

MATHEMATIQUES POUR LA SECURITE INFORMATIQUE
FMSI

PARTIEL, EPITA_ING1_2019_S6
Juin 2017, Durée : 1h30 min

H. GROSCOT

Remarques : Les **notes de cours** ainsi que le **formulaire** sont autorisés.
Toutes les **calculatrices** sont autorisées.

Exercice 1 :

1.1 Trouver un entier **q** compris entre **1** et **112** tel que **$3q \equiv 1 \pmod{113}$** .

1.2 En déduire un nombre **a** compris entre **1** et **112** tel que **$3a \equiv 10 \pmod{113}$**

1.3 Existe-t-il un nombre **r** tel que **$7r \equiv 2 \pmod{105}$** ? On pourra commencer par factoriser le nombre 105.

Exercice 2 :

On admet que le nombre **p = 100 019** est premier.

On pose **a = 7**.

2.1 Calculer la classe de **p modulo 4**.

2.2 Un logiciel nous a permis de calculer

$$7^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Pouvez-vous citer le nom d'un algorithme vu en cours permettant d'effectuer ce calcul ?

Ce résultat est-il compatible avec le petit théorème de Fermat ?

2.3 On choisit **b** compris entre 1 et p-1 tel que :

$$b \equiv 7^{\frac{p+1}{4}} \pmod{p}.$$

Un logiciel nous donne une valeur numérique suivante sur **b** : 45 195.

Vérifier que **4** divise bien **p+1**, en utilisant l'une des questions précédentes et sans effectuer la division de **p+1** par **4**.

2.4 Calculer **b^2 modulo p**.

On suggère de partir de la définition donnée en 2.3 et d'utiliser le résultat de la question 2.2.
(Ne pas présenter le calcul direct sur la valeur de **b** dans la copie !!)

2.5 Donner, en fonction de **b**, les deux solutions comprises entre 1 et **p** de l'équation :

$$x^2 - a \equiv 0 \pmod{p}.$$

Exercice 3 :

Les deux nombres suivants sont très probablement premiers (admis) :

$$p = 79\,792\,266\,297\,612\,017$$

$$q = 95\,367\,431\,640\,673$$

Leur produit vaut :

$$n = 7\,609\,583\,501\,591\,890\,121\,708\,310\,767\,441$$

On pose :

$$f = (p-1)(q-1),$$

Ce qui donne la valeur numérique suivante :

$$f = 7\,609\,583\,501\,591\,810\,234\,074\,581\,514\,752.$$

On donne de plus les nombres suivants :

$$e = 14\,348\,909$$

$$d = 4\,921\,815\,319\,221\,531\,113\,545\,903\,926\,629$$

$$w = 9\,280\,755.$$

Ces nombres sont choisis de manière à respecter la relation suivante :

$$ed = wf + 1.$$

4.1 Combien de nombres compris entre 1 et **n** sont-ils premiers avec **n** ? On donnera ce nombre en fonction de l'un des nombres précédents sans en préciser la valeur numérique.

Alice doit envoyer à Bob un message **M** qu'elle souhaite signer électroniquement.

Pour cela, elle décide d'employer le RSA, où sa clé secrète est construite à partir de **p, q, d**. Bob connaît la clé publique d'Alice, constituée des deux nombres : **e, n**.

Par ailleurs, Alice et Bob se mettent d'accord pour employer une fonction de « hashage » permettant de déduire, à partir de **M**, un nombre **m** plus petit que **M**, compris entre **0** et **n-1**.

On a :

$$m = 5\,073\,055\,667\,727\,926\,747\,805\,540\,511\,627.$$

Après avoir utilisé le RSA, Alice envoie à Bob son message constitué :

- Du message **M**
- D'un élément complémentaire, un nombre **c**, où
 $c = 7\,308\,206\,559\,258\,727\,480\,535\,487\,920\,245.$

4.2 Quelle est la relation qui relie le nombre **c** aux autres nombres présentés dans l'énoncé, **n, e, d, m** ?

4.3 Quel sont les opérations et calculs que doit effectuer Bob pour vérifier l'authenticité du message ?

4.4 Le logarithme décimal de 2 vaut à peu près : **0,3**. Le nombre **n** donné plus haut vous semble-t-il satisfaisant pour une application industrielle ?