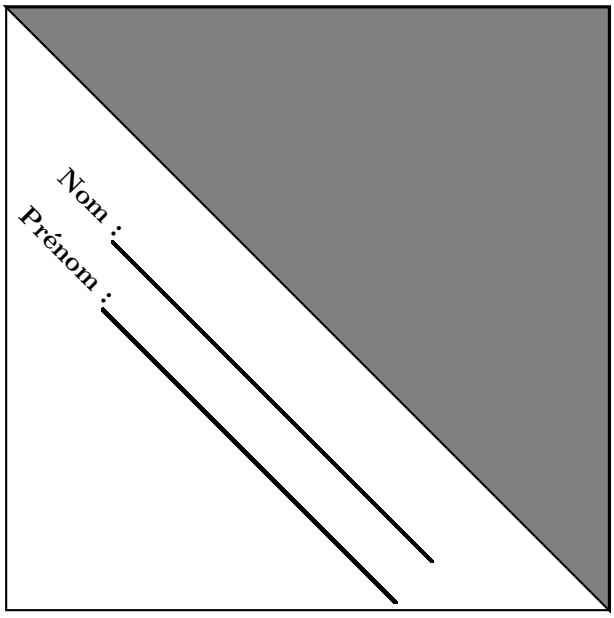
Université Côte d'Azur M1 Informatique
Sécurité 2022–2023

Examen juin 2023

Durée : 2h

Note :



L'examen comporte trois parties indépendantes. Répondez sur la copie avec clarté et concision.

1 Quizz sur la sécurité (5 points)

1. Expliquez brièvement ce qu'est le chiffrement hybride et un outil qui l'utilise.

2. Comment peut-on utiliser une fonction de hachage pour assurer une authentification ?

3. Quelle est la différence entre un VPN routé et un VPN ponté ?

4. Donnez au moins deux utilisations au bourrage (padding) et son utilité.

5. Expliquez le fonctionnement d'un mécanisme de dérivation de clé et son utilité.

2 Protocole KAD (10 points)

On s'intéresse au protocole de la FIGURE 1 ; p est un premier et α un générateur de $\mathbb{Z}_p$, noté additivement (comme dans le TD 4) :

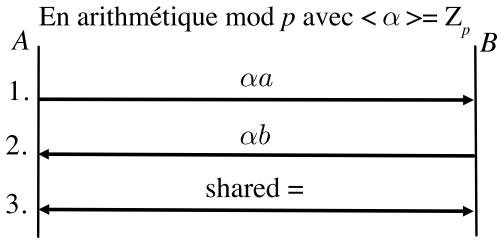


FIGURE 1 – Protocole KAD

1. Précisez tout d'abord quelles sont les données partagées entre A et B, puis les informations publiques et enfin les informations privées en complétant la tableau ci-dessous :

	A	B
partagées		
public		
privé		

2. À l'étape 3. du protocole, une valeur "shared" qui dépend des données échangées est partagée entre A et B. Expliquez comment les parties peuvent construire cette valeur "shared".

La valeur "shared" sert ensuite d'entrée à un algorithme de dérivation de clé noté `kdf()`.
3. Dites à quoi sert ce protocole et de quel protocole classique il s'inspire.

4. Précisez quelle est la taille maximale de la variable "shared".

5. Avec $\alpha = 3, p = 101$, les messages 33 et 93 ont été interceptés aux étapes 1. et 2. respectivement. Quelles sont les valeurs de a et de b ? Et de "shared" ?

Dans des communications successives utilisant ce protocole, on souhaite assurer la propriété de confidentialité persistante (ou *perfect forward secrecy* en anglais). Elle garantit que la découverte par un adversaire de la clé privée d'un correspondant (secret à long terme) ne compromet pas la confidentialité des communications passées.

6. Pour assurer la confidentialité persistante, on suppose fixée la valeur de la biclé de B. Expliquez comment assurer cette propriété sur une suite de deux échanges entre A et B.

7. Expliquez comment on pourrait utiliser ce protocole dans un mécanisme de chiffrement hybride. Vous décrirez tout particulièrement comment une donnée est chiffrée et au moyen de quels paramètres.

8. Après avoir rappelé le problème (supposé) difficile sur lequel ce protocole repose, que pensez-vous de sa sécurité ? Que faudrait-il faire pour le sécuriser ?

3 Chiffre à clé secrète [5 points]

On considère un chiffre produit itéré à 3 tours dont les 3 fonctions de substitutions (boîte S) proviennent de trois chiffres définis par mot clé. Il chiffre des clairs de 9 lettres et fournit des chiffrés de 9 lettres.

1. Complétez chacune des 3 substitutions suivantes (S1, S2, S3) de l'alphabet des clairs dans l'alphabet des chiffrés pour chaque paire `(MOTCLE, lettre clé)` spécfiés :

S1 : `(MASTER, e)`

a b c d e f g h i j k l m n o p q r s t u v w x y z

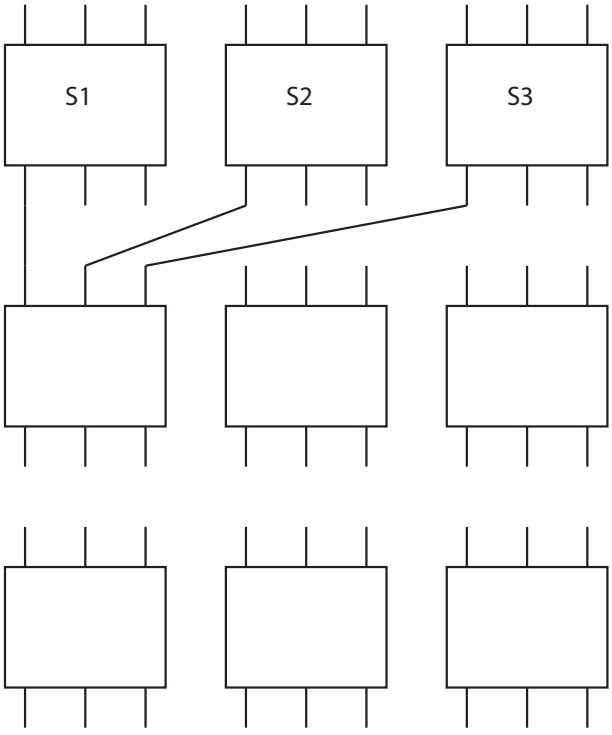
S2 : `(INFO, m)`

a b c d e f g h i j k l m n o p q r s t u v w x y z

S3 : `(NICE, u)`

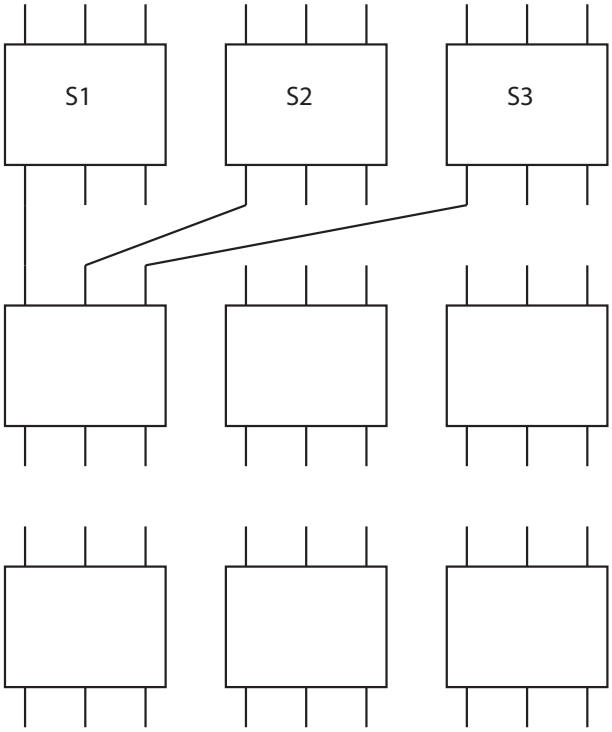
a b c d e f g h i j k l m n o p q r s t u v w x y z

2. La transposition est obtenue en reliant la j^{e} sortie de la i^{e} boîte S à la i^{e} entrée de la j^{e} boite S du tour suivant. Complétez la suite de transpositions du chiffre sur le schéma suivant :



3. Expliquez comment déchiffrer un message.

4. Déchiffrez le message `HIS YLZ BQH` en détaillant les opérations sur le schéma ci-dessous :



5. Dites ce que vous pensez de la sécurité de ce chiffre et donnez une amélioration simple et immédiate.