront utilisées pour inscrire la totalité des réponses. Pour certaines des questions de cette partie, il convient de cocher non pas une, mais plusieurs réponses exactes.

1) Citer le nom ou l'acronyme

- de deux algorithmes de chiffrement par blocs : DES IDEA
- de deux algorithmes de chiffrement à flot : RC4 SEAL

2) Algorithmes de chiffrement à flot

a. Quel est le rôle du vecteur d'initialisation (IV) dans un algorithme de chiffrement à flot ? Une réponse très brève est attendue (une à deux phrases).

b. Parmi les trois modes opératoires suivants, lequel permet de transformer un algorithme de chiffrement par blocs en un chiffrement à flot ?

❑ Electronic Code Book (ECB) ❑ Output Feedback (OFB) ❑ Cipher Block Chaining (CBC)

3) Citer deux des principales menaces contre la sécurité de l'accès radio dans les systèmes de communication avec les mobiles. Pour chacune des menaces citées, indiquer le nom d'un mécanisme de sécurité permettant de la prévenir au moins partiellement (mécanisme de protection).

- menace 1 :
- mécanisme de protection contre la menace 1 :

- menace 2 :
- mécanisme de protection contre la menace 2 :

4) Parmi les mécanismes de sécurité suivants, lesquels sont mis en œuvre dans le système GSM ? Cocher les trois réponses exactes.

☒ Authentification de l'abonné par le réseau
❑ Authentification du réseau par la carte SIM
❑ Intégrité des messages de signalisation
☒ Confidentialité du trafic et de la signalisation
☒ Confidentialité de l'identité de l'abonné (anonymat)

5) Quelles sont les propriétés de sécurité attendues d'un schéma d'authentification symétrique ? (Cocher les 2 réponses exactes.)

❑ non répudiation ☒ non-forgeabilité des réponses ❑ anonymat ☒ non rejeu ❑ confidentialité

6) Dans le système GSM, dans quels équipements l'algorithme A3/A8 d'authentification et d'établissement de clé est-il implanté ? (Cocher les deux réponses exactes.)

❑ SIM ☒ ME* ☒ BTS ❑ BSC ❑ MSC/VLR ❑HLR/AuC

Dans le système GSM, dans quels équipements le chiffrement/déchiffrement A5 est-il effectué ? (Cocher les deux réponses exactes.)

❑ SIM ❑ ME* ❑ BTS ❑ BSC ❑ MSC/VLR ❑HLR/AuC

* rappel : ME (Mobile Equipment) désigne le mobile MS (Mobile Station) privé de la carte SIM.

7) Indiquez en quelques mots en quoi consiste le rôle des valeurs Ki, RAND, SRES et Kc dans la procédure d'authentification et d'établissement de clé de session du système GSM.

- rôle de Ki :

- rôle de RAND :

- rôle de SRES :

- rôle de Kc :

8) Parmi les propriétés suivantes de l'algorithme de chiffrement A5/1 du système GSM, lesquelles peuvent être considérées comme des faiblesses cryptographiques ? *Cocher les 2 réponses exactes.*

❑ la taille de la clé est de 64 bits
❑ les avancées des registres sont irrégulières
❑ la taille de l'état du générateur A5/1 est de 64 bits
❑ le bit chiffrant est le ou exclusif de trois bits de l'état du générateur A5/1

9) Citer deux mécanismes de sécurité implantés dans le système UMTS, mais non implantés dans le système GSM.

-

-

NOM :
Prénom :

10) Indiquer en quelques mots la fonction du jeton AUTN = (SQN⊕AK || AMF || MAC-A) et le rôle des valeurs SQN, AK et MAC-A dans la procédure UMTS d'authentification et d'établissement de clé.

- fonction du jeton AUNT :

- rôle de SQN :

- rôle de AK :

- rôle de MAC-A :

11) Dans le système UMTS, quel est le rôle de la clé K ? *Cocher la bonne réponse.*

❑ clé d'authentification et d'établissement de clé ❑ clé du chiffrement f8 ❑ clé du MAC f9

Même question pour la clé de session CK :

❑ clé d'authentification et d'établissement de clé ❑ clé du chiffrement f8 ❑ clé du MAC f9

Même question pour la clé de session IK :

❑ clé d'authentification et d'établissement de clé ❑ clé du chiffrement f8 ❑ clé du MAC f9

12) Dans le système UMTS, dans lesquels des équipements suivants l'algorithme AKA réalisant les fonctions f1-f5 d'authentification et d'établissement de clé (dont un exemple est l'algorithme MILENAGE) est-il implanté ?

❑ USIM ❑ ME* ❑ Node B ❑ RNC ❑ MSC/VLR ❑ HLR/AuC

Même question pour la fonction de chiffrement f8 :

❑ USIM ❑ ME* ❑ Node B ❑ RNC ❑ MSC/VLR ❑ HLR/AuC

* rappel : ME (Mobile Equipment) désigne le mobile MS (Mobile Station) privé de la carte USIM

Fin de la partie 1