Corrigé

SR 5 ppa - Cryptographie - DST

Nom : _____

Prénom : _____

- Durée : 1 heure 30. Documents interdits, calculatrices interdites.
- Écrivez toutes les réponses directement sur le sujet. Si vous n'avez pas suffisamment de place, écrivez au dos d'une feuille en le **précisant dans la question**.

1 Question de cours (8 points)

1. [1 point] Comment ssh permet-il d'obtenir une communication à la fois rapide et sécurisée ?

   Solution: La clé de chiffrement symétrique est chiffrée avec un protocole asymétrique.

2. [1 point] Qu'est-ce que la stéganographie ? Quel exigence en matière de sécurité ce principe ne satisfait-il pas ?

   Solution: La stéganographie est l'art de dissimuler les informations. Cette méthode viole le fait que le message doit pouvoir tomber entre les mains d'un tiers non autorisé sans qu'il puisse être déchiffré.

3. [1 point] Quel est le principal problème de sécurité que posent les méthodes de chiffrement symétrique à clé ?

   Solution: Le problème de l'échange des clés.

4. [1 point] Lorsque je reçois un message, dois-je le déchiffrer avec ma clé publique ou ma clé privée ?

   Solution: Avec ma clé privée.

5. [1 point] Qu'est-ce qu'un nombre premier ? Précisez l'éventuel cas particulier.

Solution: p est premiers si les seuls diviseurs entiers positifs de p sont 1 et p. Par convention, 1 n'est pas premier.

6. [1 point] Qu'est-ce que deux nombres premiers entre eux ? Soyez précis.

Solution: Deux nombres sont premiers entre eux si leur *pgcd* est 1.

7. [1 point] Rappelez la définition de la division dans Z.

Solution: On divise a par b en définissant q et r tels que $a = bq + r$ et $0 \leq q < b$.

8. [1 point] Quelle est l'utilité de bibliothèques comme GMP

Solution: On manipule en cryptographie des nombres de plusieurs centaines de chiffres, il est impossible de les représenter avec des variables de types primitifs. Les bibliothèques comme GMP permettent de représenter en mémoires des nombres d'une précision arbitrairement grande.

2 Arithmétique (12 points)

1. [2 points] Démontrez que si $a|b$ et $b|c$, alors $a|c$

   Solution: Si $a|b$ et $b|c$, alors il existe k et k' tels que $b = ak$ et $c = bk'$. Comme $c = bk' = akk'$, alors $a|c$.

2. [2 points] Donnez dans l'ordre croissant, la liste des diviseurs positifs de 375

Diviseurs de 375

   Solution: Comme $375 = 5 \times 7 \times 11$ la liste des diviseurs est

Diviseurs de 375
$5^0 \times 7^0 \times 11^0 = 1$
$5^1 \times 7^0 \times 11^0 = 5$
$5^0 \times 7^1 \times 11^0 = 7$
$5^0 \times 7^0 \times 11^1 = 11$
$5^1 \times 7^1 \times 11^0 = 35$
$5^1 \times 7^0 \times 11^1 = 55$
$5^0 \times 7^1 \times 11^1 = 77$
$5^1 \times 7^1 \times 11^1 = 375$

3. [3 points] Effectuez les divisions suivantes :

a	b	q	r
41	8		
-10	3		
0	2		
-7	1		
-2	2		
-11	4		

Solution:

a	b	q	r
41	8	5	1
-10	3	-4	2
0	2	0	0
-7	1	-7	0
-2	2	-1	0
-11	4	$-4-$	1

4. [3 points] Donner les *pgcd* des couples de nombres suivants.

a	b	$pgcd(a, b)$
3	8	
49	35	
0	134	
44	52	
1	1022	
55	77	

Solution:

a	b	$pgcd(a, b)$
3	8	1
49	35	7
0	134	134
44	52	4
1	1022	1
55	77	11

5. [2 points] Donner, dans l'ordre croissant, tous les nombres compris entre 1 et 21 qui sont premiers avec 21.

Nombres premiers avec 21

Solution:

Nombres premiers avec 21
1
2
4
5
8
10
11
13
16
17
19
20