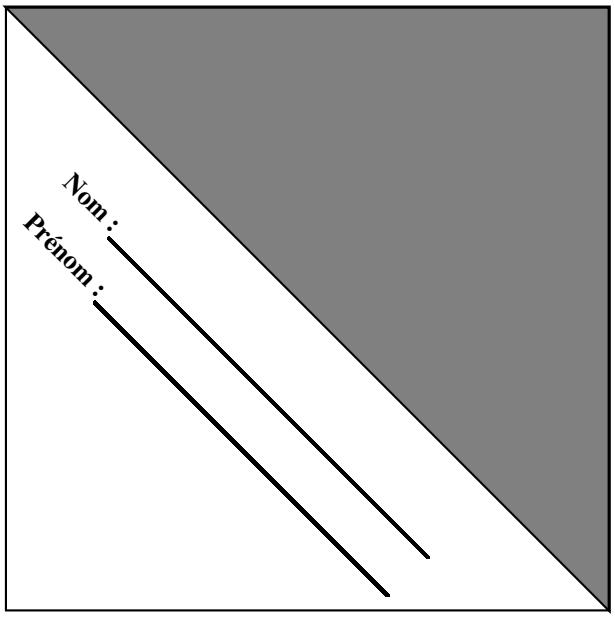
Université Côte d'Azur 2022–2023
Licence 3 Info, L3 Math-Info, L3 Sc. & Techn.

Cryptographie & calcul symbolique

Examen du 6 janvier



Durée : 1h30
Une feuille manuscrite autorisée

Note :

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

Exercice 1 : (4 points) Chiffrement & signature RSA Considérons le cryptosystème avec les clefs publiques d'Alice et de Bob respectivement égales à $(e_A, n_A) = (3, 33)$ et $(e_B, n_B) = (29, 65)$.

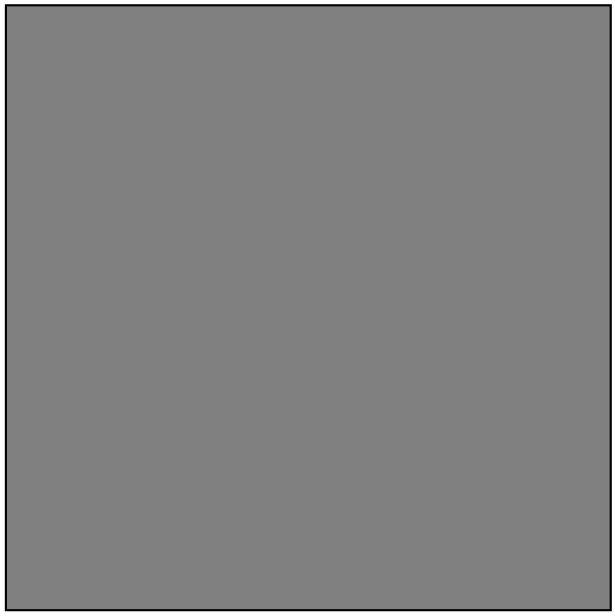
1. Trouvez la clef privée d_A correspondant à la clef publique (e_A, n_A) d'Alice.

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 : (4 points) Chiffre de Merkle-Hellman Alice souhaite recevoir des messages chiffrés, elle a choisi la suite strictement super-croissante $A = [2, 7, 11, 25, 48, 99, 201, 406]$, le module $m = 2023$ supérieur à la somme des éléments de A ainsi que l'entier $e = 71$ premier avec m.

1. Sachant que `bezout(71,2023)` renvoie $(1, 57, -2)$, 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 $M_1 = 01101010$ pour Alice. Donnez le chiffré C_1 de ce message M_1.

4. Bob envoie aussi à Alice le chiffré $C_2 = 4051$ d'un second message M_2. Effectuez chaque étape du déchiffrement de ce message afin d'aider Alice à déchiffrer le message M_2 de Bob.

5. Procédez à un calcul alternatif permettant de trouver la clef privée d d'Alice sans connaître le résultat de `bezout(71,2023)`.

Exercice 3 : (3 points) Chiffrement El Gamal Bob choisit un entier premier $p = 17$ et un générateur $\alpha = 3$ du groupe multiplicatif $\mathbb{Z}_p^*$. Il choisit l'entier $k = 6$ pour clef privée.

1. Calculez β afin que Bob diffuse sa clef publique (p, α, β).

2. Alice envoie le chiffré $C = (4, 8)$ à Bob. Il faut aider Bob à déchiffrer ce message. Commencez par calculer l'inverse de c_1^k modulo p :

3. Déchiffrez enfin le chiffré C d'Alice.

Exercice 4 : (3 points) Signature DSA Considérons le jeu de paramètres DSA où la clef publique d'Alice est $(p, q, \alpha, \beta) = (59, 29, 3, 4)$, sa clef privée $k = 7$ et l'entier aléatoire qu'elle a choisi pour signer est $r = 10$. Elle envoie à Bob le message $M = 11$ assorti de sa signature $(\gamma, \delta) = (20, 18)$. Décrivez les calculs effectués par Alice.

1. Comment Alice a-t-elle calculé β ?

2. Comment Alice a-t-elle calculé γ ?

3. Comment Alice a-t-elle calculé δ ?

Exercice 5 : (2 points) LFSR Un tel *registre à décalage linéaire* se représente sous la forme d'un polynôme $\Pi(X) = X^k - a_1 X^{k-1} - ... - a_k$ et permet d'engendrer des bits de façon pseudo-aléatoire. Considérons le LFSR suivant :

$$\Pi(X) = X^5 - X^3 - X^2 - X - 1$$

Calculez les 5 bits suivants produits par le LFSR sur les valeurs initiales $(x_0, x_1, x_2, x_3, x_4) = (1, 1, 0, 0, 1)$.

Exercice 6 : (4 points) Questions de cours

1. Qu'est-ce qu'une fonction de hachage ? Quelles sont les qualités recherchées pour les fonctions de hachage en général et aussi pour les fonctions de hachage cryptographiques en particulier ?

2. Expliquez précisément en quoi le chiffrement utilisé par la messagerie sécurisée `pgp` est *hybride* ?

3. Citez tous les algorithmes ou protocoles cryptographiques vulnérables à l'attaque *Man In The Middle*.

4. Selon le *Paradoxe des anniversaires*, combien faut-il réunir de personnes pour avoir plus d'une chance sur deux ($p \geq 1/2$) que deux personnes aient les mêmes initiales ? *(on considère qu'il y a 26 lettres et 2 initiales par personne ordonnées selon les nom et prénom)*.