



**MINISTÈRE  
DES ARMÉES**

*Liberté  
Égalité  
Fraternité*

# ANNALES DU CONCOURS

**Accès au corps des attachés  
de la DGSE**

Épreuve d'admissibilité :  
spécialité sciences et technologie - informatique



**Session 2022**



**MINISTÈRE  
DES ARMÉES**

*Liberté  
Égalité  
Fraternité*

# 3<sup>ème</sup> épreuve d'admissibilité

**Spécialité : sciences et technologie - informatique**

Épreuve consistant à répondre à une série de questions portant sur la spécialité « Sciences et technologie - Informatique ».  
Il est demandé au candidat de démontrer les étapes de son raisonnement en exploitant les documents du dossier comprenant dix pages maximum et en faisant appel à ses connaissances personnelles.



**Durée : 4 heures - coefficient 8**

**CONCOURS EXTERNE  
POUR L'ACCÈS AU CORPS DES ATTACHÉS  
SESSION 2022**

**Epreuve d'admissibilité :**

**Spécialité : Sciences et technologie -  
Informatique**

Épreuve consistant à répondre à une série de questions portant sur la spécialité « **Sciences et technologie - Informatique** ». Il est demandé au candidat de démontrer les étapes de son raisonnement en exploitant les documents du dossier comprenant dix pages maximum et en faisant appel à ses connaissances personnelles.

Durée : 4 heures ; coefficient 8

---

Le questionnaire comporte des questions pour lesquelles une ou plusieurs réponses exactes sont possibles, et également des questions à choix multiples dont les réponses devront être traitées sur la copie, en aucun cas sur le sujet.

*NDE – aucun document n'est fourni en appui de ces questions*

**Questions à Choix Multiples :**

- Bonne réponse : +1 pt
- Absence de réponse : 0 pt
- Mauvaise réponse : -2 pt

## I. (20 points)

1. (3 pts) - Pour chaque couche du modèle OSI, indiquez les protocoles qui sont au bon niveau parmi ceux proposés :
  1. Couche 1 : ARP – BLUETOOTH- ATM-ADSL
  2. Couche 2 : Ethernet-ZigBee-ARP-ISDN
  3. Couche 3 : UDP-IPv4-ARP-OSPF
  4. Couche 4 : IPv6-TCP-UDP-PPP
  5. Couche 5 : UDP-RPC-NetBIOS-SMB
  6. Couche 6 : SMB-HTTP-MIME-ASCII
  7. Couche 7 : HTTPS-SNMP-FTP-TELNET
2. (2 pts) - Conversions
  1.  $42_{(10)} = \dots\dots\dots_{(16)}$
  2.  $252_{(10)} = \dots\dots\dots_{(2)}$
3. (2 pts) - Quelle{les} est{est/sont} les affirmations fausses relatives au protocole Kerberos ?
  1. C'est un protocole d'authentification basé sur l'utilisation de tickets.
  2. C'est un protocole uniquement utilisé par Microsoft.
  3. C'est un protocole tolérant aux dérives NTP.
  4. C'est un protocole libre.
  5. Le rejeu d'une capture permet une authentification.
  6. L'usage d'un réseau sécurisé est obligatoire après la phase d'échange avec le TGS.
4. (2 pts) - Quels protocoles utilisent un chiffrement à clé secrète ?
  1. SSL
  2. AES
  3. SHA1
  4. DSA
  5. 3DES
  6. MD5
  7. SSH
  8. Blowfish
5. (3 pts) - Citez les rôles FSMO par leur acronyme ainsi que par leur nom (français).
6. (1 pt) - Lequel des rôles FSMO précédents doit être unique ?
7. (2 pts) - L'objectif d'un PRA est de :
  1. Continuer l'activité avec une interruption possible
  2. Continuer une activité sans interruption
  3. Continuer une activité si le système est assuré
  4. Identifier les causes d'un sinistre
8. (2 pts) - Quelle est la différence entre un MTA et un MTU ?
9. (1 pt) - Quel est le langage qui n'est pas orienté objet ?
  1. JAVA
  2. C
  3. C++
  4. PYTHON
10. (2 pts) - Que fait la commande suivante ?  

```
for F in `find -maxdepth 1 -type f`; do ls -l $F; done |awk 'BEGIN {sum = 0} {sum = sum + $5} END {print sum}'
```

  1. Elle calcule la taille en octet des fichiers du répertoire courant.
  2. Elle calcule la taille en octet des entrées du répertoire courant.
  3. Elle calcule la taille en octet des fichiers des répertoires descendants.
  4. Elle calcule la taille en octet des entrées des répertoires descendants.
  5. Elle ne fonctionne pas et retourne une erreur.
  6. Elle fonctionne mais retourne une erreur.
  7. Elle fonctionne mais retourne une valeur fausse.

## II. (15 points)

Décrivez l'ensemble des actions qui s'enchaînent lorsque, depuis un poste fraîchement allumé, un utilisateur d'un navigateur clique sur un lien hypertexte portant un cadenas jusqu'à ce que la nouvelle page s'affiche sur son écran. Un chronogramme détaillé sera utilisé.

## III. (20 points)

En tant que RSSI de l'entreprise *Licorne*, OIV, vous recevez une communication de l'ANSSI vous informant d'une probable intrusion sur votre SI. La communication indique que la clé du certificat racine de *Licorne* a été dérobée.

1. Qu'est-ce qu'un OIV ?
2. Qu'est-ce que l'ANSSI ? Quel est son rôle ?
3. Décrivez la chaîne SSI.
4. Quels sont les principes et usages d'un certificat racine ?
5. Décrivez une chaîne de certification.
6. Citez trois opérateurs de certification dont un français.
7. Quels sont les risques issus de ce vol ? (Au moins un risque non-technique sera demandé)
8. Qu'est-ce qu'une licorne (en dehors de l'animal mythologique...) ?

## IV. (10 points)

Vous souhaitez contracter un abonnement pour un espace de stockage S3. Vous devez rédiger deux notes synthétiques (en 15 lignes maximum chacune) au profit respectivement du DSI et du RSSI afin de leur présenter la stratégie, les gains escomptés et une analyse de risque pour ce dernier.

## V. (10 points)

Formaliser en 15 lignes maximum la différence entre virtualisation et conteneurisation avec leurs avantages et inconvénients respectifs (dans un tableau).

## VI. (5 points)

La France et les Etats-Unis ont une approche différente concernant la doctrine d'attribution. Détaillez chacune en 5 lignes maximum.

## VII. (10 points)

Fournir un code Python (Python.3) de 20 lignes maximum réalisant la fonction suivante :

Convertir un nombre en chiffres romains fourni en entrée en base 10.

Limites :

- Doit fonctionner pour tout nombre positif inférieur ou égal à 1000.
- Ne doit pas utiliser de bibliothèque spécifique (hors *sys*).

Exemple :

Saisie : `python3 conv.py XIV`

Retour : 14

## VIII. (10 points)

Citez deux failles majeures ayant impacté le protocole TLS et expliquez chaque faille (10 lignes maximum par faille).



**MINISTÈRE  
DES ARMÉES**

*Liberté  
Égalité  
Fraternité*

# Copie ayant obtenu la meilleure note

**Spécialité : sciences et technologie - informatique**

L'administration n'a volontairement pas corrigé les imperfections de fond et de forme dans la copie communiquée ci-après.



Année : 2022

Concours : Concours externe pour  
l'accès au corps des attachés

Épreuve : Informatique

## Consignes :

- Ne pas signer la composition et ne pas y apporter de signe distinctif
- Numéroté chaque page; placer l'ensemble dans l'ordre et le bon sens
- N'effectuer aucun collage ou découpage de sujets ou de feuilles
- Ne joindre aucun brouillon



1931EATT22

CONCOURS ATT EXTERNE

08/12/2022

1931EATT22

Exercice I:

## 1. Modèle OSI

- 1) Couche 1: Bluetooth - ADSL
- 2) Couche 2: Ethernet - ZigBee
- 3) Couche 3: IPv4 - ARP
- 4) Couche 4: TCP - UDP - PPP
- 5) Couche 5: RPC - NetBIOS
- 6) —
- 7) —

## 2. Conversions

$$42_{(10)} = 2A_{(16)}$$

$$252_{(10)} = 11111100_{(2)}$$

## 3. —

## 4. Les protocoles qui utilisent un chiffrement à clé secrète sont:

- |        |         |              |
|--------|---------|--------------|
| 1. SSL | 5. 3DES | 8. Blowfish. |
| 2. AES | 7. SSH  |              |

## 5. —

## 6. —

## 7. L'objectif d'un PRA est de:

1. Continuer l'activité avec une interruption possible.

8. ✓

9. le langage qui n'est pas orienté objet est :  
2 - C

10. —

Exercice IV : La virtualisation et la conteneurisation sont deux technologies qui répondent à un besoin de reproductibilité, d'isolation et de portabilité. Cependant, ces technologies se basent sur deux concepts différents :

La virtualisation se base sur l'émulation d'une machine (mémoires, CPU, carte réseau) pour y exécuter un système d'exploitation.

La conteneurisation est une "enveloppe" qui embarque les fichiers et l'environnement nécessaire pour l'exécution d'une application. L'exécution est réalisée en interaction avec le noyau système de la machine hôte.

Tableau comparatif des technologies.

	virtualisation	Conteneurisation.
Volumé	Très élevé : contient l'OS	Moderé : contient les source et les bibliothèques
Portabilité	Très bonne	Il faut faire attention aux interaction noyau de l'application.
Partage des ressources	Les ressources sont réservées par l'émulateur (inconvenient)	Les ressources sont gérées par le système hôte (avantage)
Systèmes embarqués	Permet la cohabitation de plusieurs OS, par exemple 1 classique et 1 temps-réel	



### Exercice III:

1. Un OIV (Organisme d'Importance Vitale) est un organisme privé ou public qui fournit un ou des services vitaux pour la France. Ils sont présents dans des secteurs variés: Énergie, Santé, Télécom par exemple.

2. L'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) est une autorité de sécurité et de défense. En lien étroit avec le SGDSN (Secrétariat Général de la Défense et de la Sécurité de la Nation), ses principales missions sont:

- Maintenir une expertise technique sur la cybersécurité.
- Étudier & Qualifier des produits en lien avec la cybersécurité.
- Sensibiliser les entreprises aux risques cyber.
- Accompagner les OIV dans leurs démarches de résistance et de résilience en termes de cybersécurité.
- Effectuer une veille sur l'état de la menace cyber.

3. La chaîne SSI est l'ensemble des moyens mis en œuvre pour renforcer la sécurité des systèmes d'information. Ces moyens peuvent être techniques et physiques, comme l'utilisation d'un fire-wall dans un rack serveur. Ils peuvent également être techniques et virtuels, comme l'utilisation d'un système de détection d'intrusion (IDS). Mais ils sont également non-techniques, notamment la formation des usagers aux risques et enjeux de la cybersécurité.

Ces moyens déployés doivent être en accord avec la politique de sécurité du SI, qui doit être définie en amont.

4. Un certificat racine est un moyen technique de définir et d'attester de l'identité numérique d'une entité. Il se base entre autre sur un secret cryptographique (clef privée) qu'il est impératif de sécuriser correctement.

Ce certificat racine peut être utilisé pour certifier d'autres certificats (d'une même entité généralement). Cela permet, grâce au https de s'assurer qu'un site web associé à un nom de domaine est bien possédé par l'entreprise. Un autre exemple d'utilisation du certificat racine est la génération de certificats pour les employés d'une entreprise.



Grâce à ces certificats, les employés pourront par exemple se connecter par VPN aux ressources de l'entreprise.

Le certificat racine permet également de révoquer les certificats qu'il a générés. Cette action est très utile en cas de vol, piratage ou départ d'un employé.

### 5. Exemple de chaîne de certification pour un site web.

Le certificat racine est possédé par une entreprise privée dont le métier est de générer des certificats pour d'autres entités. Cette entreprise propose des garanties très fortes sur la sécurité des certificats, elle est également très réactive pour révoquer des certificats si nécessaire.

Cette première entreprise A a généré un certificat pour l'entreprise B dont le métier est l'hébergement web.

Dans le cadre de l'hébergement web, l'entreprise B propose à ses clients des certificats pour qu'ils puissent utiliser le protocole HTTPS.

La chaîne de certification lorsque l'on visite le site d'un client (C) de l'entreprise B est donc :

Cert-A  $\rightarrow$  Cert-B  $\rightarrow$  Cert-C.

Pour vérifier la validité du Cert-C, il faut donc vérifier qu'il est valide grâce au Cert-B, qui lui-même doit être valide grâce au Cert-A.

6. GoDaddy, Microsoft Azure et OVH sont trois opérateurs de certification. OVH est un acteur français.

7. Le vol du certificat rend caduc les moyens cryptographiques mis en place grâce à ce certificat. Le vol d'un certificat permet également l'usurpation d'identité numérique. Un des risques est donc réputationnel.

Un autre risque de ce vol est le déni de service : en révoquant l'intégralité des certificats d'une entité, il est possible de créer une discontinuité dans le fonctionnement de son SI.

8. Une licorne est une jeune entreprise (start-up) dont la valorisation dépasse 1 milliard de dollars.

Année : 2022

Concours : Concours externe pour  
l'accès au corps des attachés

Épreuve : Informatique

## Consignes :

- Ne pas signer la composition et ne pas y apporter de signe distinctif
- Numéroté chaque page; placer l'ensemble dans l'ordre et le bon sens
- N'effectuer aucun collage ou découpage de sujets ou de feuilles
- Ne joindre aucun brouillon



1931EATT22

CONCOURS ATT EXTERNE

08/12/2022

1931EATT22

Exercice VI:

En France, le gouvernement estime que l'attribution est un acte de politique étrangère fort. Il estime donc que cet acte doit être suivi de conséquences à l'encontre de l'attaquant (sanctions). De ce point de vue l'attribution doit prendre en compte la politique étrangère. Jusqu'à présent peu d'attributions ont été faites par la France, mais la tendance est à la hausse.

Aux Etats-Unis, le lien politique étrangère - attribution est moins prégnant. Il est considéré que chaque attaque doit être dénoncée et donc les attributions sont beaucoup plus fréquentes.

Exercice VII:

En considérant la correspondance suivante : I=1, V=5, X=10, C=50, D=100 et M=1000. Et que IDCXIV = 264.

conv.py

input = stdin.read-line()

sum = 0

previous = 'V'

for c in input.chars():

if c == 'I':

sum += 1

else if c == 'V':

sum += 5

if previous == 'I':

sum -= 2

else if c == 'X':

sum += 10

conv.py (suite)

else if c == 'C':

sum += 50

else if c == 'D':

sum = max(100, sum\*100)

else if c == 'M':

sum = max(1000, sum\*1000)

else:

print("Not a roman number")

return

previous = c

print(sum)



### Exercice VIII :

La faille Heartbleed a affecté le protocole TLS. Elle permettait de rendre caduque les moyens cryptographiques mis en place par TLS. Cette faille se base sur un défaut d'implémentation. En effet, à l'initialisation de certains échanges une des structures utilisée n'était pas remise à zéro, son contenu était alors prédictible et permettant d'affaiblir le secret cryptographique.

Exercice II : Chronogramme détaillé des actions entre un clic utilisateur et l'affichage d'une page sur son écran.





#### Exercice IV:

- Note à l'intention de Monsieur le Directeur du Système d'Information.

Dans le cadre de l'évolution des besoins de l'entreprise et donc de son SI, il me semble primordial de faire évoluer nos capacités de stockage. Pour cela, l'équipe en charge de la transition a identifié une solution: l'offre d'abonnement pour un espace de stockage S3.

Bien que de prime abord le recours à cette solution semble être plus onéreux que notre solution actuelle, le gain escompté sur les coûts d'entretien et de maintenance de nos équipements permet de réduire significativement l'écart comptable entre les deux solutions.

Il est également à noter que cette solution améliorerait, pour nos clients, le temps d'accès, et de réponse. Le deuxième avantage étant une meilleure disponibilité de nos données, nous pourrions améliorer notre satisfaction client en adoptant cette solution.

Enfin, la rapide croissance de notre entreprise pourrait également bénéficier de cette solution, car les possibilités de mise à l'échelle du stockage sont nettement meilleures avec ce type de contrat qu'avec du matériel physiquement présent sur site.

- Note à l'intention de Monsieur le responsable de la sécurité des systèmes d'information.

Dans le cadre de l'évolution des besoins de l'entreprise et donc de son SI, il me semble primordial de faire évoluer nos capacités de stockage. Pour cela, l'équipe en charge de la transition a identifié une solution: l'offre d'abonnement pour un espace de stockage S3.

Cette offre de stockage, conforme au RGPD, nous permettrait d'externaliser les risques cyber vers une entité dont le métier inclut la gestion de ces risques. Là où aujourd'hui le piratage de notre SI permettrait aux hackers d'exfiltrer ou de rançonner nos données, avec cette solution nous pourrions offrir plus de garanties de sécurité sur ces données. Ce rapprochement entre nos données et notre SI permettrait donc de rendre l'entreprise plus résiliente à une attaque, ou même un sinistre.

Pour mitiger les risques liés à l'accès à distance, nous pourrions nous reposer sur les mécanismes d'authentification proposés par l'entreprise offrant le service. Cela devra nécessairement passer par la mise à jour

de notre politique d'accès et les droits de nos utilisateurs.

Je tiens également à attirer votre attention sur la mise en place d'un système de sauvegardes réparties sur plusieurs sites physiques grâce à cette solution.