UCBL – Mif 29 **Juin 2021**
Nom : Giraud
Prénom : Julien

CC rattrapage

(Durée 45 mins)

Toute réponse devra être justifiée. Vous enverrez par email (à gavin@univ-lyon1.fr avec TPMIF29 comme objet) le fichier réponse et vous le déposerez sur Tomuss.

Dans toute la suite, on supposera que Alice génére une paire de clés RSA R.pk=(n=pq,e) et R.sk=(d) et une paire de clés Paillier P.pk=(n) et P.sk =(ρ) (R.pk et P.pk ***partagent le même n****) de taille 2048 (n s'écrit avec 2048 bits).*

Parmi les affirmations suivantes, dire (en justifiant concisément votre réponse) celles qui sont vraies et celles qui sont fausses.

1 – Soit $M_0 \leftarrow$*Paillier.Encrypt (P.pk, 3)*. Si *Paillier.Decrypt (P.sk,* $3 \times M_0 \bmod n^2$*)=6* alors on peut affirmer que *Paillier.Decrypt (P.sk, 3)=3.*

Vraie.

2 – Soient $x_1,\ldots,x_m \in \mathbf{Z}/n\mathbf{Z}$ *et* $X_i \leftarrow$ *Paillier.Encrypt (P.pk,* x_i*)* pour tout i=1,…,m. Il existe un algorithme rapide qui prend en entrée *P.pk,* $X_1,\ldots,X_m$ et qui retourne *Y* tel que *Paillier.Decrypt (P.sk, Y)* $= x_1+\ldots+x_m \bmod n$.

Vrai grâce aux propriétés homomorphes de Paillier.

3 – Si *n* personnes veulent échanger de manière sécurisée en utilisant un cryptosystème à clé publique, *n(n-1)/2* paires de clés doivent être générées.

Faux, 2n sur un système à clé publique.

4 – La signature numérique est efficace contre les risques d'intrusion.

Vraie, la signature assure être infalsifiable.

5 – *Paillier.Decrypt(P.sk,* $X \times 2^n \bmod n^2$*) = Paillier.Decrypt(P.sk, X mod* n^2*).*

Faux.

6 - *Paillier.Decrypt(P.sk,* $(1+3n)^2 \bmod n^2$*)* = 9.

Faux, 6.

7 – Soient $x \in (\mathbf{Z}/n\mathbf{Z})^*$, $X \leftarrow$*RSA.Encrypt(R.pk,x)* et *Y*$\leftarrow$*Paillier.Encrypt(P.pk, X mod n).* On peut écrire que

RSA.Decrypt(R.sk, Paillier.Decrypt(P.sk,Y))=x

Vraie car *Paillier.Decrypt(P.sk,Y)=X et RSA.Decrypt(R.sk, X) = x.*

8 - Soient $x \in (\mathbf{Z}/n\mathbf{Z})^*$, $X \leftarrow$*Paillier.Encrypt(P.pk,x)* et *Y*$\leftarrow$*RSA.Encrypt(R.pk,X mod n).* On peut écrire que

Paillier.Decrypt(P.sk, RSA.Decrypt(R.sk,Y))=x

Faux car X est modulo n et Y est modulo n^2.

9 – Le couple de clés *(pk,sk)* avec *pk=(n=91,e=5)* et sk=*(d=29)* est un couple de clés valides RSA.
Vrai mais pas très sécurisé.