TP2: Sac à Dos; RSA

Mathieu Tuloup Mohamed Saidane

1 Sac à Dos : Chiffre de Merkle-Hellman

1. (a) Un sac à dos est dit facile si sa suite A est supercroissante c'est-à-dire que si pour n ≥ 1 on a : $\sum_{k=0}^{n-1} a_k < a_n$ en l'occurence la suite A est bien supercroissante
   (b) Le modulo N est acceptable si la somme de la suite A est strictement inférieur à N :$\sum_{k=0}^{n-1} a_k < N = 25646 < 25922$. Donc Le modulo est acceptable.
   (c) Pour vérifier si un compliqueur est acceptable on va regarder si E est premier avec le module N. Si c'est le cas E peut être le compliqueur.
   (d) Pour déterminer le Sac à dos difficile B, on a : $B_i = (A_i \times E)[N]$ avec E=10693 et N=25922 donc B=(9413,6596,11580,9500,15988)
   (e) La faciliteur $D = E^{-1}[N] = 20373$ avec N=25922
   (f) La clé publique de Bob est B=(9413,6596,11580,9500,15988) le sac à dos difficile et N=25922
   (g) Pour déchiffrer le message on va utiliser la clé privée, à savoir le sac à dos facile A ainsi que le faciliteur D.De plus on va utiliser l'algorithme glouton, à noter que A doit être supercroissante . On détermine C=$D \times 41577$. On applique l'algorithme glouton qui ici nous renvoie qu'il n'a pas de solution car $C \neq 0$
2. (a) La suite A est bien supercroissante donc c'est un sac à dos facile.
   (b) La somme de la suite A : :$\sum_{k=0}^{n-1} a_k = 103 < N = 105$. Le modulo N est acceptable.
   (c) Bob peut prendre le compliqueur E=31 car 31 est premier avec le modulo N=105.
   (d) B=(62,93,81,88,102,37)
   (e) $D = E^{-1}[N] = 61$
   (f) La clé publique de Bob est B=(62,93,81,88,102,37) le sac à dos difficile et N=105
   (g) Pour chiffré un message de n=18 bits $M = (m_1, ..., m_n)$, on calcul le cryptogramme. le message chiffré vaut 82.
   (h) Pour le message chiffré 262257139 : Il n'y a pas de solution avec algo glouton.
   (i) Pour le message chiffré 232680541 : Il n'y a pas de solution avec algo glouton.

2 Methode RSA et notations

2.1 Exercie 1

1. Alice doit faire M'= $C^D mod$ N = 204
2. p=17 et q=23 car $17 \times 23 = 391$ et p et q sont premiers. $\phi(N) = (p-1) \times (q-1) = 352$
3. $D = E^{-1} mod\ \phi$. On a trouvé l'inverse modulaire de E mod Φ grâce à l'algorithme d'Euclide étendu qui vaut 7 soit la valeur de D.

2.2 Exercice 2

1. (a) Pour chiffrer le message M il faut calculer le cryptogramme $C = M^E$ mod N= 122.
   (b) Le message déchiffré est 65.
2. (a) p $\times$ q = 3763. $\phi(N)$= 3640
   (b) E = 307< ϕ = 3640 et pgcd(E,ϕ)=1. Donc E est bien acceptable. E^{-1} mod N = D soit ici 83.
   (c) Clé publique : E = 307 et N = 3763. Clé privé : D = 35.
   (d) Il faut se débarrasser des éléments restants afin que nul ne puisse recréer notre clé privée car ce sont des éléménts qui ont permis de la définir.

2.3 Exercice 3

1. (a) Le cryptogramme de METHODE est : 859 ; 452
   (b) Le message du cryptogramme 256 ;115 ;613 ;10 est : CRYPTO
   (c) le cryptogramme de AVEZVOUSBIENREUSSI est : 32 ; 916 ; 546 ; 983 ; 403 ; 1001 ; 709 ; 857 ; 716 ; 1034 ; 567 ; 919
   (d) le message du cryptogramme 1019 ;35 ;567 ;36 ;384 ;703 ;99 ;59 est : SANSPROBLEME
   (e) Le message du cryptogramme 533 ;813 est : FIN