

**MATHEMATIQUES POUR LA SECURITE INFORMATIQUE
FMSI**

**PARTIEL, EPITA_2020_S6
Mars/Avril 2017, Durée : 1h30 min**

H. GROSCOT

NOM :

PRENOM :

Place n°

Remarques : Il est demandé de répondre simplement aux questions, dans les cases. Lorsque rien n'est précisé, une valeur numérique suffit. Lorsqu'on demande une formule, il suffit de la donner avec les valeurs de l'énoncé sans ajouter de notation complémentaire.

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

Exercice 1 :

Soit $n = 1463$. Ce nombre a été construit comme le produit de trois nombres premiers distincts p_1, p_2, p_3 , où $p_1 < p_2 < p_3 < 20$.

1.1 Quels sont les trois nombres p_1, p_2, p_3 ?

1.2 Quelle est la formule donnant $\varphi(n)$ en fonction de p_1, p_2, p_3 ?

1.3 Quelle est la valeur de $\varphi(n)$?

1.4 Le groupe $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition est cyclique. Combien de générateurs possède-t-il ?

Exercice 2 :

2.1 On pose $p = 21587$. Si une personne munie d'une calculatrice souhaite vérifier que p est premier comment fait-elle (une seule phrase) ?

2.2 On suppose que cette vérification a été faite (on ne vous le demande pas). Par ailleurs, $21587 = 2 \times 43 \times 251 + 1$, où 43 et 251 sont premiers.

2.3 Quelle est la nature de $\mathbb{Z}/p\mathbb{Z}$ muni de l'addition et de la multiplication ?

2.4 Le nombre d'éléments inversibles pour la multiplication de $\mathbb{Z}/p\mathbb{Z}$ vaut :

2.5 Le nombre de générateur du groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ vaut (une formule et la valeur numérique) :

On admet que $g = 2$ est un générateur de ce groupe multiplicatif.
On a effectué sur ordinateur les quelques calculs suivants :

$$g^{95} \equiv 4581 \pmod{p}, g^{96} \equiv 9162 \pmod{p}, g^{97} \equiv 18324 \pmod{p}, g^{98} \equiv 15061 \pmod{p}, \\ g^{99} \equiv 8535 \pmod{p}, g^{100} \equiv 17070 \pmod{p}, g^{196} \equiv 19112 \pmod{p}.$$

2.6 Existe-t-il un entier positif a inférieur à p tel que $a^2 \equiv 19112 \pmod{p}$? Justifier et donner sa valeur (uniquement des formules et la valeur, pas de rédaction).

2.7 Existe-t-il un autre entier positif b inférieur à p tel que $b^2 \equiv 19112 \pmod{p}$? Justifier et donner sa valeur (uniquement des formules et la valeur, pas de rédaction).

Exercice 3 :

Martine envoie un Gérard un message qu'elle signe en utilisant le RSA. Le message est long, on l'appelle M . Martine utilise une fonction de hashage H connue de Gérard pour calculer :

$$m = H(M). \\ m = 42\ 653\ 567\ 721\ 081\ 195\ 475$$

Pour signer, elle a besoin de fabriquer une clé. Martine part du nombre suivant :

$$p = 1\ 569\ 875\ 435\ 281.$$

Martine a effectué les premières vérifications suivantes :

$$7^{p-1} \equiv 1 \pmod{p}, 1513^{p-1} \equiv 1 \pmod{p}, 12035^{p-1} \equiv 1 \pmod{p}.$$

3.1 Que pensez-vous concernant la nature du nombre p ?

Martine a confirmé la nature de p à l'aide d'un test de Miller Rabin. Elle a fait de même avec le nombre q suivant :

$$q=32\,546\,887.$$

3.2 Pouvez-vous affirmer avec certitude que p et q sont premiers ? (une seule phrase)

On pose :

$$n=pq=51\,094\,558\,396\,166\,520\,247$$

$$f=(p-1)(q-1)=51\,094\,556\,826\,258\,538\,080$$

$$e=25\,829\,711\,613\,387\,463\,663$$

$$d=27\,383\,134\,542\,441\,090\,607$$

On a vérifié :

$$ed\equiv 1(\text{mod } f).$$

Martine a calculé le nombre c suivant :

$$c=m^d(\text{mod } n).$$

Ce qui a donné :

$$c=34\,566\,211\,176\,812\,038\,117.$$

Dans un premier temps, Martine a envoyé à Gérard les nombre n et e .

Ensuite, Gérard reçoit de Martine le message que nous appelons pour le moment M' , accompagné de la signature c , Gérard recalcule $m' = H(M')$ avec la fonction de hashage H . Il trouve :

$$m'=51\,787\,651\,733\,821\,195\,973.$$

Gérard calcule ensuite la quantité suivante :

$$c^e(\text{mod } n).$$

Il trouve la quantité suivante (une valeur numérique, ou l'un des nombres présentés ci-dessus) avec une justification en une phrase maximum :

3.3 Mettez-vous à la place de Maurice et commentez ce résultat (2 phrases).