Nom : mai 2020
Prénom :

UVSQ – M2 SeCReTs 2020
Contrôle de connaissances
Cours sur la sécurité des réseaux mobiles

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. La consultation du cours est autorisée.

1. Quelle entité produit et maintient les spécifications techniques des réseaux mobiles ?
- ☐ La Wi-Fi Alliance
- ☐ L'ITU-T (International Telecommunications Institute)
- ☐ L'IEEE (Institute of Electrical and Electronics Engineers)
- ☐ Le 3GPP (3rd Generation Partnership Project)

2. L'intégrité des données utilisateur (« user plane ») est assurée sur la voie radio
- ☐ en 2G
- ☐ en 3G
- ☐ aucun des deux

3. L'intégrité de la signalisation (« control plane ») est assurée sur la voie radio
- ☐ en 2G
- ☐ en 3G
- ☐ aucun des deux

4. La signalisation (« control plane ») peut être chiffrée sur la voie radio
- ☐ en 2G
- ☐ en 3G
- ☐ aucun des deux

5. Les données utilisateur (« user plane ») peuvent être chiffrées sur la voie radio
- ☐ en 2G
- ☐ en 3G
- ☐ aucun des deux

6. Les algorithmes suivants sont cassés
- ☐ COMP128-1
- ☐ A5/2
- ☐ UEA1

7. Selon la norme GSM, le chiffrement des communications des abonnés a lieu :
- ☐ entre le téléphone et l'antenne-relai (BTS)
- ☐ entre le téléphone et le commutateur (MSC-VLR) dans le cœur de réseau
- ☐ entre la carte SIM et le HLR dans le cœur de réseau
- ☐ de bout en bout entre les 2 téléphones en communication

8. De quel type sont les algorithmes de chiffrement A5/1 et A5/2, développés initialement dans la norme GSM ?
- ☐ algorithme de chiffrement à flot, initialisé par une clé de 64 bits
- ☐ algorithme de chiffrement à flot, initialisé par une clé de 128 bits
- ☐ algorithme de chiffrement par bloc de 64 bits, initialisé par une clé de 64 bits
- ☐ algorithme de chiffrement par bloc de 64 bits, initialisé par une clé de 128 bits

9. Quelles sont les données spécifiques à un abonné mobile, stockée sur sa carte SIM ?
- ☐ son IMEI (International Mobile Equipment Identity)
- ☐ son IMSI (International Mobile Subscriber Identity)
- ☐ sa clé d'authentification au réseau (Ki en GSM, K en UMTS)
- ☐ son MSISDN (numéro de téléphone)

10. L'attaque par fausse BTS en 2G
- ☐ permet d'écouter le trafic en direction d'un mobile
- ☐ permet de modifier le trafic en provenance d'un mobile
- ☐ nécessite que l'attaquant soit à proximité de la victime
- ☐ nécessite que l'attaquant connaisse la clé secrète (Ki) de la victime

11. Avec une carte SIM 2G, je peux accéder
- ☐ Au réseau 2G
- ☐ Au réseau 3G

12. AUTN fait partie du vecteur d'authentification 3G et 4G. A quoi sert-il ?
- ☐ Il permet d'authentifier le réseau
- ☐ Il permet d'authentifier l'abonné
- ☐ Il est utilisé pour dériver les clés de session
- ☐ Il permet de vérifier la fraicheur du challenge

13. Selon la norme UMTS, le chiffrement des communications des abonnés a lieu :
- ☐ entre le téléphone et l'antenne-relai (NodeB)
- ☐ entre le téléphone et les équipements dans le cœur de réseau (MSC-VLR et SGSN)
- ☐ entre la carte SIM et le HLR dans le cœur de réseau
- ☐ entre le téléphone et le contrôleur radio (RNC)

14. Selon la norme GPRS, le chiffrement des communications des abonnés a lieu :

- entre le téléphone et l’antenne-relai (BTS)
- entre le téléphone et le routeur de paquet (SGSN) dans le cœur de réseau
- entre la carte SIM et le HLR dans le cœur de réseau
- de bout en bout entre le téléphone et le serveur en connexion

15. Dans le cas où la clé d’authentification d’un abonné mobile est compromise par un attaquant, ce dernier peut-il déchiffrer les communications radio entre le téléphone de l’abonné et le réseau mobile légitime ?

- non
- oui, mais uniquement les communications à venir
- oui, y compris les communications passées