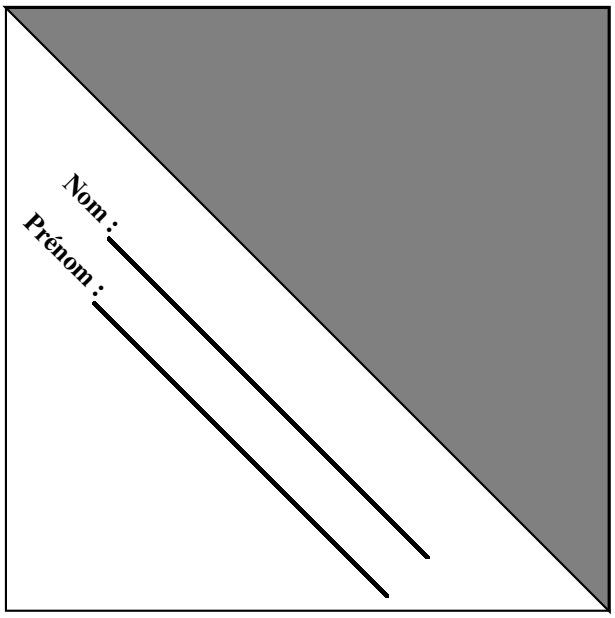
Université Côte d'Azur 2025–2026
L3 Informatique, L3 Math-Info

Codes, cryptographie & calcul symbolique

Examen du 9 janvier



Durée : 1h30
Une feuille manuscrite recto autorisée

Note :

On vous demande d'écrire les formules littérales avant d'effectuer les applications numériques.

Exercice 1 : (4 points) Chiffrement & signature RSA

Dans ce cryptosystème, les clefs publiques d'Alice et de Bob sont respectivement $(e_A, n_A) = (3, 33)$ et $(e_B, n_B) = (29, 65)$.

1. Trouvez la clef privée d_A correspondant à la clef publique (e_A, n_A) d'Alice.

2. Alice a chiffré son message M pour Bob et obtenu le chiffré $C = 2$. Elle veut le signer avant de l'envoyer. Comment signe-t-elle le chiffré C et qu'envoie-t-elle exactement à Bob ?

3. Comment Bob ou un tiers même peut-il vérifier la signature d'Alice ?

4. Comment s'y prend Bob pour déchiffrer le message d'Alice ? Vous devez calculer la clef privée d_B de Bob avant de découvrir le message M d'Alice.

5. A présent, comment s'y était prise Alice pour chiffrer le message clair M ?

Exercice 2 : (5 points) Chiffre de Merkle-Hellman Alice souhaite recevoir des messages chiffrés au moyen d'un cryptosystème de Merkle-Hellman. Elle choisit pour cela une suite super-croissante :

$$A = (3, 5, 10, 25, 57, 119, 243, 496, 1002)$$

un module $m = 2022$ supérieur à la somme des éléments de A et un entier $e = 809$ premier avec m.

1. Calculez la clef publique d'Alice en en donnant la formule au préalable.

2. Bob veut envoyer le message $M = 101010101$ à Alice, donnez le chiffré C_1 correspondant.

3. La clef privée d'Alice est constituée du triplet (A, d, m). Calculez l'entier d manquant. Détaillez votre façon de procéder (par tâtonnements, avec l'algorithme d'Euclide étendu ou en utilisant les propriétés de l'indicatrice d'Euler).

4. Chloé envoie le chiffré $C_2 = 5936$ suivant à Alice. Aidez cette dernière à déchiffrer le message de Chloé, en détaillant chaque étape y compris la trace de l'algorithme utilisé.

Exercice 3 : (4 points) Signature DSA

Considérons le jeu de paramètres DSA où la clef publique de Bob est $(p, q, \alpha, \beta) = (83, 41, 3, 29)$ et sa clef privée $k = 7$.

1. Comment Bob a-t-il calculé β ?

2. La première composante de la signature (γ, δ) ne dépend pas du message à signer mais juste de l'entier aléatoire $r = 14$ choisi par Bob. Calculez γ en commençant par donner sa formule.

3. Le message à signer est $M = 33$. Calculez la seconde partie δ de la signature sachant que :

$$\delta = (M \ + \ k.\gamma) \ . \ r^{-1} \bmod q$$

4. Après avoir vérifié que γ et δ sont dans le bon intervalle, procédez à la vérification de la signature. Vous donnerez les formules littérales avant d'effectuer les calculs nécessaires.

Exercice 4 : (4 points) Questions de cours

1. A quoi fait référence le terme *One Time Pad (OTP)* ? Détaillez un peu.

2. Expliquez en quoi consiste l'attaque de Yuval ? Détaillez.

3. Alice et Bob veulent jouer à pile ou face par téléphone sans tricherie possible. On suppose qu'ils se sont mis d'ccord sur une fonction à sens unique bijective f de E dans F et d'une partition $E = E_0 \uplus E_1$. Rappelez le protocole en 4 étapes leur permettant de jouer à distance.

4. Reconstituez la version récursive de l'algorithme d'Euclide étendu qui, outre le pgcd, calcule les coefficients de Bézout du couple d'entiers (a, b) :

```
def bezout(a,b) :
    if b == 0 :
        return ...
    q = ...
    r = ...
    (g,u,v) = ...
    return ...
```

Exercice 5 : (3 points) Factorisation Le nombre $n = 17399$ est un entier RSA car c'est le produit de deux nombres premiers p et q. On cherche à le factoriser.

1. Ici, on vous révèle que $\varphi(n) = 17136$ et la factorisation en devient possible. *Casser* cet entier n en réussissant à trouver ces deux facteurs. Vous détaillerez votre méthode.

2. Quelle est, en toute généralité, la classe de complexité du *Problème de la factorisation* ?