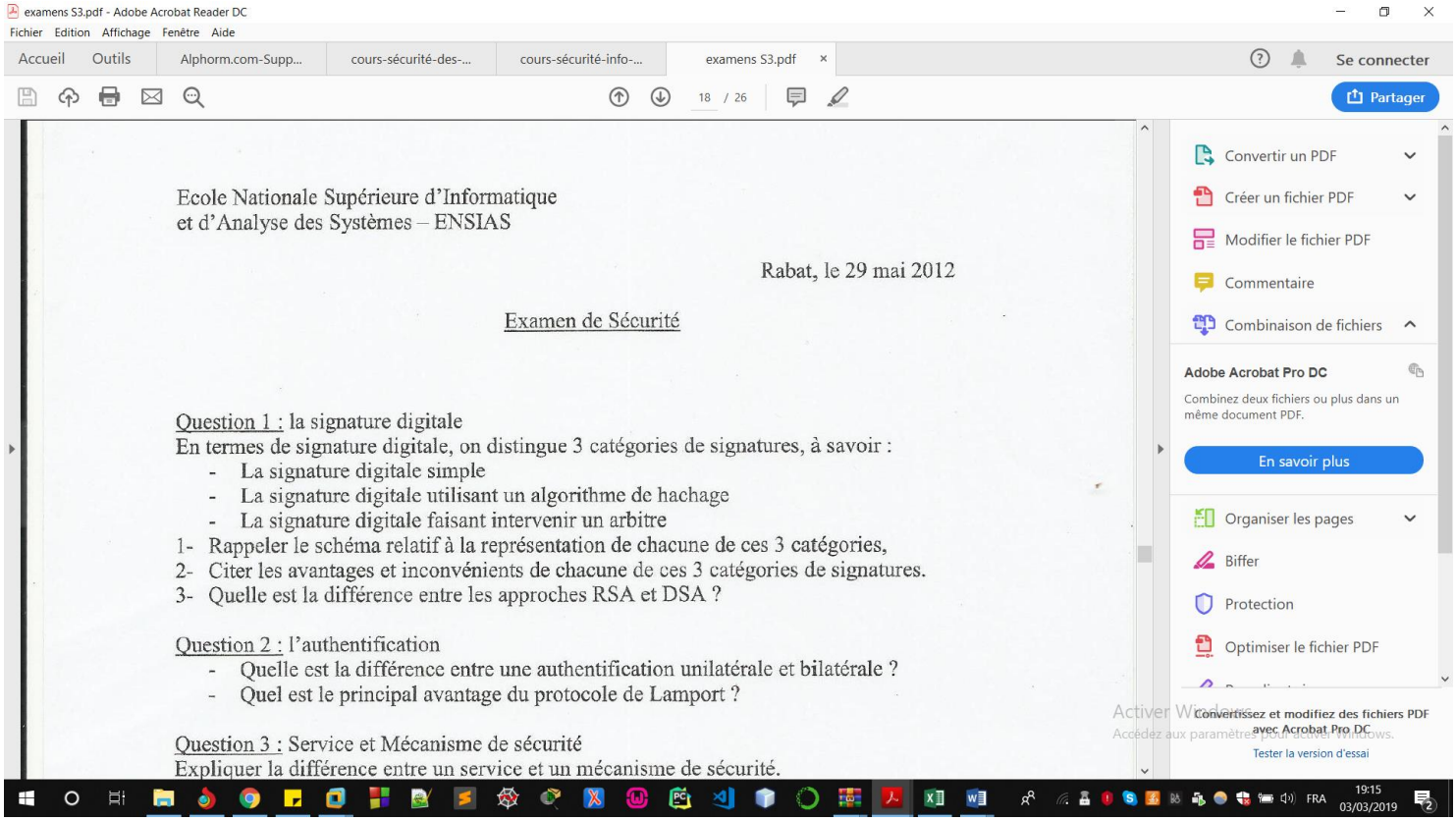
QCM tiré des prises de notes du cours de Sécurité des Systèmes

1. La **triade de la sécurité** est :
   - ☐ La **CIA** pour Confidentialité-Intégrité-Disponibilité
   - ☐ La **CIA** pour Confidentialité-Intégrité-Authentification
   - ☐ La **CIA** pour Contrainte-Information-Attaque
   - ☐ Protection-Détection-Réaction
2. On peut considérer qu'on a plus ou moins :

sécurité informatique ⊂ sécurité des systèmes ⊂ sécurité des systèmes d'information ⊂ sécurité de l'information

   - ☐ Vrai
   - ☐ Faux
3. Une source de la menace concrétise…….. Une menace exploite une…….. menant à un …….
   Le propriétaire impose des …… pour réduire le …… sur ses ……...
   - ☐ Menace vulnérabilité risque contre-mesures risque actifs
   - ☐ Attaque vulnérabilité incident privilèges risque actifs


examens S3.pdf - Adobe Acrobat Reader DC
Fichier Edition Affichage Fenêtre Aide
Accueil Outils Alphorm.com-Supp... cours-sécurité-des-... cours-sécurité-info-... examens S3.pdf
Se connecter
Partager
18 / 26
Ecole Nationale Supérieure d'Informatique
et d'Analyse des Systèmes – ENSIAS
Rabat, le 29 mai 2012
Examen de Sécurité
Question 1 : la signature digitale
En termes de signature digitale, on distingue 3 catégories de signatures, à savoir :
- La signature digitale simple
- La signature digitale utilisant un algorithme de hachage
- La signature digitale faisant intervenir un arbitre
1- Rappeler le schéma relatif à la représentation de chacune de ces 3 catégories,
2- Citer les avantages et inconvénients de chacune de ces 3 catégories de signatures.
3- Quelle est la différence entre les approches RSA et DSA ?
Question 2 : l'authentification
- Quelle est la différence entre une authentification unilatérale et bilatérale ?
- Quel est le principal avantage du protocole de Lamport ?
Question 3 : Service et Mécanisme de sécurité
Expliquer la différence entre un service et un mécanisme de sécurité.
Convertir un PDF
Créer un fichier PDF
Modifier le fichier PDF
Commentaire
Combinaison de fichiers
Adobe Acrobat Pro DC
Combinez deux fichiers ou plus dans un même document PDF.
En savoir plus
Organiser les pages
Biffer
Protection
Optimiser le fichier PDF
Convertissez et modifiez des fichiers PDF avec Acrobat Pro DC
Tester la version d'essai
Activer Windows
FRA
19:15
03/03/2019

examens S3.pdf - Adobe Acrobat Reader DC

Fichier Edition Affichage Fenêtre Aide

Accueil Outils Alphorm.com-Supp... cours-sécurité-des-... cours-sécurité-info-... examens S3.pdf

Se connecter

18 / 26

Partager

Question 3 : Service et Mécanisme de sécurité

Expliquer la différence entre un service et un mécanisme de sécurité.

C:\Users\marouan\Desktop\examens S4 2012\Sécurite des Systemes Informatiques.jpg

Exercice 1 :

1- Rappeler le principe de fonctionnement d'un certificat numérique.
2- En quoi consiste un certificat auto-signé ? Qu'est-ce qui en justifie l'usage ?
3- Donner les différentes phases par lesquelles passe la mise en place d'un environnement supportant les certificats auto-signés (faire un schéma), et incluant 2 entités (l'émetteur et le récepteur du certificat), ainsi que le fichier à signer.
4- Quelles sont les contraintes techniques imposées par l'environnement Java, nécessaires à la signature d'un fichier ?

Exercice 2 :

On souhaite implémenter le mécanisme de contrôle d'accès, en faisant appel au contrôle d'accès mandataire.

1- Rappeler les règles appliquées aux labels qui sont nécessaires afin de prendre les décisions d'accès.
2- Quels sont les droits d'accès en lecture/écriture dont bénéficient les sujets S1 et S2, sur l'objet O1, dans la situation suivante ?
On dispose de 2 sujets, S1 et S2, ayant les labels de sécurité respectifs :
- S1: Secret [Finances]
- S2: Top Secret [Production, Ventes, Finances]

On dispose d'un objet, noté O1 (fichier clientèle), ayant le label de sécurité suivant :
- O1: Secret [Finances, Ventes]

Justifier votre réponse.

Convertir un PDF
Créer un fichier PDF
Modifier le fichier PDF
Commentaire
Combinaison de fichiers
Adobe Acrobat Pro DC
Combinez deux fichiers ou plus dans un même document PDF.
En savoir plus
Organiser les pages
Biffer
Protection
Optimiser le fichier PDF
Convertissez et modifiez des fichiers PDF avec Acrobat Pro DC
Tester la version d'essai

Activer Windows
Accédez aux paramètres pour activer Windows.

FRA 19:15 03/03/2019

Exams S4 2014-2015.pdf - Adobe Acrobat Reader DC

Fichier Edition Affichage Fenêtre Aide

Accueil Outils Alphorm.com-Supp... cours-sécurité-des-... cours-sécurité-info-... Exams S4 2014-201...

Se connecter

29 / 43

Partager

Exercice 1 :

Expliquer la différence entre un service et un mécanisme de sécurité.

Exercice 2 : Répondre par vrai ou faux

Question :	Vrai	Faux
1. La sténographie correspond à une technique de cryptanalyse pouvant agir sur le son ou l'image numérique.		
2. Le chiffrement RSA est un système cryptographique symétrique.		
3. La non répudiation est un service de sécurité.		
4. La signature digitale utilisant un algorithme de hachage, selon l'approche RSA, permet de générer une signature différente pour le même message, à deux instants différents.		
5. Le protocole de Lamport permet de garantir le mécanisme de contrôle d'accès en se basant sur une fonction unidirectionnelle.		
6. Le protocole de Diffie Hellman se base sur le principe de trouver un entier 'a' étant données les 2 valeurs déjà connues 'g^a' et 'g'.		
7. Un certificat auto-signé ne nécessite pas de validation de la part d'une autorité de certification.		
8. Le protocole de Needham et Schroeder est un exemple d'authentification bilatérale.		

Exercice 3 :

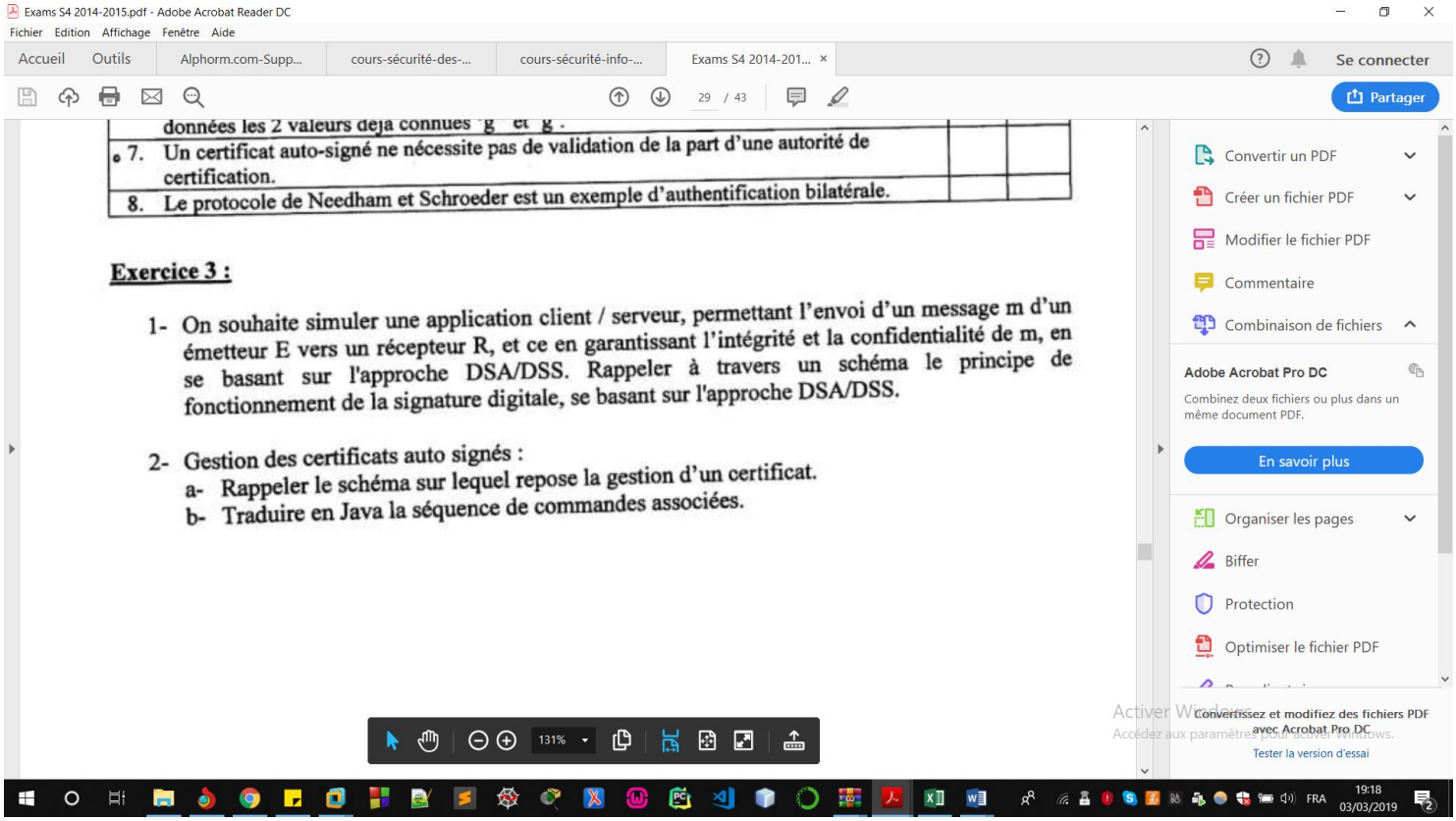
1- On souhaite simule[illegible]envoi d'un message m d'un émetteur E vers un[illegible] la confidentialité de m, en [illegible] schéma le principe de

131%

Convertir un PDF
Créer un fichier PDF
Modifier le fichier PDF
Commentaire
Combinaison de fichiers
Adobe Acrobat Pro DC
Combinez deux fichiers ou plus dans un même document PDF.
En savoir plus
Organiser les pages
Biffer
Protection
Optimiser le fichier PDF
Convertissez et modifiez des fichiers PDF avec Acrobat Pro DC
Tester la version d'essai

Activer Windows
Accédez aux paramètres pour activer Windows.

FRA 19:18 03/03/2019



Réponses au QCM de Sécurité de Systèmes

(Date de dernière mise à jour : 03 mars 2019)

Vous remarquerez que la réponse à chaque question est la première réponse exceptées pour les questions **5** et **21**.