Grenoble INP – Ensimag
Année 2019-2020
N° d'inscription (carte étudiant) :
NOM :
Prénom :
Né(e) le : **à (ville + dépt ou pays) :**
N° du groupe de TD:
N° de la place :

UE Réseaux et sécurité

Examen du 16/01/2020 - Durée 2h30
1 feuille A4 recto-verso autorisée

NOTE IMPORTANTE : vous devez répondre sur les feuilles de ce sujet d'examen pour les parties en QCM. Vous traiterez les autres exercices sur une copie d'examen séparée, dans laquelle vous glisserez les QCM.
La durée de chaque partie devrait être approximativement de 0h30 pour les QCM de sécurité, et de 2h pour l'examen sur les réseaux. Les deux parties seront notées séparément. Le barème est indicatif.
Modalités des QCM
Sauf indication contraire (comme « Entourer la ou les propositions ») pour une Question à Choix Multiples, une seule des solutions proposées est correcte, c'est-à-dire une réponse adéquate à la question posée (certaines « solutions » peuvent être des affirmations vraies sans répondre à la question). Entourez le numéro (alphabétique) de la réponse exacte.
Barème : Réponse exacte : 1 point / Réponse fausse : -0,5 point / Omission : 0 point.

Partie 1. Questions à Choix Multiples sur la sécurité

Question 1. *Lorsque l'on chiffre un message avec une clef privée (de l'émetteur), que garantit-on ?*

A. On ne garantit rien, c'est insuffisant
B. On en garantit la légitimité (authenticité)
C. On garantit la confidentialité du contenu
D. On ne peut pas puisque cette clef est privée.

Question 2. *Quand parle-t-on d'authentification mutuelle entre deux entités ?*

A. Lorsque des deux entités sont administrées par la même personne ;
B. Lorsque chacune des entités doit s'authentifier vis-à-vis de l'autre ;
C. Lorsque la communication entre les deux entités est chiffrée ;
D. Lorsque les deux entités sont situées sur le même réseau.

Question 3. *Pourquoi vérifier l'intégrité d'un logiciel ?*

A. Pour s'assurer qu'il ne contient pas de virus ;
B. Pour s'assurer que le logiciel que je télécharge n'a pas été corrompu ;
C. Pour s'assurer que le logiciel fonctionne bien comme promis ;
D. Pour s'assurer qu'il est gratuit.

Question 4. *Comment pouvez-vous protéger la confidentialité de vos données ?*

A. En les chiffrant
B. En calculant leur empreinte de manière à vérifier leur intégrité ;

C. En les envoyant vers des supports externes ou vers le Cloud ;
D. En les publiant sur Internet.

Question 5. *Si on connaît le hachage cryptographique d'un mot de passe, on peut :*
A. Calculer le mot de passe ;
B. Connaître la longueur du mot de passe ;
C. Vérifier si le mot de passe est le même que celui d'un autre utilisateur ;
D. Empêcher l'accès de l'utilisateur au système.

Question 6. *Quel est le résultat du chiffrement par la méthode de transposition vue en cours du texte en clair : "GENERATIONCSE" avec le mot clé "PHELMA" ? (2,5 points réponse correcte, -1 réponse fausse)*
A. VLRPDAIPSYOST
B. VLRPDBJPSYQST
C. KRFMDAZMBFKE
D. AGTERENEICSON
E. ANEERGSOINCTE
F. ANEERGTOINCSE
G. RIEDOLAULRCOE

Question 7. *Entourer la (ou les) proposition(s) ci-dessous qui sont vraie(s) :*
A. Il n'existe aucune méthode de chiffrement sûre, si l'attaquant dispose de machines suffisamment puissantes et de suffisamment de temps (fût-ce des milliers d'années) pour mener sa cryptanalyse à texte chiffré connu ;
B. Les algorithmes de chiffrement symétriques sont adaptés au chiffrement de gros flux de données ;
C. Pour de la cryptographie symétrique, il faut au départ qu'on ait fait parvenir la clé par des canaux sûrs à chaque interlocuteur légitime ;
D. En chiffrant les données, on perd de l'information.

Question 8. *Entourer la (ou les) proposition(s) ci-dessous qui sont vraie(s) :*
A. Un certificat contient au moins une clé ;
B. Tout le monde a le droit de lire le contenu d'un certificat : il n'a pas besoin d'être confidentiel ;
C. Un certificat contient la clé privée de la personne pour laquelle il a été émis ;
D. Un certificat contient la clé privée de l'autorité qui l'a émis.

Question 9. *On considère les échanges suivants de messages, où on note inv(Ka) la clé privée de A, sa clé publique étant Ka, et m un message lisible (clair) :*
1) A -> B : $\{A, Na\}_{Kb}$
2) B-> A : $\{B, Na\}_{Ka}$.
Entourer la (ou les) proposition(s) ci-dessous qui sont vraie(s) :
A. un message de la forme $\{m\}_{inv(Kb)}$ permet de garantir que le message provient de B
B. un message de la forme $\{m\}_{inv(Kb)}$ permet d'être sûr que le message a été construit par B
C. les échanges 1) et 2) permettent à A de s'authentifier auprès de B
D. les échanges 1) et 2) permettent à B de s'authentifier auprès de A

Partie 2. Questions à Choix Multiples sur les réseaux

Question 10. *Vous envoyez un email à un de vos professeurs. Son serveur de réception est reception.imag.fr. Votre serveur d'envoi est smtp.fai.fr. Quel protocole reception.imag.fr doit-il interpréter pour accepter les nouveaux messages provenant de smtp.fai.fr ?*

A. SMTP
B. POP
C. IMAP
D. POP ou IMAP
E. Aucun de ceux-ci

Question 11. *Dans le modèle TCP/IP, on est certain qu'un routeur possède :*

A. Une couche TCP
B. Une couche UDP
C. Une couche IP
D. Une couche 802.11
E. Toutes ces couches.

Question 12. *Dans la liste suivante, un des noms ne désigne pas un protocole : lequel ?*

A. HTTP
B. XML
C. X11
D. SSL
E. ARP

Question 13. *Qu'appelle-t-on une technique d'accès multiple ?*

A. une technique qui permet de recevoir plusieurs types de services (ex : téléphone, Internet, télévision)
B. une technique qui permet à plusieurs utilisateurs de partager le même support de transmission
C. une technique qui permet d'accéder à un réseau via différents systèmes de transmission (ex : radio, paire de cuivre, fibre optique …)
D. une technique qui permet de se connecter en mobilité à partir de plusieurs localisations

Question 14. *On considère un canal de transmission qui a pour seul défaut d'avoir une bande fréquentielle limitée (il n'ajoute notamment pas de bruit). Laquelle des propositions suivantes est correcte ?*

A. Les informations numériques sont forcément dégradées à travers ce canal.
B. On ne peut pas répondre tant qu'on ne connaît pas la distance entre l'émetteur et le récepteur.
C. On peut transmettre les informations numériques à travers ce canal avec une probabilité d'erreur nulle à condition que le débit binaire ne soit pas trop important.
D. Aussi grande que soit la valeur du débit binaire, il est possible de transmettre les informations numériques à travers ce canal avec une probabilité d'erreur nulle.

Question 15. *La figure 1a montre le relevé temporel des signaux sur les deux entrées d'un modulateur IQ. La modulation utilisée est une modulation QAM32. Son diagramme de constellation est représenté sur la figure 1b. Quels sont les bits d'information émis ?*

A. La séquence commence par 0111110001…
B. La séquence commence par 1011101001…
C. La séquence commence par 0101010100…
D. Il n'y a pas assez de données pour pouvoir répondre à la question.
E. Aucune réponse ne convient.

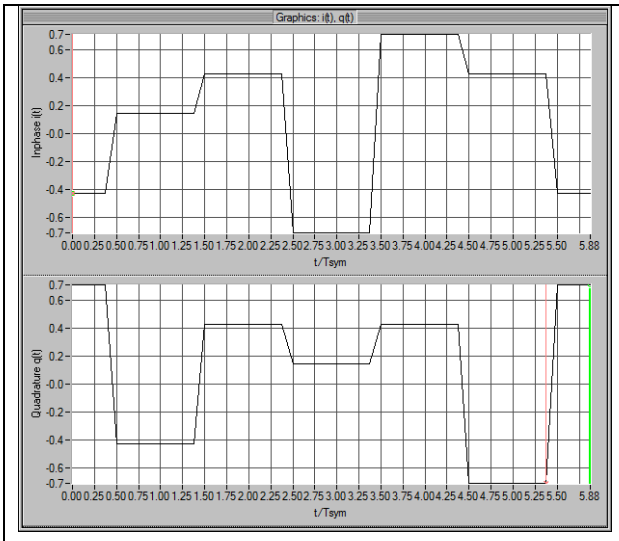


Figure 1a : relevés temporels sur les voies I et Q

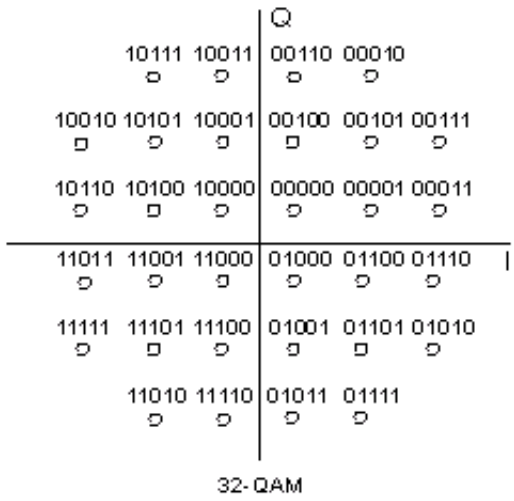


Figure 2b : diagramme de constellation de la modulation QAM32

Question 16. *Quelles sont les deux propositions correctes ? Un modulateur IQ :*

A. est constitué d'un déphaseur permettant de faire de la modulation de phase
B. comprend un oscillateur local de fréquence fixe
C. comprend un oscillateur local commandé en tension pour pouvoir faire varier la fréquence
D. comprend un ou des convertisseurs numériques / analogiques

Question 17. *Quelles sont les correspondances correctes entre les types de techniques d'accès citées dans la première colonne du tableau et les propriétés proposées dans la deuxième ?*

A. 1c / 2a /3d
B. 1b / 2c / 3d
C. 1b / 2a / 3c
D. 1a / 2b /3c
E. 1c / 2b / 3d

1) CSMA 2) CDMA 3) FDMA/TDMA	a) Quand ils transmettent leurs données, les utilisateurs émettent en même temps, dans la même bande de fréquence.

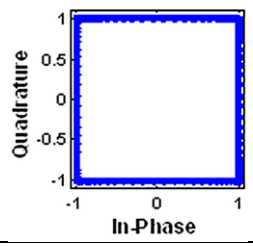
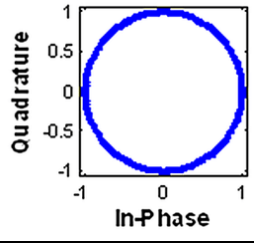
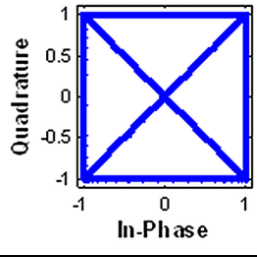
	b) Il peut y avoir des collisions (c'est-à-dire des trames de données émises en même temps et qui se brouillent) c) Aucune phrase ne convient. d) L'une ou l'autre (exclusivement) de ces deux techniques est utilisée en GSM.

Question 18. *La modulation MSK est particulièrement adaptée pour :*

A. l'ADSL
B. les faisceaux hertziens
C. les systèmes de transmission à bas débit et faible coût de l'Internet des objets
D. les systèmes de transmission à très haut débit 4G et 5G des réseaux mobiles

Question 19. *Quelles sont les correspondances correctes entre les modulations citées dans la première colonne du tableau et les diagrammes vectoriels affichés dans la deuxième colonne ? (Un diagramme vectoriel représente l'évolution temporelle continue du signal IQ sur le diagramme de constellation lorsque l'on émet une séquence infinie aléatoire de données)*

A. 1a / 2c / 3b
B. 1a / 2b / 3c
C. 1b / 2a / 3c
D. 1b / 2c / 3a
E. 1c / 2b /3a
F. 1c / 2a /3b

1) QPSK 2) OQPSK 3)MSK	a) 	b) 	c) 

Exercice 1 (2 points)

Un utilisateur sur ensipcserveur.imag.fr (adresse IP 129.88.240.65) exécute un navigateur WWW pour accéder aux documents sur web.ensimag.fr (adresse IP 195.221.228.24). Au même instant, un autre utilisateur travaillant sur la même machine ensipcserveur utilise ssh pour travailler sur web.ensimag.fr. Enfin, un troisième utilisateur, loggé sur web.ensimag.fr, utilise en même temps un navigateur pour accéder à une page web sécurisée désignée par https://ensipcserveur.imag.fr/index.html.

Question 20. *Faites un schéma qui présente l'architecture en couches des protocoles utilisés, les points de connexion avec les ports et adresses, et les chemins empruntés par les données échangées au niveau de ces applications.*

Exercice 2 : Performances (2 points)

Deux stations éloignées de 10 000 km sont connectées par (exactement) un routeur. Les liens entre le routeur et les stations offrent un débit de 100 kb/s. On transfère un fichier de taille 1 Moctet en utilisant un protocole Arrêt et Attente : le fichier est découpé en paquets de 1000 octets ; on envoie un paquet à la fois et on attend la confirmation de sa réception par un paquet ACK de taille 10 octets. On néglige le temps de traitement et le temps d'attente. Comme d'habitude, on suppose que la vitesse de propagation est 2/3 de celle de la lumière dans le vide, donc $2x10^8$m/s.

Question 21. *Quel est le temps total de transmission ? Faites un schéma et détaillez votre raisonnement pour expliquer votre calcul.*

Exercice 3 : Messagerie (2 points)

Alice a un compte de courrier électronique sur un serveur Web www.fnac.fr, et Bernard lit ses messages sur fidji.imag.fr. Admettons que le serveur SMTP d'entrée du domaine imag.fr soit drakkar.imag.fr . Alice compose un message à destination de bernard@imag.fr (le compte de messagerie de Bernard, hébergé dans une boîte aux lettres sur fidji) à partir de son ordinateur à domicile, relié à l'internet par ADSL.

Question 22. *Sans détailler les messages des protocoles (dites juste « telle machine utilise tel protocole avec telle autre machine pour obtenir ou transmettre telle information », ou bien « telle opération se déroule sur telle machine »), décrivez la suite des opérations, les protocoles et les machines impliquées qui vont permettre au message d'Alice de parvenir à Bernard.*

Exercice 4 : Communication radio (4 points)

Un système radio utilise un canal fréquentiel de bande 6 MHz. La modulation utilisée est de type QAM avec un nombre de symboles égal à 4,16, 32 ou 64. La rapidité de modulation est toujours de 5 Mbauds.

Question 23. *Est-il possible de réaliser la transmission numérique sans interférences entre symboles ? Si oui, comment ? (Précisez les caractéristiques des blocs à prévoir dans la chaîne de transmission).*

La puissance de bruit mesuré à l'entrée du récepteur est de -103 dBm dans une bande de 5 MHz. (Le filtre utilisé pour la mesure se comporte comme un filtre idéal de bande passante égale à 5 MHz autour de la fréquence porteuse du signal radio). La puissance du signal à l'entrée du récepteur vaut -75 dBm .

Question 24. *Est-elle suffisante pour assurer un taux d'erreurs binaires de 10^{-6} avec une modulation QAM64 ? Quel rapport doit-on calculer pour répondre ? Donnez sa valeur.*

Si on augmente la distance d'un facteur 2, la puissance reçue diminue. Pour conserver la même qualité de transmission, on change alors de modulation et on passe à une modulation QAM32.

Question 25. *Dites ce que sera la nouvelle valeur du débit binaire. Si la puissance reçue n'avait pas changé, de combien de dB aurait alors augmenté l'énergie du bit en réception ?*

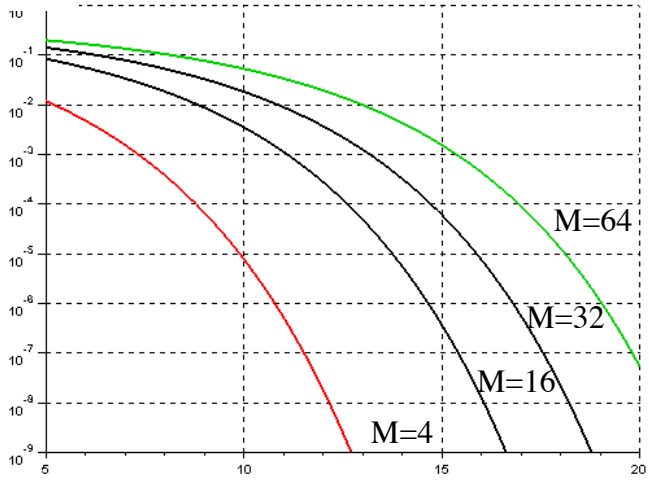
Question 26. *Suffit-il de choisir une modulation QAM32 pour garantir à nouveau un taux d'erreurs binaires de 10^{-6} ? Si non, proposez une autre solution.*

Annexes

Rappel des numéros de ports réservés vus dans le cours : ftp=20&21, ssh=22, smtp=25, dns=53, www=80, pop=110, imap :143, https=443, imaps=993, pop3s=995... Les numéros >49151 sont alloués dynamiquement. Les numéros de ports sont sur 16 bits.

Courbes de performance des modulations QAM-M :

TEB



E_b/N_0 (dB)

E_b=Puissance reçue $\times T_b$

$N_0/2$: DSP du bruit

Bande occupée avec filtrage de Nyquist :
en bande de base $B_{occ}=(D_S/2)\times(1+\alpha)$ / avec modulation $B_{occ}=D_S(1+\alpha)$

Formule du bilan de liaison radio en espace libre :

$$\left(\frac{P_R}{P}\right)_{dB} = g_{E_{dB}} + g_{R_{dB}} + 20\log\left(\frac{\lambda}{4\pi r}\right)$$

Application numérique : $10\log_{10}(2) \approx 3$ / $10\log_{10}(3) \approx 4{,}8$ / $10\log_{10}(5) \approx 7$