Corrigé du devoir 1.

Exercice 14 de la feuille 1 (le petit théorème de Fermat):

1) Soit p un nombre premier et soit $1 \leq k \leq p-1$.

Alors, $\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p!}{(p-k)!k!}$ est un entier naturel. Donc, on a l'égalité suivante dans $\mathbb{Z}$:

$$p! = \left(\begin{array}{c} p \\ k \end{array} \right) \times (p-k)!k!$$

On en conclut que p divise $\left(\begin{array}{c} p \\ k \end{array} \right) \times (p-k)!k!$ dans $\mathbb{Z}$.

Or p est un nombre premier et $(p-k)!k!$ est un produit d'entiers qui sont tous strictement inférieurs à p. On en conclut que p ne divise pas $(p-k)!k!$. Et le lemme de Gauss permet alors d'en conclure que p divise $\left(\begin{array}{c} p \\ k \end{array} \right)$ dans $\mathbb{Z}$, c'est-à-dire, que $\left(\begin{array}{c} p \\ k \end{array} \right) = 0 \bmod p$.

2) On veut montrer que pour tout $a \in \mathbb{Z}$, on a $a^p = a \bmod p$. Comme la classe $\overline{a^p}$ de a^p modulo p est égale à $\overline{a}^p$, où $\overline{a}$ est la classe de a modulo p, il suffit de montrer que c'est vrai pour tout $a \in \{0, ..., p-1\}$ (ensemble de représentants des classes modulo p).

On va montrer par récurrence sur a que pour tout $a \in \{0, ..., p-1\}$, on a $a^p = a \bmod p$.

Si $a = 0$ et si $a = 1$, le résultat est clair.

Supposons que pour $a \in \mathbb{N}^*$, on ait $a^p = a \bmod p$. Alors,

$$\begin{array}{rcl} (a+1)^p & = & (\sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) a^k) \bmod p \\ & = & (a^p + 1) \bmod p \ \text{ (par le 1))} \\ & = & (a+1) \bmod p \ \text{ (par hypothèse de récurrence)} \end{array}$$

Ainsi, on a $a^p = a \bmod p$, pour tout $a \in \{0, ..., p-1\}$.

3) Soit a un entier premier avec p, alors, a est inversible modulo p. Donc, en multipliant $a^p = a \bmod p$ par $a^{-1} \bmod p$, on obtient $a^{p-1} = 1 \bmod p$.

4) $561 = 3 \times 11 \times 17$.

5) Soit a un entier premier avec 561, alors a est premier avec 3, avec 11 et avec 17.

En appliquant le petit théorème de Fermat avec $p = 3$, on obtient $a^2 = 1 \bmod 3$. Or $560 = 230 \times 2$, et on obtient $a^{560} = 1^{230} \bmod 3 = 1 \bmod 3$.

En appliquant le petit théorème de Fermat avec $p = 11$, on obtient $a^{10} = 1 \bmod 11$. Or $560 = 56 \times 10$, et on obtient $a^{560} = 1^{56} \bmod 11 = 1 \bmod 11$.

En appliquant le petit théorème de Fermat avec $p = 17$, on obtient $a^{16} = 1 \bmod 17$. Or $560 = 35 \times 16$, et on obtient $a^{560} = 1^{35} \bmod 17 = 1 \bmod 17$.

Ainsi, $a^{560} - 1$ est divisible à la fois par 3, par 11 et par 17 et comme ces trois entiers sont premiers entre eux deux à deux, $a^{560} - 1$ est divisible par $561 = 3 \times 11 \times 17$. Ce qui prouve que $a^{560} = 1 \bmod 561$.

6) Soit n un entier $n > 1$. On suppose que n est sans facteurs carrés et que $p - 1$ divise $n - 1$ pour tout facteur premier p de n.

On pose $n = p_1...p_r$, alors $p_i \neq p_j$ si $i \neq j$ et $(p_i - 1)|(n-1)$ pour tout $i \in \{1, ..., r\}$.

Soit a un entier premier avec n.

Soit $i \in \{1, ..., r\}$. En appliquant le petit théorème de Fermat avec $p = p_i$, on obtient $a^{p_i - 1} = 1 \bmod p_i$. Or $p_i - 1$ divise $n - 1$, donc $a^{n-1} = 1 \bmod p_i$.

Ainsi, $a^{n-1} - 1$ est divisible par p_i pour tout $i \in \{1, ..., r\}$ et comme les p_i sont premiers entre eux deux à deux, $a^n - 1$ est divisible par $n = p_1...p_r$. Ce qui prouve que $a^{n-1} = 1 \bmod n$.

Exercice 5 de la feuille 2

1) partieldecrypto

2) Méthode utilisée avec la table:

Nous surlignons les 6 lignes C,R,Y,P,T,O. Nous savons que, pour chiffrer la première lettre du message en clair inconnu de nous, le chiffreur a parcouru la colonne correspondant à cette lettre jusqu'à la ligne C et qu'il a pris la lettre dans cette case: le R.

Donc, pour retrouver la lettre inconnue, à partir du R et du C (première lettre du mot clé CRYPTO), nous parcourons la ligne C, jusqu'au R, où nous remontons la colonne, ce qui nous donne la lettre p.

Pour la deuxième lettre, il faut trouver cette fois l'intersection de la ligne R (deuxième lettre du mot-clé) avec une colonne inconnue qui donne la case R; nous trouvons a.

Pour la troisième lettre, la recherche de la colonne qui rencontre la ligne Y en P nous donne r.

En utilisant successivement toutes les lettres du mot-clé et les 6 premières lettres du cryptogramme, nous trouvons ainsi les 6 premières lettres du message en clair: partie

Pour la septième lettre, nous reprenons la ligne C, correspondant à la première lettre du mot-clé, nous trouvons la case N, nous remontons la colonne correspondante, et nous en déduisons que la septième lettre du message en clair est l.

Nous continuons ainsi, pour déchiffrer tout le message.

3) Méthode alternative sans la table: Nous mettons en correspondance les 26 lettres de l'alphabet, de A à Z, avec les éléments de $\mathbb{Z}/26\mathbb{Z}$ notés de 0 à 25. Le mot clé CRYPTO est une chaîne de caractères de longueur 6, qui correspond à la clé $(2, 17, 24, 15, 19, 14)$ dans $(\mathbb{Z}/26\mathbb{Z})^6$. Le texte en clair inconnu a été décomposé en blocs de messages de 6 caractères qui correspondent à des vecteurs $(x_1, x_2, x_3, x_4, x_5, x_6) \in (\mathbb{Z}/26\mathbb{Z})^6$.

Ainsi, la fonction de chiffrement est une fonction $e : (\mathbb{Z}/26\mathbb{Z})^6 \to (\mathbb{Z}/26\mathbb{Z})^6$ et un bloc $(x_1, x_2, x_3, x_4, x_5, x_6)$ du message en clair a été chiffré par $e((x_1, x_2, x_3, x_4, x_5, x_6)) = (x_1+2, x_2+17, x_3+24, x_4+15, x_5+19, x_6+14)$.

Pour déchiffrer, il suffit donc d'appliquer $d = e^{-1}$ à un vecteur $(y_1, y_2, y_3, y_4, y_5, y_6) \in (\mathbb{Z}/26\mathbb{Z})^6$ qui correspond à un bloc de six caractères du message chiffré. Et d est définie par $d((y_1, y_2, y_3, y_4, y_5, y_6)) = (y_1 - 2, y_2 - 17, y_3 - 24, y_4 - 15, y_5 - 19, y_6 - 14)$.

Ainsi, pour déchiffrer la chaîne de 6 caractères alphabétiques RRPIBS,

- on le convertit en un vecteur de $(\mathbb{Z}/26\mathbb{Z})^6$, $(17, 17, 15, 8, 1, 18)$,
- on applique la fonction de déchiffrement: $d((17, 17, 15, 8, 1, 18)) = (15, 0, 17, 19, 8, 4)$ dans $(\mathbb{Z}/26\mathbb{Z})^6$,
- on convertit $(15, 0, 17, 19, 8, 4)$ en texte clair, ce qui donne partie.

Nous obtenons ainsi les 6 premières lettres du message en clair et on recommence la même procédure avec NUCRKM, puis avec RKM mais en faisant le même raisonnement avec les 3 premières lettres du mot clé: CRY.