Université de Tlemcen Année Universitaire 2020-2021 Faculté des Sciences Département Informatique	Module Sécurité Informatique L3

Méthode RSA

Exercice

Alice utilise le protocole RSA et publie sa clé publique N=187 et e=3

a) Encoder le message m=14 avec la clé publique d'Alice
b) En utilisant le fait que Ø(N)=160 trouver la clé privée d'Alice
c) Pour assurer l'authenticité des messages, Alice signe chaque note avec sa clé privée et chiffre le résultat avec la clé publique de Bob (253, 13).
Si Bob reçoit le message 20, alors quel le message clair envoyé par Alice ?

----------Corrigé----------

a) $C=m^e \bmod N$
$C=14^3 \bmod 187$
$C=126$

b) $e*d=1 \bmod Ø(N) \Rightarrow e*d+ k* Ø(N)=1$
$3*d+ k*160=1$
En appliquant la méthode de division euclidienne étendue entre 160 et 3 :
$160=3 * 53 +1 \rightarrow 1=160-53*3$

Donc $d=-53 =-53+160=107$

c) $M=(20^{dB} \bmod 253)^3 \bmod 187$
d_B est la clé privé de Bob
Bob déchiffre le message avec sa clé privée (le résultat est la signature d'Alice) ensuite déchiffre la signature avec la clé publique d'Alice pour trouver le message d'origine

Calcul de la clé privée de Bob
1- Factoriser le N=253 en produit de deux nombre premiers
N=253=23*11
2- Calculer Ø(N)= (23-1)*(11-1)=22*10=220
3- $e*d=1 \bmod Ø(N) \rightarrow e*d+k Ø(N) =1$
$13d+k220=1$
Appliquer la division euclidienne étendue entre 220 et 13:
$220=13*16+12 \rightarrow 12=220-13*16$
$13=12*1+1 \rightarrow 1=13-12*1 \rightarrow 1=13-(220-13*16)*1 \rightarrow 1=17*13-220$
$\rightarrow d=17$

d) $M=(20^{17} \bmod 253)^3 \bmod 187$

$M=191^3 \bmod 187=64$