Hana BERRACHED

Échelle d'évaluation standard : **A (% de réussite supérieur à 75%)**	Échelle d'évaluation pondérée : **A (% de réussite supérieur à 75%)**

Cryptographie/Généralités

Échelle d'évaluation standard : **A (% de réussite supérieur à 75%)**

AAVs :

- [2] Expliquer les termes de base liés à la cryptographie

- [2] Appliquer un système de codage simple

- [3] Comparer différentes fonctions de hachage

Question 1 — **Question à réponse unique**

Qu’est-ce que RSA ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Un algorithme de chiffrement asymétrique
B	☐	☐	Non	Une autorité de certification
C	☐	☐	Non	Une clé de chiffrement
D	☐	☐	Non	Un algorithme de hachage
E	☐	☐	Non	Un algorithme de chiffrement symétrique

Commentaire de correction de la question

Le chiffrement RSA est un algorithme de cryptographie asymétrique, il utilise une paire de clés composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles.

Question 2 — **Question à réponses multiples**

Quelles sont les caractéristiques des fonctions de hachage cryptographiques ? (2 réponses attendues)

Réponses correctes	0 discordance	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Deux valeurs identiques permettent d’obtenir un hash identique.
B	☐	☐	Non	Deux valeurs identiques donnent un hash différent.
C	☐	☐	Non	Comme le chiffrement des données, le hachage permet de retrouver la valeur d’origine.
D	☑	☑	Non	Quel que soit le nombre de caractères de la valeur de départ, la taille du hash obtenu reste identique.
E	☐	☐	Non	La taille du hash obtenu correspond toujours au nombre de caractères de la valeur de départ.

Commentaire de correction de la question

Une fonction de hachage est une fonction qui associe des valeurs de taille fixe à des données de taille quelconque.

On veut qu’une fonction de hachage donne une "empreinte" (un haché) de notre donnée initiale, mais on ne veut pas qu’à partir d’une empreinte, on puisse fabriquer un message dont le haché soit cette empreinte. Cela revient à résister à la préimage.

Question 3 — **Question à réponse unique**

À quoi sert une Rainbow Table ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	À hacher les mots de passe.
B	☐	☐	Non	À attaquer un mot de passe par force brute.
C	☑	☑	Non	À réduire le temps nécessaire pour cracker les mots de passe.
D	☐	☐	Non	À la récupération de mots de passe forts.
E	☐	☐	Non	À générer des mots de passe forts.

Commentaire de correction de la question

Les Rainbow Tables (ou “Tables arc-en-ciel”) sont utilisées par les cybercriminels pour déchiffrer des mots de passe. Par rapport à l’attaque par force brute ou par dictionnaire de mot de passe, les Rainbow Tables permettent de réduire le temps et la mémoire nécessaire pour cracker les mots de passe.

Question 4 — **Question à réponses multiples**

Quelles sont les propositions exactes concernant le codage ? (3 réponses attendues)

Réponses correctes	0 discordance	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Il doit protéger les informations.
B	☑	☑	Non	Il transforme de l'information en symboles.
C	☑	☑	Non	Il est utilisé par la compression de données.
D	☐	☐	Non	Il dissimule les données.
E	☑	☑	Non	Il peut maximiser l'efficacité de la transmission d’information.

Commentaire de correction de la question

Les opérations de chiffrement et de codage font partie de la théorie de l'information et de la théorie des codes. La différence essentielle réside dans la volonté de protéger les informations et d'empêcher des tierces personnes d'accéder aux données dans le cas du chiffrement. Le codage consiste à transformer de l'information (des données) vers un ensemble de mots. Chacun de ces mots est constitué de symboles. La compression est un codage : on transforme les données vers un ensemble de mots adéquats destinés à réduire la taille, mais il n'y a pas de volonté de dissimuler (bien que cela se fasse implicitement en rendant plus difficile d'accès le contenu).

Question 5 — Question à réponse unique

Une fonction de hachage H doit être résistante à la recherche de collision. D'après vous quand parle-t-on de collision entre x et x' ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Quand H(x) = H(x') avec x différent de x'
B	☐	☐	Non	Quand H(x) ≠ H(x') avec x différent de x'
C	☐	☐	Non	Quand H(x) = x' avec x différent de x'
D	☐	☐	Non	Quand H(x) = x avec x différent de x'
E	☐	☐	Non	Quand H(x') = x avec x différent de x'

Commentaire de correction de la question

En informatique, une collision désigne une situation dans laquelle deux données ont un résultat identique avec la même fonction de hachage.

Question 6 — Question à réponse unique

Quel est le code du mot BONJOUR en appliquant le code César + 3 ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	ERLNRTU
B	☑	☑	Non	ERQMRXU
C	☐	☐	Non	GTSOTZW
D	☐	☐	Non	DQPLQWT
E	☐	☐	Non	DQPLQTU

Commentaire de correction de la question

Le chiffre de César consiste à coder en décalant les lettres de 3 rangs.
L'alphabet en clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ -> BONJOUR
L'alphabet chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC -> ERQMRXU

Question 7 — **Question à réponse unique**

Quelle notion est utilisée pour passer de CESI FOREVER à 1234 5672827 ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Substitution
B	☐	☐	Non	Inversion
C	☐	☐	Non	Transposition
D	☐	☐	Non	Arrangement
E	☐	☐	Non	Combinaison

Commentaire de correction de la question

Une chiffrement par substitution va "simplement" remplacer un caractère par un autre signe, qui peut être un autre caractère, un logo, un dessin ou même un chiffre ou un nombre dans ce cas.

Question 8 — **Question à réponse unique**

Le chiffrement du message "POUR L'HONNEUR" donne "41 35 51 43 32 23 35 34 34 15 51 43". Quelle technique de chiffrement a été utilisé ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Carré de Polybe
B	☐	☐	Non	Chiffre des templiers
C	☐	☐	Non	Chiffre de Vigerène
D	☐	☐	Non	Code de César
E	☐	☐	Non	Une autre technique non listée

Commentaire de correction de la question

Le carré de Polybe est une technique de chiffrement par substitution monoalphabétique, il consiste à ordonner les lettres de l'alphabet en ordre alphabétique dans un tableau carré de 5 cases de côté dont chaque ligne et chaque colonne sont numérotées, de gauche à droite et de haut en bas.

Cryptographie-Applications

Échelle d'évaluation standard : **A (% de réussite supérieur à 75%)**

AAVs :

- [4] Sélectionner différentes solutions pour assurer la confidentialité d'un système
- [4] Comparer différentes technologies de tunnelisation
- [2] Expliquer le fonctionnement des certificats numériques
- [4] Discriminer différentes techniques d'authentification

Question 1 — **Question à réponses multiples**

Qu’est-ce que S/MIME ? (3 réponses attendues)

Réponses correctes	0 discordance	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Un protocole d’authentification.
B	☑	☑	Non	Un protocole de chiffrement des e-mails.
C	☐	☐	Non	Un protocole VPN.
D	☐	☐	Non	Une fonction de hachage.
E	☑	☑	Non	Un protocole de signature de courriels.

Commentaire de correction de la question

S/MIME (Secure/Multipurpose Internet Mail Extensions) est une norme de cryptographie et de signature numérique de courriels encapsulés au format MIME.

Question 2 — **Question à réponses multiples**

Quelles sont les affirmations exactes ? (2 réponses attendues)

Réponses incorrectes	4 discordances	0 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☐	Oui (+1)	TLS prend en charge d'anciens algorithmes qui présentent des failles de sécurité connues.
B	☐	☐	Non	SSL présente des failles de sécurité connues.
C	☐	☑	Oui (+1)	TLS génère des clés de façon plus sécurisée que SSLv3.
D	☐	☑	Oui (+1)	TLS a été adopté par de nombreux acteurs de l’Internet pour sécuriser le trafic lié aux sites web.
E	☑	☐	Oui (+1)	Récemment, TLS a été supplanté par SSL.

Commentaire de correction de la question

Transport Layer Security (TLS) et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges par réseau informatique, notamment par Internet.
SSL 3.0 est la dernière version de SSL, qui inspirera son successeur TLS. Le protocole est banni en 2014, à la suite de la publication de la faille POODLE.
La plupart des navigateurs sont aussi des clients TLS.

Question 3 — **Question à réponses multiples**

Que peut ont affirmer à propos du protocole PPTP ? (3 réponses attendues)

Réponses correctes	0 discordance	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	C’est le protocole actuellement préconisé pour les communications sensibles ou confidentielles.
B	☑	☑	Non	Il est pris en charge par de nombreux systèmes d'exploitation.
C	☑	☑	Non	C’est un protocole Microsoft.
D	☐	☐	Non	Il est connu pour être compliqué à configurer.
E	☑	☑	Non	C’est un protocole de réseau privé virtuel.

Commentaire de correction de la question

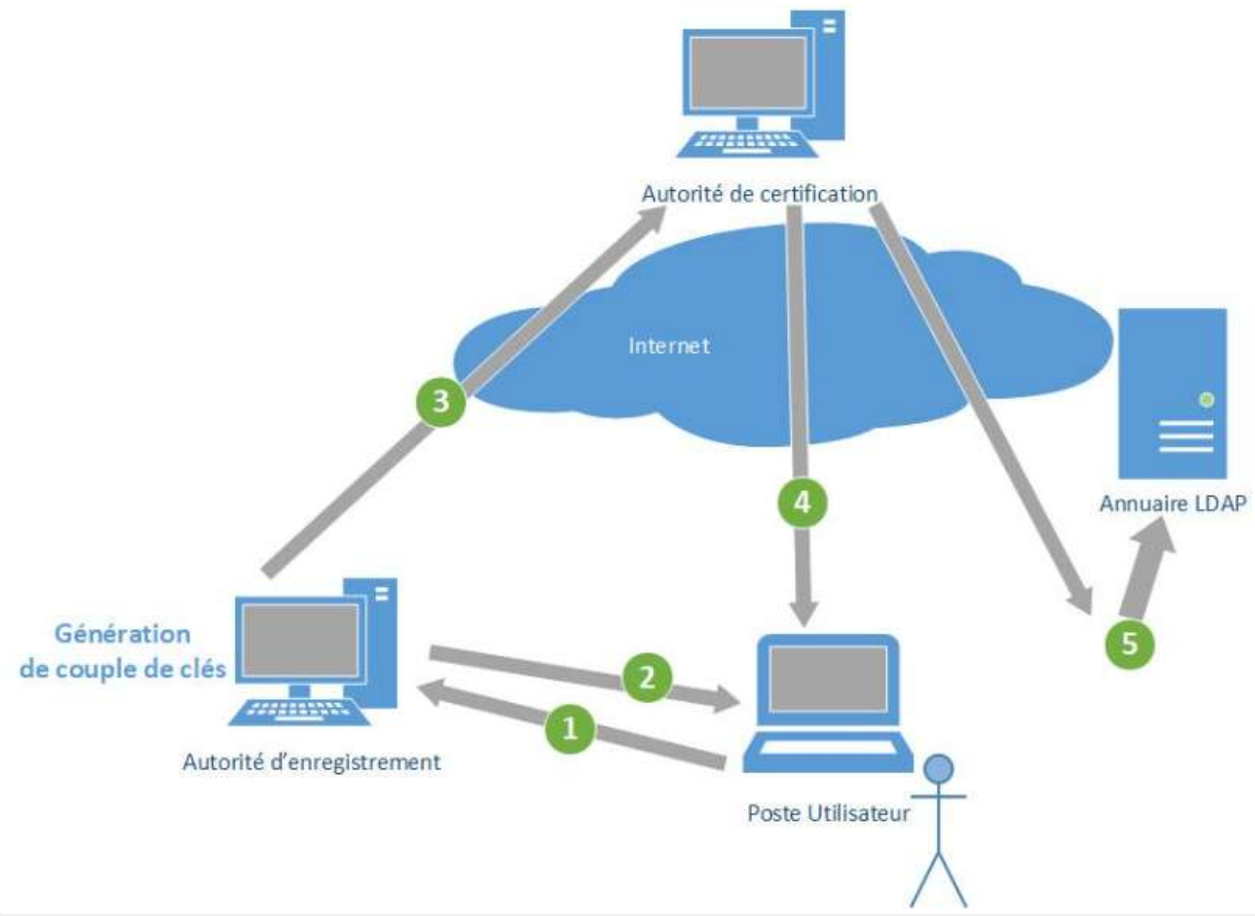
Point-to-point tunneling protocol est un protocole d'encapsulation PPP sur IP conçu par Microsoft. Il permet de mettre en place des réseaux privés virtuels (VPN).

PPTP est très facile à configurer et compatible avec la plupart des systèmes d’exploitation de bureau et mobiles. Il existe un client PPTP3 ainsi qu'un serveur PPTP4 sous Linux et Mac OS X comporte un client PPTP.

De nombreuses vulnérabilités et failles ont été identifiées pour le protocole PPTP.

Question 4 **Question d'association**

Voici un schéma de l’organisation d’une PKI et présentant les étape nécessaires pour obtenir un certificat numérique.
Les étapes sont numérotées de 1 à 5 dans l'ordre chronologique.
Associez les étapes correspondantes à chacune des descriptions proposées.



Réponses incorrectes	4 discordances	0 point obtenu sur 1

Élément à associer	Réponse attendue	Réponse saisie	Réponse discordante
Demande de certificat (Envoi de la clé publique pour la certification).	étape 3	étape 2	Oui (+1)
Envoi de la clé privée.	étape 2	étape 5	Oui (+1)
Identification de l’utilisateur.	étape 1	étape 1	Non
Publication de certificat et de la CRL.	étape 5	étape 4	Oui (+1)
Envoi du certificat signé.	étape 4	étape 3	Oui (+1)

Commentaire de correction de la question

Dans une infrastructure à clé publique ; pour obtenir un certificat numérique, l'utilisateur fait une demande auprès de l'autorité d'enregistrement. Celle-ci génère un couple de clé (clé publique, clé privée), envoie la clé privée au client, applique une procédure et des critères définis par l'autorité de certification qui certifie la clé publique et appose sa signature sur le certificat, parfois fabriqué par un opérateur de certification.

Question 5 — **Question à réponses multiples**

Qu’est ce que Kerberos ? (2 réponses attendues)

Réponses correctes	0 discordance	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Un protocole d’authentification compatible uniquement avec Active Directory.
B	☐	☐	Non	Une PKI.
C	☑	☑	Non	Un protocole d’authentification compatible aussi bien avec les systèmes libres ou propriétaires.
D	☑	☑	Non	Un protocole utilisant une authentification forte.
E	☐	☐	Non	Un protocole qui garantit la sécurité des données stockées sur les systèmes.

Commentaire de correction de la question

Kerberos est un protocole d'authentification réseau. Il existe plusieurs implémentations libre ou propriétaire du protocole Kerberos. L'implémentation propriétaire la plus courante est la version de Microsoft Kerberos v5 intégré à Active Directory. Il repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets. Kerberos est un protocole d'authentification forte.

Question 6 — **Question à réponse unique**

Vous voulez permettre à votre équipe de travailler à distance en bénéficiant d’un accès sécurisé aux ressources de l’entreprise. Que proposez vous d'utiliser?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Un proxy
B	☑	☑	Non	Un VPN
C	☐	☐	Non	Un annuaire Active Directory
D	☐	☐	Non	Une clé Wifi
E	☐	☐	Non	Un ordinateur portable

Commentaire de correction de la question

Utiliser un VPN en télétravail depuis chez soi ou à l’extérieur présente de nombreux avantages:

- Naviguer sur Internet en toute sécurité et confidentialité.
- Limiter le risque de fuite de données confidentielles si le salarié se connecte à un réseau public.
- Accéder à tous les contenus utiles dans le cadre de leur travail.
- Voyager sans contraintes à l’étranger.

Question 7

Question à réponses multiples

Parmi les propositions suivantes, sélectionner celles qui sont des composantes d'IPsec :

Réponses correctes | 0 discordance | 1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	AH
B	☐	☐	Non	LSA
C	☑	☑	Non	ESP
D	☐	☐	Non	LTP
E	☐	☐	Non	SSP

Commentaire de correction de la question

AH est le premier et le plus simple des protocoles de protection des données qui font partie de la spécification IPsec. Il est détaillé dans la RFC 2402. ESP est le second protocole de protection des données qui fait partie de la spécification IPsec. Il est détaillé dans la RFC 2406.

Question 8

Question à réponse unique

Parmi les propositions suivantes, sélectionner celle qui combine les fonctionnalités des protocoles L2F et PPTP :

Réponses correctes | 1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	GRE
B	☐	☐	Non	IPsec
C	☐	☐	Non	SSL
D	☑	☑	Non	L2TP
E	☐	☐	Non	ESP

Commentaire de correction de la question

Layer 2 Tunneling Protocol (L2TP) signifie protocole de tunnelisation de niveau 2, utilisé pour créer des réseaux privés virtuels (VPN). Il combine les fonctionnalités de L2F de Cisco et le PPTP de Microsoft.

Question 9 — **Question à réponse unique**

Laquelle de ces technologies n'est **PAS** une solution de tunnelisation ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	IPsec
B	☐	☐	Non	GRE
C	☐	☐	Non	SSH
D	☐	☐	Non	TLS
E	☑	☑	Non	AES

Commentaire de correction de la question

AES est un algorithme de chiffrement symétrique.

SSH prend en charge la tunnellisation en permettant la création de tunnels SSH. Ces tunnels SSH sont utilisés pour encapsuler et sécuriser le trafic réseau, ce qui est particulièrement utile dans les cas suivants : Accès à distance sécurisé, Encapsulation de protocoles, Transfert de données sécurisé.

TLS permet de chiffrer les données transitant entre un client et un serveur, assurant ainsi la confidentialité et l'intégrité de la communication.

GRE est un protocole de tunnellisation simple.

IPsec (Internet Protocol Security) est en effet un protocole de sécurité utilisé pour sécuriser les communications sur les réseaux IP. Il est souvent associé à la tunnellisation.

Question 10 — **Question à réponse unique**

Lors d'un téléchargement d'un fichier volumineux sur Internet, pourquoi, de temps en temps, on vous fournit une empreinte MD5 ou SHA1 ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Pour vérifier la confidentialité.
B	☑	☑	Non	Pour vérifier l'intégrité.
C	☐	☐	Non	Pour vérifier votre identité.
D	☐	☐	Non	Pour vérifier la résilience.
E	☐	☐	Non	Pour assurer la traçabilité.

Commentaire de correction de la question

La signature (ou le hash) fournit est l'empreinte des données que vous téléchargez. En recalculant cette empreinte avec les données téléchargés, vous pouvez vérifier l'intégrité si le hash est similaire ou non avec ce qui est fourni.

Question 11 — **Question à réponse unique**

Quelle méthode n'est **PAS** une technique d'authentification ?

Réponses correctes	1 point obtenu sur 1

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Couple login/password
B	☐	☐	Non	Biométrie digitale
C	☐	☐	Non	Token
D	☐	☐	Non	Code numérique
E	☑	☑	Non	Contrôle de redondance cyclique

Commentaire de correction de la question

le CRC permet d'assurer l'intégrité des données lors de la lecture d'un CD-ROM ou dans une trame par exemple.