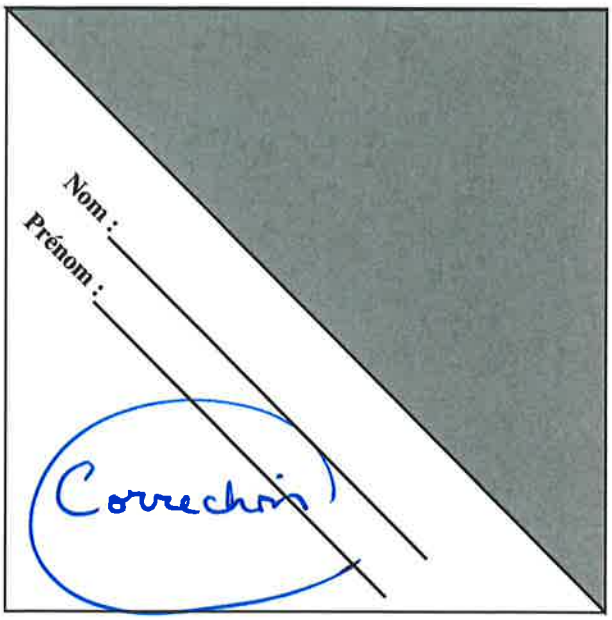
Université Côte d'Azur 2023–2024
Licence 3 Info, L3 Math-Info, L3 Sc. & Techn.

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 ?

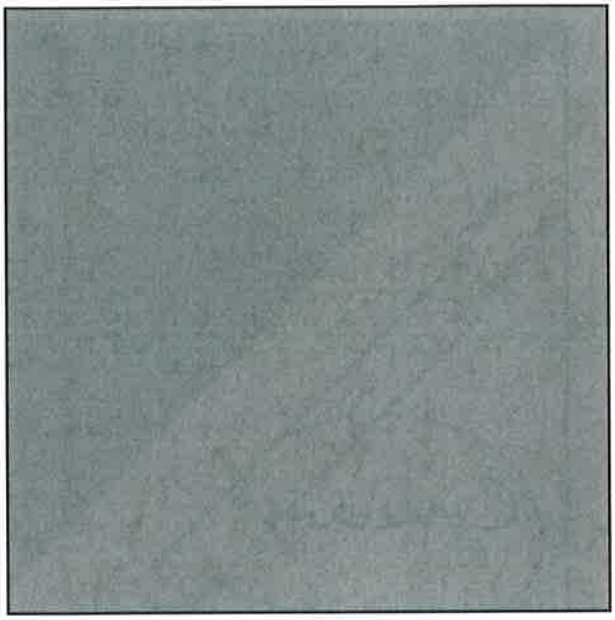
   Sur le pb du logarithme discret
   Il est dans NP ∩ co-NP

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 ?

   D'une part, on ne peut pas choisir la taille de la clef. D'autre part, on préfère que les clefs soient aléatoires.

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.

   a a été choisi par Alice, b par Bob
   $g^a \bmod p = 4$ donc $a = 2$
   $g^b \bmod p = 7$
   puissances de g mod p :
   [1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7]
   donc $b = 11$
   Le secret s : $g^{ab} \bmod p = 10$



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 ?

$d \equiv e^{-1} \bmod m \equiv -118 \bmod 2023 = 1905$

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

`B = [(e * a) % m for a in A]`

$B = [740, 600, 1080, 497, 1354, 222, 1524, 1402, 232]$

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

$C_1 = 600 + 1080 + 497 + 1354 + 1524 + 1402$

$C_1 = 5960$

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.

$S = (C_1 \times d) \bmod m = 579$

on exécute `linear_subset_sum(A, S)` :

$946 > S$ donc $n_2[8] = 0$

$450 \leq S$ donc $n_2[7] = 1$ $S \leftarrow -450 + 579 = 129$

$215 > S$ donc $n_2[6] = 0$

$103 \leq S$ donc $n_2[5] = 1$ $S \leftarrow 129 - 103 = 26$

$45 > S$ donc $n_2[4] = 0$

$21 \leq S$ donc $n_2[3] = 1$ $S \leftarrow 26 - 21 = 5$

$9 > 5$ donc $n_2[2] = 0$, $n_2[1] = 1$ et $n_2[0] = 0$

$n_2 = 010101010$.

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

$2023 = 7 \times 17^2$ donc $\varphi(2023) = 6 \times 16 \times 17 = 1632$

$d \equiv e^{-1} \bmod m \equiv e^{\varphi(m)-1} \bmod m$

$d \equiv e^{1631} \bmod m = 1905$.

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.

$n_A = 5 \times 13$ $\varphi(n_A) = 4 \times 12 = 48$

$n_B = 7 \times 11$ $\varphi(n_B) = 6 \times 10 = 60$

$e_A d_A \equiv 1 \mod 48$ or $1 = 5 \cdot 29 - 3 \cdot 48$ donc $d_A = 5$

$e_B d_B \equiv 1 \mod 60$ or $1 = 7 \times 43 - 5 \times 60$ donc $d_B = 7$

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

$z = C^{d_A} \mod n_A = 50^5 \mod 65 = 20$

donc $(C, z) = (50, 20)$

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

on vérifie avec la clef pub. d'Alice e_A :

$C \stackrel{?}{=} z^{e_A} \mod n_A$? $20^{29} \mod 65 = 50 \rightarrow$ s'g. valide

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

$M = C^{d_B} \mod n_B = 50^7 \mod 77 = 8$

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.

p premier et α générateur de $\mathbb{Z}_p^*$

$\beta = \alpha^k \mod p$ avec k clef privée avec $k < p$

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) ?

$c_1 = \alpha^r \mod p$ pour un entier r aléatoire

$c_2 = M \cdot \beta^r \mod p$

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

$M = c_2 \times c_1^{-k} \mod p$ avec $k = 9$

$c_1^k \mod p = 11^9 \mod 23 = 19$

on cherche $(19, 23) = (-5, +5, 1)$ donc $c_1^{-k} = -6 = 17$

d'où $M = (18 \times (-6)) \mod 23$

$M = 7$.

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

Grâce au choix de l'entier r aléatoire, le chiffrement de 2 messages identiques diffèrent.

Inconvénient : la lg du chiffré est le double de celle du message.

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 ?

$\beta = \alpha^k \bmod p = 3^7 \bmod 83 = 29$

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.

$\gamma = (\alpha^r \bmod p) \bmod q$

$\gamma = 11.$

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

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

$r^{-1} \bmod q = 3$ car bezout$(14, 41) = (1, 3, -1)$

$\delta = ((33 + (7 \times 11)) \,.\, 3) \bmod 41 = 2.$

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.

4. cours

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

4. cours

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 (a,1,0)
    q = a//b
    r = a%b
    (g,u,v) = bezout(b,r)
    return g, v, u-q*v
```