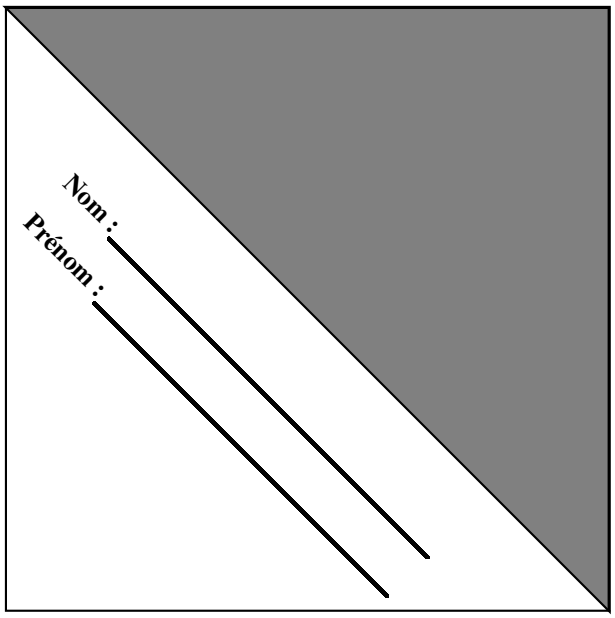
Université Côte d'Azur 2023–2024
Licence 3 Info, L3 Math-Info, L3 Sc. & Techn.

Cryptographie & calcul symbolique

Examen du 18 décembre



Durée : 1h30
Une feuille manuscrite autorisée

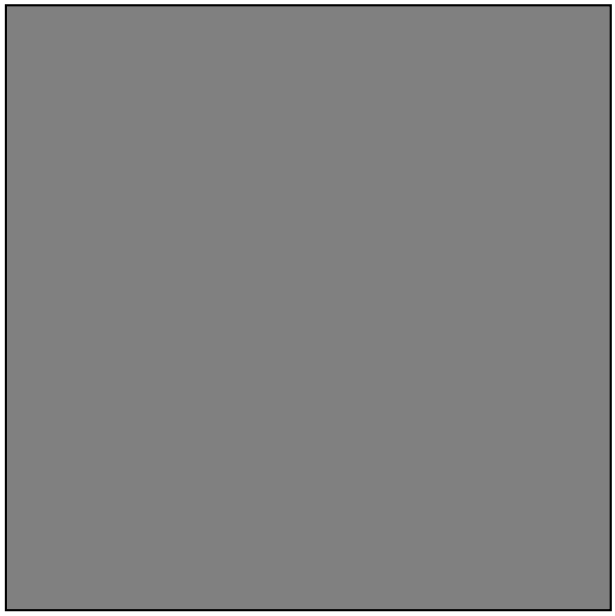
Note :

Exercice 1 : (3 points) Protocole de Diffie-Hellman Alice et Bob utilisent ce protocole pour partager un secret s et choisissent comme paramètres le générateur $g = 2$ et le module $p = 13$.

1. Sur quel problème repose la sûreté de ce protocole ? Dans quelle classe de complexité est-il ?

2. En plus que d'être vulnérable à l'attaque *Man in The Middle*, pourquoi ce protocole n'est pas adapté à l'échange d'une clef secrète pour faire du chiffrement symétrique ?

3. Eve espionne leurs communications, elle connaît donc les paramètres g et p. Elle voit passer un envoi d'Alice avec la valeur 4 et un envoi de Bob avec la valeur 7. Aidez Eve à retrouver leur secret en détaillant votre méthode et tous vos calculs.



Exercice 2 : (4 points) Chiffre de Merkle-Hellman Alice souhaite recevoir des messages chiffrés, elle a choisi la suite strictement super-croissante $A = [2, 5, 9, 21, 45, 103, 215, 450, 946]$, le module $m = 2023$ supérieur à la somme des éléments de A ainsi que l'entier $e = 120$ premier avec m.

1. Sachant que `bezout(120,2023)` renvoie $(1, -118, 7)$, quelle est la clef privée d d'Alice ?

2. Alice doit calculer sa clef publique avant de la diffuser. Donnez la formule littérale puis calculez cette clef.

3. Bob veut chiffrer le message $M_1 = 011010110$ pour Alice. Donnez le chiffré C_1 de ce message M_1.

4. Bob envoie aussi à Alice le chiffré $C_2 = 2721$ d'un second message M_2. Aidez Alice à déchiffrer ce message en détaillant toutes les étapes du déchiffrement de ce message M_2 chiffré par Bob.

5. Procédez à un calcul alternatif de l'inverse de $120 \mod 2023$ qui produit la partie de la clef privée d d'Alice.

Exercice 3 : (3,5 points) Chiffrement & signature RSA Considérons le cryptosystème RSA où la clef publique d'Alice est $(e_A, n_A) = (29, 65)$ et la clef publique de Bob est $(e_B, n_B) = (43, 77)$.

1. Trouvez les clefs privées d_A et d_B respectivement pour Alice et pour Bob.

2. Alice envoie à Bob le message chiffré puis signé (C, Z). Calculez la signature Z sachant que le message chiffré est $C = 50$.

3. Comment Bob ou un tiers aurait-il pu vérifier la validité de cette signature ?

4. Il ne reste plus qu'à aider Bob à déchiffrer le chiffré C pour obtenir le message initial M d'Alice.

Exercice 4 : (3,5 points) Chiffrement El Gamal La clef publique de Bob dans un cryptosystème El Gamal est $(p, \alpha, \beta) = (23, 7, 15)$.

1. Quelles sont les propriétés de chaque paramètre ? Expliquez comment et à partir de quoi cette clef a été calculée.

2. Alice lui envoie le chiffré $(c_1, c_2) = (11, 18)$ de son message M. Quelles formules a-t-elle appliquées pour obtenir le chiffré (c_1, c_2) ?

3. Pourriez-vous aider Bob à déchiffrer le message d'Alice sachant que sa clef privée est $(p, \alpha, \beta, k) = (23, 7, 15, 9)$.

4. Citez le principal avantage et le principal inconvénient du chiffrement El Gamal.

Exercice 5 : (3 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 :

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

Exercice 6 : (3 points) Questions de cours

1. Citez trois propriétes principales des fonctions de hachage cryptographiques. Quelles sont les fonctions de hachage qu'il est préférable d'utiliser actuellement, citez-en trois.

2. Définissez précisément les deux notions d'*identification* et d'*authentification*.

3. 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 ...
```