Sylvain Escassut
Nils Fradin

TP1 : RSA

Exercice 1 (RSA (12 points))

1. Le résultat du calcul de n est :
   n = p x q = 7 x 3 = 21
   Le résultat de phi(n) est :
   phi(n) = (p - 1) (q - 1) = (3 -1) (7 - 1) = 2 x 6 = 12

   Chiffrement de M = 2
   C = M^e mod n= 2^5 mod (21) = 11

   Déchiffrement de c = 3
   m = c^d mod n = 3^5 mod 21 = 12

2. Nous avons tout d'abord calculer le différentes variables indispensable au chiffrement d'un message. Pour travailler avec de grand nombre on a du utiliser le type de GMP qui est : mpz_t . Il a fallut calculer la clé publique et les clé privé.

Exercice 2 (Side channel (8 points))