#6

a) $d = \frac{3(p-1)(q-1)+1}{7}$

Pour que d soit un entier, il faut que $3(p-1)(q-1)+1$ soit divisible par 7.

$3(p-1)(q-1)+1 \equiv 3(2-1)(3-1)+1 \equiv 7 \equiv 0 \pmod 7$

donc $3(p-1)(q-1)+1$ est divisible par 7

$\Rightarrow d$ est bien un entier !

b)

Pour le b), nous allons utiliser le lemme suivant :

Lemme d'Euclide

Soient $a, b, c \in \mathbb{Z}$. Si a divise bc et $(a,b)=1$, alors a divise c.

Ici, on veut mq $a \neq 0$, càd que $m^7 \not\equiv 0 \pmod n$, en sachant que $(m,n)=1$.

Supposons que $m^7 \equiv 0 \pmod n$

$\Rightarrow n \mid m^7 \Rightarrow n \mid m^6 \cdot m$

mais $(m,n)=1$, alors selon le lemme d'Euclide, $n \mid m^6$

$\Rightarrow n \mid m^5 \cdot m$, mais par le lemme d'Euclide $\Rightarrow n \mid m^5$

$\Rightarrow \ldots$

$\Rightarrow n \mid m \cdot m \Rightarrow n \mid m$ par le lemme d'Euclide.

contradiction, n ne peut pas diviser m car ils sont copremiers.

On conclut que $m^7 \not\equiv 0 \pmod{n} \Rightarrow a \neq 0$.

Puis, $m_1 \equiv a^d \equiv m^{7d} \pmod{n}$.

Par le m̂ argument que pour «a», on peut conclure que $m^{7d} \not\equiv 0 \pmod{n} \Rightarrow m_1 \neq 0$.

c) Le numéro utilise le thm suivant:

thm d'Euler: Soit $\varphi(n)$ la fonction d'Euler et

Soit m tq $(m,n)=1$.

Alors, $m^{\varphi(n)} \equiv 1 \pmod{n}$

Béatrice calcul $m_1 \equiv a^d \pmod{n}$, où $m_1 \in \{1, \dots, n-1\}$

ici, $\varphi(n) = (p-1)(q-1)$, car $n = p.q$ avec p, q des premiers.

$$m_1 \equiv a^d \equiv m^{7d} \equiv m^{3(p-1)(q-1)+1} \equiv m^{3\varphi(n)+1} \equiv \left(m^{\varphi(n)}\right)^3 \cdot m$$

$$\equiv 1^3 \cdot m \equiv m \pmod{n}.$$

et $m \in \{1, \dots, n-1\} \Rightarrow m_1 = m$.

Alors Béatrice réussira à décoder le message d'Alain.

#9

a) On veut montrer que $F(N)=F(r)$ s'il n'y a pas d'erreur dans la multiplication $N=m\cdot n$.

Premièrement, convainquons-nous que la fct F renvoie le modulo 9 du nombre qu'on lui fourni.

Notons que $10^i \equiv 1^i \equiv 1 \pmod{n}$ $\forall i \in \mathbb{Z}$.

$$M \equiv a_p \cdot 10^p + a_{p-1} \cdot 10^{p-1} + \ldots + a_2 10^2 + a_1 \cdot 10 + a_0 \pmod{9}$$

$$\equiv a_p \cdot 1^p + a_{p-1} \cdot 1^{p-1} + \ldots + a_2 \cdot 1^2 + a_1 + a_0 \pmod{9}$$

$$\equiv F(M) \pmod{9}.$$

$\Rightarrow M \equiv F(M) \pmod{9}$

On a alors :

$$F(r) \equiv r \equiv F(m)\,F(n) \equiv m \cdot n \equiv N \equiv F(N) \pmod{9}$$

et puisque $F(r), F(N) \in \{0, 1, \ldots, 8\}$, on a $F(r) = F(N)$.

b) exemple: $\underset{m}{61} \cdot \underset{n}{75} = \underset{N}{4575}$.

$F(N)$: $4+5+7+5 = 21 \equiv 3 \pmod{9}$.

$F(r)$: $F(m) = 6+1 = 7 \equiv 7 \pmod 9$
$F(n) = 7+5 = 12 \equiv 3 \pmod 9$

$r = F(m) \cdot F(n) = 7 \cdot 3 = \underline{21} \Rightarrow F(r) = 2+1 = 3$

on a bien $F(r) = F(N)$ ✓.

Si on avait fait une erreur dans la multiplication

Disons $61 \cdot 75 =^{*} 4585$

on aurait le même $F(r) = 3$, mais

$F(N)$: $4+5+8+5 = 22 \equiv 4 \pmod 9$

$F(r) \neq F(N)$, on a donc fait une erreur dans la multiplication !!

c) On ne peut pas conclure qu'on a pas d'erreur de calculs si $F(r) = F(N)$.

Cela nous indique seulement que nous sommes à un multiple de 9 de la bonne réponse.

ex : Si on avait fait l'erreur $61 \cdot 75 =^{*} 4584$

on aura $F(r) = 3$, $F(N) = 3$, mais on sait que ce n'est pas la bonne réponse.

#11

On sait que $\varphi(n) = \varphi(851) = (23-1)(37-1)$
$= 792.$

On cherche alors $d \in \{1, \dots, \underbrace{851-1}_{=850}\}$ tel que

$47 \cdot d \equiv 1 \pmod{792}$

On a que $(47, 792) = 1$. alors $\exists d, f$ tels que

$1 = f \cdot 792 + 47 \cdot d \equiv 47 \cdot d \pmod{792}$

On cherche alors ce d avec l'algorithme d'Euclide.

$792 = 16 \cdot 47 + 40$ (1)

$47 = 1 \cdot 40 + 7$ (2)

$40 = 5 \cdot 7 + 5$ (3)

$7 = 1 \cdot 5 + 2$ (4)

$5 = 2 \cdot 2 + 1.$ (5)

(1) $40 = 792 - 16 \cdot 47$

(2) $7 = 47 - 1 \cdot 40$

(3) $5 = 40 - 5 \cdot 7$

(4) $2 = 7 - 5$

(5) $1 = 5 - 2 \cdot 2$

$$\overset{(4)}{=} 5 - 2(7-5) = -2 \cdot 7 + 3 \cdot 5$$

$$\overset{(3)}{=} -2 \cdot 7 + 3(40 - 5 \cdot 7) = 3 \cdot 40 - 17 \cdot 7$$

$$\overset{(2)}{=} 3 \cdot 40 - 17(47 - 1 \cdot 40) = -17 \cdot 47 + 20 \cdot 40$$

$$\overset{(1)}{=} -17 \cdot 47 + 20(792 - 16 \cdot 47)$$

$$= 20 \cdot 792 - 337 \cdot 47.$$

alors $1 \equiv -337 \cdot 47 \pmod{792}$

on veut $d \in \{1, \dots, 850\}$, alors

$-337 \equiv 455 = d \pmod{792}$

#12.

a)

on a $10^i \equiv (-1)^i \pmod{11}$ puisque $10 \equiv -1 \pmod{11}$

on sait aussi que N sera divisible par 11 si et seulement si $N \equiv 0 \pmod{11}$.

Alors, 11 divise N ssi

$0 \equiv N$

$\equiv a_0 + a_1 10 + a_2 \cdot 10^2 + \ldots + a_{N-2} \cdot 10^{N-2} + a_{N-1} \cdot 10^{N-1} \pmod{11}$

$\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + \ldots + a_{N-2} \cdot (-1)^{N-2} + a_{N-1} (-1)^{N-1} \pmod{11}$

$\equiv a_0 - a_1 + a_2 - a_3 + \ldots + a_{N-2} (-1)^{N-2} + a_{N-1} \cdot (-1)^{N-1}$.

$\square$

b). On remarque que $100 \equiv -1 \pmod{101}$.

Alors, par un processus similaire, 101 divise N ssi

$0 \equiv N \pmod{101}$

$\equiv a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + 10^3 \cdot a_3 + 10^4 a_4 + 10^5 \cdot a_5 + \ldots \pmod{101}$

$\equiv (a_0 + 10 \cdot a_1) + \underbrace{10^2}_{100} (a_2 + 10 a_3) + \underbrace{10^4}_{100^2} (a_4 + 10 a_5) + \underbrace{\ldots}_{100^3} \pmod{101}$

$\equiv (a_0 + 10 \cdot a_1) - (a_2 + 10 \cdot a_3) + (-1)^2 (a_4 + 10 a_5) + \ldots \pmod{101}$

$\equiv (a_0 + 10 \cdot a_1) - (a_2 + 10 \cdot a_3) + (a_4 + 10 a_5) - \ldots \pmod{101}$

$\Rightarrow 0 \equiv -(a_0 + 10 \cdot a_1) + (a_2 + 10 \cdot a_3) - (a_4 + 10 a_5) + \ldots$

$\boxtimes$

Exercice B :

On a $(e_B, e_C) = 1$. Alors, il existe $x, y \in \mathbb{Z}$ tels que $e_B x + e_C y = 1$.

De plus, m_B et m_C sont calculés avec les clés d'encryption :

$$m^{e_B} \equiv m_B \pmod{n}$$
$$m^{e_C} \equiv m_C \pmod{n}$$

Alors, avec le calcul suivant on peut retrouver m :

$$m_B^x \cdot m_C^y \equiv m^{e_B x} \cdot m^{e_C y} \equiv m^{e_B x + e_C y} \equiv m \pmod{n}$$

n, e_B et e_C sont des données publiques.

Un malfaiteür interceptant les messages encryptés m_B et m_C pourra retrouver m en :

1. trouvant $x, y \in \mathbb{Z}$ tq $e_B x + e_C y = 1$
2. calculant $m_B^x \cdot m_C^y \equiv m \pmod{n}$.

Et boom, le message n'est plus confidentiel.

Exer C :

a) « Jet »

$\downarrow$ Nombres associés aux lettres

10 5 20

$\downarrow$ $a \equiv 3^N \pmod{29}$

5 11 25

$\downarrow$ Nouvelles lettres

E K Y

b) 3^N, pour chaque valeur de $N \in \{1, \dots, 28\}$, va nous donner une valeur distincte modulo 29.

Alors, en connaissant seulement « a », il est possible de retrouver le N de départ. Voici une façon de faire :

L'inverse modulo est l'élément a^{-1} tel que

$a \cdot a^{-1} \equiv 1 \pmod{29}$.

Par ex: que vaut $3^{-1} \pmod{29}$?

$29 = 9 \cdot 3 + 2 \Rightarrow 2 = 29 - 9 \cdot 3$

$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 2 = 3 - (29 - 9 \cdot 3) = 10 \cdot 3 - 29$

$\Rightarrow 1 \equiv 10 \cdot 3 \pmod{29}$

Alors, $3^{-1} \equiv 10 \pmod{29}$.

Maintenant, intéressons-nous à a^{-1}.

$$1 \equiv a \cdot a^{-1} \equiv a \cdot (a)^{-1} \equiv a \cdot (3^N)^{-1} \equiv a \cdot 3^{-N} \equiv a \cdot (3^{-1})^N$$

$$\equiv a \cdot 10^N \pmod{29}.$$

La techique serait alors la suivante :

- Vérifier si $a \cdot 10 \equiv 1 \pmod{29}$.
  ↳ si c'est le cas, alors $N = 1$.
- Vérifier si $a \cdot 10^2 \equiv 1 \pmod{29}$.
  ↳ si c'est le cas, $N = 2$.
- ... continuer jusqu'à obtenir $a \cdot 10^N \equiv 1 \pmod{29}$.

c) décoder « X M F »

nombres associés

24 13 6

Retrouver le « N ».
J'ai ici utilisé l'ordinateur.

24 26 18

Le mot décodé

X Z R