Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 2ème année

TMC

Examen février 2014

Durée : 1h30 – Documents autorisés

IBE — 6 points

1 – 6pts Réalisez une comparaison détaillée des usages et fonctionnalités de l'IBE proposé par Jon Callas par rapport à ceux d'une PKI.
Vous chercherez les différents critères et propritétés/fonctionnalités permettant de réaliser cette comparaison.
Vous traiterez, entre autres, de :
- l'établissement de la confiance ;
- le cycle de vie des certificats ;
- le caractère « *on-line* » et « *off-line* » de l'IBE.

Dans quels cas se justifie l'utilisation d'un IBE ? Et dans quelle version, « off-line » ou « on-line » ?

Communication radio — 6 points

2 – 3pts On veut créer un réseau de capteurs alimentés par batterie utilisant la bande de fréquences ISM, « *Industrial Science and Medical* » autour des $2,45GHz$.
Le composant radio sélectionné est le nRF24L01.
Expliquez les avantages et inconvénients du choix de ce composant pour la mise au point du protocole de communication inter-capteurs.

3 – 3pts Quelle(s) différence(s) entre « *saut de fréquence* » et « *étalement de spectre* » ?
En quoi cela peut représenter un système de protection des communications ?
Sur quel(s) algorithme(s) de cryptographie pourrait-on s'appuyer pour les mettre en œuvre ?

MANETs — 8 points

4 – 2pts Citez des moyens de limiter le mécanisme d'« inondation » dans les algorithmes de routage dans les MANETs ?

5 – 2pts Décrivez comment une « *sybil attack* », c-à-d créer des faux nœuds, peut impacter un algorithme de routage comme OLSR.

6 – 2pts Qu'est-ce que peut apporter la « géolocalisation » dans le cadre d'un MANET ?
Y a-t-il des risques ?

7 – 2pts Dans quels cas le protocole TCP pose des problèmes lors de l'évolution d'un MANET ?
Dans au moins deux cas, vous décrirez les problèmes possibles dans le cycle de vie d'une communication TCP.
Est-ce que l'usage supplémentaire de la cryptographie pour l'authentification/chiffrement impacte ces problèmes ?
Comment y remédier ?