DM de révision avril 2024

Nom :	Note : / 20
	Classe :

Sommaire

Préparation des épreuves 2024

1 Les épreuves pratiques 2024 NSI

1.1 Le lien officiel

https://cyclades.education.gouv.fr/delos/public/listPublicECE

1.2 Travail demandé

Organisez-vous un planning prévisionnel de révision de ces 48 sujets, soit 96 exercices, pour les avoir tous faits au lundi 13 mai 2024. Profitez évidemment des vacances et des jours fériés. A rendre pour cette question votre planning prévisionnel à envoyer via l'ENT **avant la fin des vacances scolaires**.

2 L'épreuve écrite de spécialité

2.1 Révision de l'épreuve écrite bac blanc n°2

Le second Bac Blanc aura lieu le mardi 30 avril de 13H30 à 17H30. Les élèves qui terminent avant la fin du temps prévu iront en projet dans la salle 109.

Vous pouvez vous entrainer sur des sujets via la banque de sujets du site pixees par exemple. Cet entraînement sera permanent en tâche de fond jusqu'aux épreuves écrites de spécialités.

3 Préparation du grand oral

3.1 Choisir sa ou ses questions

Vous devez fournir des propositions de questions de grand oral, soit une question simple, soit une question combinée avec votre deuxième spécialité. **Ces propositions seront fournies dans votre devoir, non évaluées évidemment.**

Rédiger sur copie les réponses aux questions posées ci-dessous.

Cryptanalyse

4 Cryptographie quelques fonctions utiles

La fonction chr(x)

Q1. Quelle est le type de la valeur x à fournir à la fonction ?

Q2. Que réalise la fonction chr (x) ?

Q3. Donnez les résultats pour x =
☐ $41
☐ $1f40d
☐ 90
☐ 65

La fonction ord(y)

Q4. Quelle est le type de la valeur y à fournir à la fonction ?

Q5. Que réalise la fonction ord (y) ?

Q6. Donnez les résultats pour y =
☐ ‘B’
☐ ‘b’
☐ '🐍'

Un premier bilan

Q7. Que pensez-vous de l’utilité des fonctions chr( ) et ord( ) dans les programmes de cryptographique.

5 Le codage de César

Analyse du codage de César

```
 7  def codageCesar(m,k):
 8      mc = ''
 9      for c in m:
10          index = ((ord(c)-65) + k)%26
11          mc+=chr(65+index)
12      return mc
```

Q8. Que réalise cette fonction ? Précisez en particulier le rôle des variables m, k mc et des valeurs 65 et 26

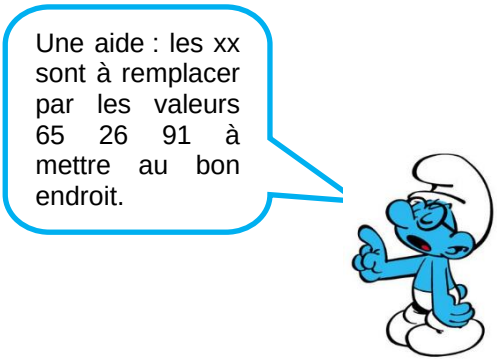
Q9. Commenter plus particulièrement ces deux lignes :

```
10          index = ((ord(c)-65) + k)%26
11          mc+=chr(65+index)
```

Le décodage de César

Q10. Compléter le code de la fonction décodage de César donné ci-dessous, puis codez le et faites-le fonctionner.

```
def decodageCesar(mc,k):
    m = ''
    for c in mc:
        index = ((ord(c)- xx ) - k) % xx
        m+=chr( xx +index)
    return m
```



6 Le challenge

Où se trouve le réseau d'agents ennemis ? C'est à vous de découvrir la ville où se situe leur base. Pour cela vous devez décoder le message de votre QG qui a été codé avec la clé FCSC.

# DECRYPTAGE DE VIGENERE
chaine_a_decoder = '''Gqfltwj emgj clgfv ! Aqltj rjqhjsksg ekxuaqs, ua
xtwkn'feuguvwb gkwp xwj, ujts f'npxkqvjgw nw tjuwczugwygjtfkf
qz uw efezg sqk gspwonu. Jgsfwb-aqmu fPspygk nj 29 cntnn hqzt
dg igtwy fw xtvjg rkkunqf'''

cle = 'FCSC'

Q11. Donnez le nom de la ville.

Q12. Envoyer votre code python avec votre nom via l'ENT, la note sera établie après une interrogation orale et une démonstration du fonctionnement.

Quelques conseils

1) Supprimer tous les caractères du message qui ne sont pas des lettres
2) Mettez toutes les lettres du message en majuscules.
3) On identifie la valeur des décalages imposé par la clé.
4) On décode le message en utilisant ces décalages en fonction de la longueur de la clé.

Voilà les codes ci-dessous que vous pouvez copier dans Spyder

```
def codageCesar(m,k):
    mc = ''
    for c in m:
        index = ((ord(c)-65) + k)%26
        mc+=chr(65+index)
    return mc

# Test de la fonction
message = 'VIVENSI'
message_code = codageCesar(message,15)
assert message_code == 'KXKTCHX', "Le codage est erroné"


def decodageCesar(mc,k):
    m = ''
    for c in mc:
        index = ((ord(c)- xx ) - k) % xx
        m+=chr( xx +index)
    return m

# Test de la fonction
message_code = 'UZPJLZAMHUAHZAPXBL'
message_decode = decodageCesar(message_code,7)
print(message_decode)
```

7 La sécurité des communications

Voilà la ressource permettant de répondre aux questions de cette partie.
https://eduscol.education.fr/sti/sites/eduscol.education.fr.sti/files/ressources/pedagogiques/16723/16723-la-revue-3ei-n111-janvier-2024-ensps.pdf

7.1 Introduction : les domaines concernés

Q13. Citez les trois domaines concernés par les problèmes de cybersécurité et présentés dans le document page 5.

Q14. Citez les trois exemples proposés en cas d'étude pour la cybersécurité des trois domaines de la question précédente.

7.2 Principes fondamentaux de la cybersécurité

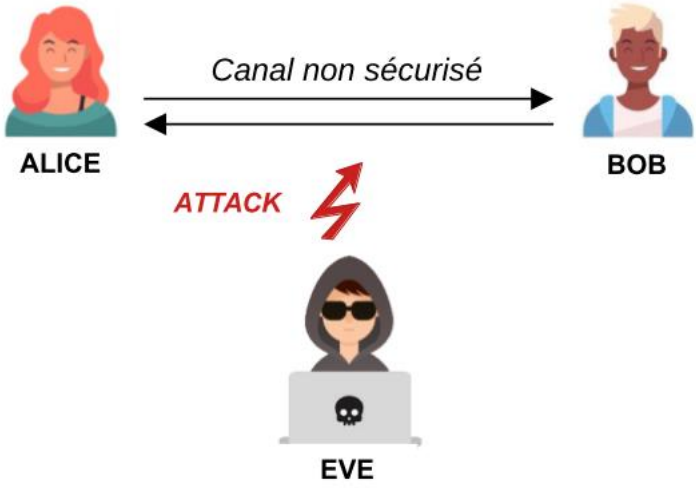


Figure 1 : Schéma simplifié d'une attaque

Dans le contexte de la cyber sécurité des communications réseau définir les termes suivants :

Q15. La confidentialité :

Q16. L'intégrité

Q17. L'authentification

Q18. La non répudiation

Q19. La disponibilité

7.3 Pour approfondir

A partir des pages mentionnées répondre aux questions ci-dessous de manière simple et concise.

Confidentialité

[Pages 14-16]

Q20. Quels sont les problèmes des chiffrements symétriques ?

Q21. Que peut faire un attaquant qui trouve la clé de chiffrement d'une discussion entre 2 personnes ?

Q22. Citez le nom de l'algorithme de chiffrement symétriques le plus utilisé.

Q23. Pourquoi l'algorithme asymétrique qui est plus sécurisé que l'algorithme symétrique n'est-il pas utilisé pour gérer toutes les étapes d'un échange numérique ?

Q24. A quoi sert l'algorithme asymétrique ?

Intégrité

[Pages 17-18]

Q25. A quoi sert une fonction de Hachage ?

Q26. Donnez quelques propriétés d'une bonne fonction de hachage.

Q27. Citez une fonction de hachage cryptographique la plus utilisée.

Q28. C'est quoi une signature numérique ?

Authentification

[Pages 18-20]

Q29. En quoi consiste une attaque "Men in the middle" ?

Q30. A quoi sert un certificat ?