Université Côte d'Azur — L3 Info, L3 MI, L3 ST
Cryptographie et calcul symbolique — 2023-24

TD n° 5

Cryptographie à clef publique (suite)

Problème de la somme des sous-ensembles

Exercice 1) Ce problème est NP-complet. Il existe toutefois un algorithme pour le résoudre dans le cas d'un nombre d'entiers restreint. On rappelle cet algorithme donné en cours :

```
def subsetSum(L,k):
    if k == 0 :  return True
    for i in range(len(L)):
        if subsetSum (L[:i]+L[i+1:],k-L[i]):
            print(L[i])
            return True
    return False
```

Appliquez l'algorithme `subsetSum()` afin de résoudre ce problème avec la suite L dans les deux cas suivants :

$$L = [225, 53, 141, 77, 365, 99, 2023]$$

1. pour l'entier $k = 658$;
2. pour l'entier $k' = 987$.

Exercice 2) On peut trouver une solution au problème de la somme des sous-ensembles dès lors que la suite est *super-croissante*. On rappelle l'algorithme vu en cours et qui sera utilisé en TP :

```
def linearSubsetSum (L,k):   #  que si L est super-croissante !
    res = [] ;  s = k
    for i in range(len(L)-1,-1,-1) :
        if s >= L[i] :
            res.append(L[i])
            s = s - L[i]
    if s == 0 :
        return (res,k)
    else :
        return (False,k)
```

Vérifiez que la suite suivante est super-croissante puis appliquez-lui cet algorithme dans les deux cas suivants :

$$L = [4, 15, 37, 83, 190, 387, 781, 1580]$$

1. pour l'entier $k = 1293$;
2. pour l'entier $k' = 2023$.

Chiffre de Merkle-Hellman

Exercice 3) 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. Calculez 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.

Exercice 4) Alice souhaite recevoir des messages chiffrés au moyen d'un cryptosystème de Merkle-Hellman. Elle publie pour cela sa clef publique :

$$B = (1510, 940, 1323, 1210, 836, 1115, 50)$$

1. Bob chiffre le message $M = 0101011$ pour Alice. Quel est le chiffré C correspondant ?
2. Alice a égaré une partie de ses paramètres privés ! Elle n'a plus que le module $m = 1832$ et l'entier $e = 557$, premier avec m. Pas de panique, elle sait qu'elle peut retrouver la suite super-croissante A qu'elle s'était choisie ...

   Commencez par retrouver la clef privée d d'Alice puis donnez une formule permettant de passer de la suite publique B à la suite super-croissante A et calculez-la (même si d'habitude, on fait plutôt l'inverse).
3. Aidez Alice à déchiffrer le message chiffré C envoyé par Bob.

Chiffre El Gamal

Exercice 5) Bob choisit un entier premier $p = 17$ et un générateur $\alpha = 3$ du groupe $(\mathbb{Z}_p^*, \times)$. 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 $C = (11, 16)$ à Bob. Il faut aider Bob à déchiffrer ce message. Commencez par calculer l'inverse de c_1^k modulo p.
3. Déchiffrez le chiffré C d'Alice sachant que le message initial $M = (c_2 \,.\, c_1^{-k}) \mod p$.

Exercice 6) Bob veut transmettre le message $M = 1299$ à Alice. Pour cela, il récupère la clef publique d'Alice : $(p, \alpha, \beta) = (2579, 2, 949)$.

1. Sachant que Bob choisit l'entier aléatoire $r = 853$, chiffrez le clair qu'il veut transmettre à Alice.
2. Etant donnée que la clef privée d'Alice (qui lui a notamment permis de calculer β) était $k = 765$, aidez Alice à déchiffrer le message reçu de Bob.

Mise en gage

Exercice 7) Jouer à pile ou face par téléphone Le protocole suivant est présenté de façon ludique mais est significatif de la puissance des fonctions à sens unique. Alice et Bob veulent jouer à pile ou face par téléphone, mais veulent s'assurer qu'il n'y aura pas de tricherie : celui qui *lance la pièce* ne doit pas pouvoir mentir sur le résultat obtenu.

On suppose pour cela que l'on dispose d'une fonction à sens unique bijective f de E dans F et d'une partition $E = E_0 \uplus E_1$. Trouvez un protocole en 4 étapes pour mimer le jeu de pile ou face à distance.