Composition de Crypto

La composition est composée de plusieurs exercices

Le support de cours est permis. La majeure partie des questions font appel au sens pratique.

1. Scytale

Pour cet exercice il est recommandé de faire un dessin pour arriver aux diverses réponses.

a) Rappeler le fonctionnement d'un scytale (4 lignes) ?
b) Une bande chiffrée par un scytale a été interceptée. Elle contient n caractères non séparés par des blancs. Elle a une une longueur l. La hauteur moyenne d'un caractère est de c. On va supposer que l'enroulement de la bande autour du scytale n'introduit pas de perte de taille. Soit d le diamètre du scytale :
   - Quel est le type d'algorithme de base qu'offre le scytale(permutation, transposition, substitution) ?
   - En supposant que le message chiffré intercepté est du français quel est son indice de coïncidence supposé ?
   - Ecrire les équations de d en fonction de c, l en fonction de d, n et c. Quelle est la hauteur maximale h du scytale pour la bande interceptée?
   - Transformer l'utilisation cylindrique du scytale en utilisation linéaire.
   - Comment décrypter le message intercepté ?

2. Mise en séquestre de la clé privée d'une autorité

a) Rappeler le besoin de mise en séquestre d'une clé privée d'autorité. (5 lignes maximum)

Schéma de Shamir

Soit à diviser certaines données *D* en n pièces $D_1, \ldots, D_n$ de telle sorte que:

- la connaissance de *k* ou plus D_i pièces rend *D* facilement calculable.
- la connaissance de *k-1* ou moins D_i pièces rend *D* complètement indéterminée.

Ce régime est appelé schéma **à seuil** *(k ;n)* . Si k = n alors tous les participants sont nécessaires pour restituer le secret.

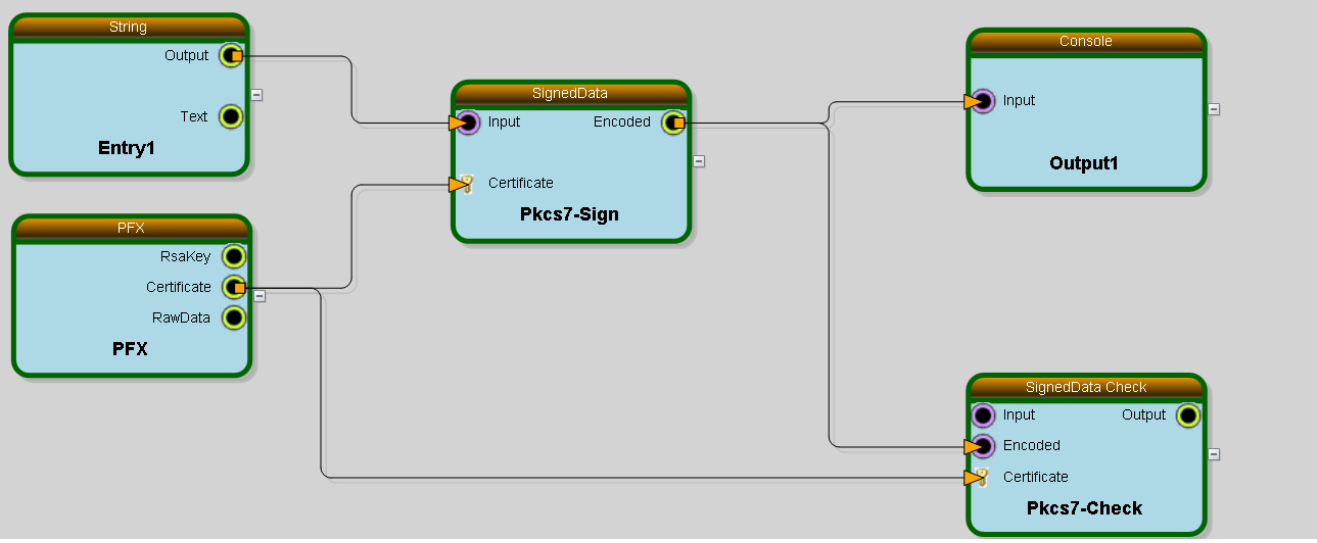
b) Soit le polynôme créé par l'autorité $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_{k-1}x^{k-1}$, combien de points (i, f(i)) sont-ils nécessaires pour obtenir les divers coefficients du polynôme?
c) En supposant qu'à chaque destinataire i d'une pièce D_i on affecte un numéro i et un point (i, f(i)) quelle est la relation entre Di et f(i) ?
d) En supposant que D = a_0 et que les autres coefficients sont générés d'une façon aléatoire, et à partir de la question c imaginer la méthode de mise en séquestre d'une clé privée ainsi que sa restitution à partir de k pièces.
e) Soit n le nombre de participants qui reçoivent une partie du secret, est ce que le nombre de participants peut évoluer?
f) Discuter de l'utilité du point précédent. (3 lignes)
g) Est-ce que le polynôme peut être changé sans changer le secret ?
h) discuter de l'utilité du point précédent. (3 lignes)
i) Est-ce qu'un participant peut recevoir plus qu'une pièce ?
j) discuter de l'utilité du point précédent. (3 lignes)

Schéma XOR

Soit Ri un nombre aléatoire ayant la taille de la clé privée S , avec 0 ≤ i ≤ k-2.
Supposons que R_{k-1} = S XOR R_0 XOR R_1 .. XOR R_{k-2}.

k) Les différents Ri 0 ≤ i ≤ k-1 sont distribués à k participants. Comment obtenir S à partir des différents Ri ?
l) Quel est le seuil de ce schéma (voir la définition au début de l'exercice).
m) Comparer ce schéma par rapport aux points e, g et i du schéma de Shamir.

3. **PKCS7 et DER**



SignedData désigne la fonctionnalité Signature PKCS7.
SignedData-Check désigne la fonctionnalité de Vérification de Signature PKCS7.
Les entrées/sorties Certificate désignent un handle (ou contexte) d'un certificat avec ou sans clé privée.

a) Lors du lancement de ce schéma, le programme demande un mot de passe. Parmi les 5 blocs, lequel est à l'origine de cette demande et pourquoi ?
b) Quelle partie du standard PKCS définit le bloc intitulé PFX ?
c) La valeur RawData (données brutes) du certificat est la suivante :

```
30 82 05 46 30 82 03 2E A0 03 02 01 02 02 08 0E A4 09 60 00 00 00 07 30 0D 06 09 2A 86 48 86 F7
0D 01 01 05 05 00 30 69 31 0B 30 09 06 03 55 04 06 13 02 46 52 31 13 30 11 06 03 55 04 07 13 0A
43 6F 75 72 62 65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13 06 45 41 53 45 49 54 31 15 30 13 06
03 55 04 0B 13 0C 43 52 59 50 54 4F 43 45 4E 54 45 52 31 1D 30 1B 06 03 55 04 03 13 14 45 41 53
45 49 54 20 52 4F 4F 54 20 4B 45 59 20 34 30 39 36 30 1E 17 0D 30 39 30 31 30 38 31 38 32 39 31
38 5A 17 0D 31 31 31 30 32 39 31 38 32 39 31 38 5A 30 70 31 0B 30 09 06 03 55 04 06 13 02 46 52
31 13 30 11 06 03 55 04 07 13 0A 43 6F 75 72 62 65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13 06
45 41 53 45 49 54 31 1A 30 18 06 03 55 04 03 13 11 45 2E 41 4F 55 41 44 20 53 69 67 6E 61 74 75
72 65 31 1F 30 1D 06 09 2A 86 48 86 F7 0D 01 09 01 16 10 65 61 6F 75 61 64 40 65 61 73 65 69 74
2E 66 72 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02
82 01 01 00 DF 33 67 A7 1E 88 CE FD EB 3C 0C FC 30 D5 B0 D2 ED 3D 5E 5D 47 81 89 22 48 64 92 19
E2 F0 22 AB 82 37 23 60 32 9B D0 BD 1F 09 8A 5F A4 D1 C6 77 DD 10 C9 A8 28 B9 76 DC 01 88 AF F8
DD 9B 37 22 BD 70 76 ED 1D CF A2 7C 48 90 79 01 CB 31 22 03 83 68 71 D4 47 C7 84 AF AD 61 13 22
F8 A2 56 BA 0D 78 77 E6 6B C4 AE CC 1D 83 50 E2 10 B6 B4 D4 83 33 55 79 A2 EC B6 D3 BF C6 AB CA
48 E2 2C C3 56 CA DB B3 73 50 E1 35 E7 E8 89 DD 1E 90 F2 09 29 A5 4A 46 72 2B BD CF C2 38 0C C1
82 7E 45 FB 0E 89 4E F5 AE 23 9B B3 39 3A 3A 67 F9 26 AF 04 D2 D6 34 6E AF 12 1A C4 75 10 32 E2
79 C1 38 9A CF A0 55 08 9E 94 FE 57 E0 DD 32 89 42 72 89 D0 47 CC 1E 02 EC BD 9C 7F 72 E6 CB 58
2B 62 53 F9 B5 60 D5 87 0C 56 02 76 5D F4 A9 C3 9F 4C D5 C0 03 FC 63 65 7F 76 C1 B1 11 4D A2 C5
91 66 FC E1 02 03 01 00 01 A3 81 EA 30 81 E7 30 09 06 03 55 1D 13 04 02 30 00 30 11 06 09 60 86
48 01 86 F8 42 01 01 04 04 03 02 07 80 30 0B 06 03 55 1D 0F 04 04 03 02 06 C0 30 1D 06 03 55 1D
0E 04 16 04 14 EC 15 E6 C8 A0 D9 07 72 01 D4 1A 91 0F B9 81 DE 8E FF 60 D6 30 81 9A 06 03 55 1D
23 04 81 92 30 81 8F 80 14 E0 49 B9 A5 6D 94 31 CE 5D D6 2E 9A 6C CC F4 34 BD DD 9B 35 A1 6D A4
6B 30 69 31 0B 30 09 06 03 55 04 06 13 02 46 52 31 13 30 11 06 03 55 04 07 13 0A 43 6F 75 72 62
65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13 06 45 41 53 45 49 54 31 15 30 13 06 03 55 04 0B 13
0C 43 52 59 50 54 4F 43 45 4E 54 45 52 31 1D 30 1B 06 03 55 04 03 13 14 45 41 53 45 49 54 20 52
4F 4F 54 20 4B 45 59 20 34 30 39 36 82 08 0E A4 09 60 00 00 00 01 30 0D 06 09 2A 86 48 86 F7 0D
01 01 05 05 00 03 82 02 01 00 A1 35 5D 6C 2B 9B A0 FC 21 73 B1 7A 5E D0 63 02 FB 74 68 87 11 73
2C DA D9 A1 4F C6 C2 BB C4 57 20 D0 22 E0 B3 6B C9 81 84 E2 70 AB 01 93 3D D1 44 88 88 FB 63 13
D7 07 A8 F2 1E 0F 3E E8 DE 54 57 E0 3C 48 39 A5 D5 E3 42 15 F6 CB 53 C4 41 78 B2 10 3A 77 EC 44
93 69 0C A9 59 FD 72 1B 17 CE D5 0B 25 7F 7B E0 43 39 28 44 7D 3E F0 C1 E0 4A 98 A9 10 A9 EF 6B
27 28 04 4E A8 E9 99 73 30 27 08 E6 53 D0 31 4A EF A4 D8 CD FD D4 B1 2E 2A 7D 90 B1 F5 AF 01 02
16 00 3E 10 BC 40 5E 52 54 F0 4D 94 09 D4 AB 23 92 6F DD 8D 69 66 95 F7 EF 2F 02 D7 AC E2 AF C1
2E 93 33 88 62 DF E6 6D 18 F0 4F 98 75 5E D1 03 85 01 8A 7B 2F 4D AC A3 12 B4 D8 D3 33 00 15 BE
E2 37 AB 5D 77 9C 0A 74 FE FD 09 A3 3E 68 6B 2D C9 9F E7 3A 8A 25 C1 D8 08 9F F2 B1 4F 63 F3 EA
9F F5 1E F0 06 1E 5C 9D 9A D8 90 F0 9A EF D2 DB 57 94 F5 14 CA 59 FC 0E D5 9B FE 65 5A D8 57 4A
2A 46 21 58 AE 4A 7C 9D CE 87 C5 BE FD E5 3C FA 5A 84 DA CE 99 07 A1 75 C0 E9 78 20 72 D2 8C 4F
1F EF 62 40 57 6B 87 87 B0 55 0D E3 09 B8 88 E9 30 F9 F5 8A 2B DE 3D 30 E4 F2 6A EE 5B 4A 61 93
BC 7F 81 16 AA DF 42 67 46 CF 7B 2A BC 6C BD 90 2A 6A 49 FC 12 54 77 7E 5B 1E 90 1A 0E DA 25 24
46 6B 5E D2 EA 3A 62 A7 A1 D0 13 B4 07 27 F2 C8 5A 65 8B FC AF F0 9C 99 BD 44 83 9D 5E 80 19 F8
C6 15 B8 D0 A5 48 93 98 0C B1 06 A9 71 C8 F7 11 E5 F2 CF 4B 83 F6 8F 8C 6A F3 7F 72 EC A3 C1 0A
0A CE C5 26 FC 94 7C 18 83 35 12 9B C6 C7 E9 10 01 75 BB 96 8D B1 99 6D C0 D7 06 16 B0 73 02 46
6E B7 62 2D 48 2B 25 77 54 2F 2B 82 C9 8B D4 D6 A0 86 3F 36 D1 2D BA B5 10 BD 38 DC 04 EA F4 7E
```

D2 FF A8 59 67 34 3F CC BB 16

d) Sans compter les octets définir la taille totale du certificat.
e) Le certificat est émis par une autorité utilisant une clé RSA de 4096 bits. Définir les deux premiers octets et les deux derniers octets de la signature.

f) La sortie Encoded suivante de SignedData correspond à la valeur binaire PKCS7 SignedData en signature jointe.

```
30 82 07 2B 06 09 2A 86 48 86 F7 0D 01 07 02 A0 82 07 1C 30 82 07 18 02 01 01 31 0F 30 0D 06 09
60 86 48 01 65 03 04 02 01 05 00 30 10 06 09 2A 86 48 86 F7 0D 01 07 01 A0 03 04 01 30 A0 82 05
4A 30 82 05 46 30 82 03 2E A0 03 02 01 02 02 08 0E A4 09 60 00 00 00 07 30 0D 06 09 2A 86 48 86
F7 0D 01 01 05 05 00 30 69 31 0B 30 09 06 03 55 04 06 13 02 46 52 31 13 30 11 06 03 55 04 07 13
0A 43 6F 75 72 62 65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13 06 45 41 53 45 49 54 31 15 30 13
06 03 55 04 0B 13 0C 43 52 59 50 54 4F 43 45 4E 54 45 52 31 1D 30 1B 06 03 55 04 03 13 14 45 41
53 45 49 54 20 52 4F 4F 54 20 4B 45 59 20 34 30 39 36 30 1E 17 0D 30 39 30 31 30 38 31 38 32 39
31 38 5A 17 0D 31 31 31 30 32 39 31 38 32 39 31 38 5A 30 70 31 0B 30 09 06 03 55 04 06 13 02 46
52 31 13 30 11 06 03 55 04 07 13 0A 43 6F 75 72 62 65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13
06 45 41 53 45 49 54 31 1A 30 18 06 03 55 04 03 13 11 45 2E 41 4F 55 41 44 20 53 69 67 6E 61 74
75 72 65 31 1F 30 1D 06 09 2A 86 48 86 F7 0D 01 09 01 16 10 65 61 6F 75 61 64 40 65 61 73 65 69
74 2E 66 72 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A
02 82 01 01 00 DF 33 67 A7 1E 88 CE FD EB 3C 0C FC 30 D5 B0 D2 ED 3D 5E 5D 47 81 89 22 48 64 92
19 E2 F0 22 AB 82 37 23 60 32 9B D0 BD 1F 09 8A 5F A4 D1 C6 77 DD 10 C9 A8 28 B9 76 DC 01 88 AF
F8 DD 9B 37 22 BD 70 76 ED 1D CF A2 7C 48 90 79 01 CB 31 22 03 83 68 71 D4 47 C7 84 AF AD 61 13
22 F8 A2 56 BA 0D 78 77 E6 6B C4 AE CC 1D 83 50 E2 10 B6 B4 D4 83 33 55 79 A2 EC B6 D3 BF C6 AB
CA 48 E2 2C C3 56 CA DB B3 73 50 E1 35 E7 E8 89 DD 1E 90 F2 09 29 A5 4A 46 72 2B BD CF C2 38 0C
C1 82 7E 45 FB 0E 89 4E F5 AE 23 9B B3 39 3A 3A 67 F9 26 AF 04 D2 D6 34 6E AF 12 1A C4 75 10 32
E2 79 C1 38 9A CF A0 55 08 9E 94 FE 57 E0 DD 32 89 42 72 89 D0 47 CC 1E 02 EC BD 9C 7F 72 E6 CB
58 2B 62 53 F9 B5 60 D5 87 0C 56 02 76 5D F4 A9 C3 9F 4C D5 C0 03 FC 63 65 7F 76 C1 B1 11 4D A2
C5 91 66 FC E1 02 03 01 00 01 A3 81 EA 30 81 E7 30 09 06 03 55 1D 13 04 02 30 00 30 11 06 09 60
86 48 01 86 F8 42 01 01 04 04 03 02 07 80 30 0B 06 03 55 1D 0F 04 04 03 02 06 C0 30 1D 06 03 55
1D 0E 04 16 04 14 EC 15 E6 C8 A0 D9 07 72 01 D4 1A 91 0F B9 81 DE 8E FF 60 D6 30 81 9A 06 03 55
1D 23 04 81 92 30 81 8F 80 14 E0 49 B9 A5 6D 94 31 CE 5D D6 2E 9A 6C CC F4 34 BD DD 9B 35 A1 6D
A4 6B 30 69 31 0B 30 09 06 03 55 04 06 13 02 46 52 31 13 30 11 06 03 55 04 07 13 0A 43 6F 75 72
62 65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13 06 45 41 53 45 49 54 31 15 30 13 06 03 55 04 0B
13 0C 43 52 59 50 54 4F 43 45 4E 54 45 52 31 1D 30 1B 06 03 55 04 03 13 14 45 41 53 45 49 54 20
52 4F 4F 54 20 4B 45 59 20 34 30 39 36 82 08 0E A4 09 60 00 00 00 01 30 0D 06 09 2A 86 48 86 F7
0D 01 01 05 05 00 03 82 02 01 00 A1 35 5D 6C 2B 9B A0 FC 21 73 B1 7A 5E D0 63 02 FB 74 68 87 11
73 2C DA D9 A1 4F C6 C2 BB C4 57 20 D0 22 E0 B3 6B C9 81 84 E2 70 AB 01 93 3D D1 44 88 88 FB 63
13 D7 07 A8 F2 1E 0F 3E E8 DE 54 57 E0 3C 48 39 A5 D5 E3 42 15 F6 CB 53 C4 41 78 B2 10 3A 77 EC
44 93 69 0C A9 59 FD 72 1B 17 CE D5 0B 25 7F 7B E0 43 39 28 44 7D 3E F0 C1 E0 4A 98 A9 10 A9 EF
6B 27 28 04 4E A8 E9 99 73 30 27 08 E6 53 D0 31 4A EF A4 D8 CD FD D4 B1 2E 2A 7D 90 B1 F5 AF 01
02 16 00 3E 10 BC 40 5E 52 54 F0 4D 94 09 D4 AB 23 92 6F DD 8D 69 66 95 F7 EF 2F 02 D7 AC E2 AF
C1 2E 93 33 88 62 DF E6 6D 18 F0 4F 98 75 5E D1 03 85 01 8A 7B 2F 4D AC A3 12 B4 D8 D3 33 00 15
BE E2 37 AB 5D 77 9C 0A 74 FE FD 09 A3 3E 68 6B 2D C9 9F E7 3A 8A 25 C1 D8 08 9F F2 B1 4F 63 F3
EA 9F F5 1E F0 06 1E 5C 9D 9A D8 90 F0 9A EF D2 DB 57 94 F5 14 CA 59 FC 0E D5 9B FE 65 5A D8 57
4A 2A 46 21 58 AE 4A 7C 9D CE 87 C5 BE FD E5 3C FA 5A 84 DA CE 99 07 A1 75 C0 E9 78 20 72 D2 8C
4F 1F EF 62 40 57 6B 87 87 B0 55 0D E3 09 B8 88 E9 30 F9 F5 8A 2B DE 3D 30 E4 F2 6A EE 5B 4A 61
93 BC 7F 81 16 AA DF 42 67 46 CF 7B 2A BC 6C BD 90 2A 6A 49 FC 12 54 77 7E 5B 1E 90 1A 0E DA 25
24 46 6B 5E D2 EA 3A 62 A7 A1 D0 13 B4 07 27 F2 C8 5A 65 8B FC AF F0 9C 99 BD 44 83 9D 5E 80 19
F8 C6 15 B8 D0 A5 48 93 98 0C B1 06 A9 71 C8 F7 11 E5 F2 CF 4B 83 F6 8F 8C 6A F3 7F 72 EC A3 C1
0A 0A CE C5 26 FC 94 7C 18 83 35 12 9B C6 C7 E9 10 01 75 BB 96 8D B1 99 6D C0 D7 06 16 B0 73 02
46 6E B7 62 2D 48 2B 25 77 54 2F 2B 82 C9 8B D4 D6 A0 86 3F 36 D1 2D BA B5 10 BD 38 DC 04 EA F4
7E D2 FF A8 59 67 34 3F CC BB 16 31 82 01 A0 30 82 01 9C 02 01 01 30 75 30 69 31 0B 30 09 06 03
55 04 06 13 02 46 52 31 13 30 11 06 03 55 04 07 13 0A 43 6F 75 72 62 65 76 6F 69 65 31 0F 30 0D
06 03 55 04 0A 13 06 45 41 53 45 49 54 31 15 30 13 06 03 55 04 0B 13 0C 43 52 59 50 54 4F 43 45
4E 54 45 52 31 1D 30 1B 06 03 55 04 03 13 14 45 41 53 45 49 54 20 52 4F 4F 54 20 4B 45 59 20 34
30 39 36 02 08 0E A4 09 60 00 00 00 07 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 30 0D 06 09
2A 86 48 86 F7 0D 01 01 01 05 00 04 82 01 00 58 22 4A A2 DF 3A 3A A9 33 98 84 4B F8 F7 A3 E8 9B
F5 FB 44 36 E2 3C 9A D8 ED BC 00 1E 42 15 25 F5 9B 9D 5A 4F 0C 35 A3 31 13 70 1B A8 8B 8D D1 04
8D FF 2F E3 3D 98 33 B1 DE 59 E4 79 67 C4 F3 28 12 9C AE 1F 38 55 31 D0 0E F6 32 A0 AE 03 B6 5C
5F 11 59 9E 5F 18 3C 99 18 0E 78 D5 FA 24 8B 78 B1 49 A9 D5 18 34 D8 3F A9 90 5D C3 55 98 DC 9B
EB B9 0D F4 73 A6 9D 7F FE D7 55 91 10 01 60 09 10 F1 B3 2C 6D 95 1B 69 F7 8F CE 8E C3 12 AD 97
03 28 A9 07 61 6A 3D 7B D9 2C C9 66 04 9B C8 60 1B 96 37 27 A4 18 77 86 61 C4 84 07 59 29 E0 97
79 BF CC A6 71 CE 19 42 96 E3 DB 6A 53 D4 59 FF B7 82 54 C2 A2 B0 F4 D2 71 66 31 D6 A4 D4 22 12
70 18 AD AE 5B 75 1B F8 C6 7E 44 48 57 32 D0 7C BC ED 2B 0A 02 74 AB 7B 58 B5 27 CB F6 4D 5D F0
50 AE 9B 25 8E 10 16 AE 28 D9 25 2A 36 88 ED
```

- Quelle est la valeur de Output de Pkcs7-Check ?
- Pourquoi la liaison Certificate de PFX avec Certificate de Pkcs7-Check est inutile ?
- Si la signature PKCS7 est disjointe comment faut-il compléter le schéma ?
- Sachant que le champ Certificates est optionnel dans Pkcs7-SignedData, comment la signature peut être vérifiée ?

4. **Obtention de p et q à partir d'une clé privée RSA**

Les notations suivantes sont utilisées : $N = p * q$, et $S*P = 1 \bmod (p-1)(q-1)$
On va supposer que les valeurs S,N,P sont connues et que le but est de calculer p et q pour obtenir les composantes du théorème du reste chinois.

a) Ecrire S*P sous la forme de k * a + 1
b) A partir de la formule suivante et considérant que p, q et 1 sont négligeables par rapport à N, calculer k.
c) Définir p + q .
d) Sachant que p*q et p+q sont maintenant connus, déduire leur valeur de p et q en mettant l'équation qui les lie mais sans la résoudre.