Exercice 1. Une solution est d'utiliser deux jeux de clés asymétriques : un jeu pour signer le message, et un pour chiffrer. Par exemple avec RSA, si Alice a une clé (d_A, e_A, N_A), et Bob une clé (d_B, e_B, N_B). Soit m le message. Alice commence par le signer avec sa clé privée : $m' = m^{d_A} \bmod N_A$, puis le chiffre avec la clé publique de Bob : $m'' = m'^{e_B} \bmod N_B$. Note : pour que m' puisse être déchiffré correctement, il faut que $m' < N_B$, et pour cela il suffit que $N_A < N_B$. De son côté, Bob déchiffre avec sa clé privée : $m' = m''^{d_B} \bmod N_B$, puis vérifie que $m' < N_A$, et enfin vérifie la signature d'Alice et extrait le message avec $m = m'^{e_A} \bmod N_A$.

Perles : une copie propose de transmettre le message en clair...

Exercice 2. h_1 n'est pas à sens unique car étant donné y, il suffit de factoriser $x^3 - y$ sur $F_p[x]$; elle n'est donc pas non plus résistante aux collisions (voir cours).

h_2 est à sens unique (calcul de racine cubique mod n), et résistante aux collisions. En effet, si on sait trouver x et y tels que $x^3 = y^3 \bmod n$, alors $x^3 - y^3 = 0 \bmod n$, donc $x - y$ ou bien $x^2 + xy + y^2$ a un pgcd non-trivial avec n, et donc on saurait factoriser n. (Note: L'enoncé oublie de préciser que p et q sont inconnus.)

Si on considère que le domaine de départ de h_3 est F_p, alors h_3 est à sens unique et résistante aux collisions (c'est le problème du logarithme discret sur F_p). De plus pour peu que 3 soit générateur du groupe cyclique de F_p, l'équation $3^x \equiv 3^y \bmod p$ n'a d'autre solution que $x = y$, car elle implique $3^{x-y} \equiv 1 \bmod p$. Si on considère que le domaine de départ de h_3 est $\mathbb{Z}$, alors h_3 n'est pas à sens unique, et donc pas résistante aux collisions, puisque $h_3(x) = h_3(x + p - 1)$ car $3^{p-1} = 1 \bmod p$. Les deux réponses sont correctes, si bien argumentées.

Perles : une copie propose de factoriser $3^x - y$ sur $F_p[x]$ en utilisant le logarithme discret... Une autre dit que p et q ayant tous deux 512 bits, on a $p = q + k$ avec k petit ! Prendre $x' = x + kn$ pour h_2 est triché : on a en effet $x' = x \bmod n$. De même, 3^{x^2} n'est pas $(3^x)^2$: prendre par exemple $x = 3$, on a $3^{x^2} = 3^9 = 19683$, alors que $(3^x)^2 = 27^2 = 729$. Pour $h_3(x) = 3^x$, une copie parle de difficulté de calcul de racine cubique. Une copie indique que h_1 est inversible car il suffit de chercher $x^3 = kp + 3$, pour $y = 3$ par exemple, avec tous les premiers p de 1024 bits... Enfin le classique "dur de factoriser les nombres premiers" (Bill Gates l'a faite aussi).

Exercice 3. C'est essentiellement un exercice de cours. Le premier cas est auto-synchronisant, car au bout de t étapes, le chiffrement ne dépend que des t derniers c_i, supposés corrects ; le second ne l'est pas, car les t derniers m_i dépendent du déchiffrement correct des précécents, donc un m_i incorrect empêche le déchiffrement correct de tout ce qui suit.

Exercice 4. Les valeurs obtenues à partir de $s_0 = s_1 = s_2 = s_3 = 1$ sont $s_4 = 0, s_5 = 1, s_6 = 1, s_7 = 1, s_8 = 1, s_9 = 0, s_{10} = 1, \ldots$ Comme on a $s_0 = s_5, \ldots, s_3 = s_8$, on a $s_i = s_{i+5}$ pour tout $i \geq 0$. La suite est périodique, de période 5.

Le polynôme associé à la suite est $f(x) = x^4 + x^3 + x^2 + x + 1$, de degré $l = 4$. Ce polynôme est irréductible sur GF(2). On sait (cf cours 3) que chacun des $2^l - 1$ états initiaux possibles

où les cellules ne sont pas toutes nulles produit une suite de période k, où k est le plus petit entier tel que $f(x)$ divise $x^k + 1$ dans $\mathbb{F}_2[x]$, et que de plus k divise $2^l - 1$. Ici on a $k = 5$, car $f(x)(x + 1) = x^5 + 1$.

Pour savoir le nombre de suites différentes (modulo translation), il suffit donc de regarder les 5 premières valeurs, notamment leur poids (nombre de 1). Si le poids de s_0, s_1, s_2, s_3 est pair, alors $s_4 = 0$; s'il est impair, alors $s_4 = 1$; dans tous les cas, le poids de s_0, s_1, s_2, s_3, s_4 est pair. En poids 0, on n'a que la suite $[0, 0, 0, 0, 0, \ldots]$; en poids 2, on a quatre choix $[1, 0, 0, 0, 1, 1, 0, \ldots]$, $[0, 1, 0, 0, 1, 0, 1, 0, \ldots]$, $[0, 0, 1, 0, 1, 0, 0, 1, 0, \ldots]$, $[0, 0, 1, 0, 1, 0, 0, 1, 0, \ldots]$, $[0, 0, 0, 1, 1, 0, \ldots]$, qui ne donnent que deux périodes par translation ; en poids 4, on a cinq choix $[1, 1, 1, 1, 0, 1, \ldots]$ (suite de la première question), $[1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, \ldots]$, $[1, 1, 0, 1, 1, 1, 1, 0, 1, \ldots]$, $[1, 0, 1, 1, 1, 1, 0, \ldots]$, donc une seule période par translation. Au total, on n'a donc que 4 "schémas périodiques" possibles modulo translation, en comptant la suite identiquement nulle.

L'énoncé étant imprécis, on pouvait aussi penser qu'il s'agissait des suites obtenues avec le même schéma périodique ; la réponse 5 a donc aussi été comptée bonne.

Perles : période 8...

Exercice 5. C'était un exercice calculatoire. L'inverse de $x^7 \bmod m(x)$ se calcule par l'algorithme d'Euclide étendu : il faut trouver $u(x)$ et $v(x)$ tels que $u(x)x^7 + v(x)m(x) = 1$. On écrit :

$$\begin{aligned} m(x) &= q_1 x^7 + r_1, & q_1 = x, r_1 = x^4 + x^3 + x + 1 \\ x^7 &= q_2 r_1 + r_2, & q_2 = x^3 + x^2 + x, r_2 = x \\ r_1 &= q_3 r_2 + r_3, & q_3 = x^3 + x^2 + 1, r_3 = 1. \end{aligned}$$

On en déduit (en identifiant + et − modulo 2) :

$$\begin{aligned} r_1 &= m + q_1 x^7 \\ r_2 &= x^7 + q_2(m + q_1 x^7) = q_2 m + (q_2 q_1 + 1)x^7 \\ r_3 &= r_1 + q_3[q_2 m + (q_2 q_1 + 1)x^7] = (q_3 q_2 + 1)m + (q_3 q_2 q_1 + q_3 + q_1)x^7 \\ &= (x^6 + x^2 + x + 1)m + (x^7 + x + 1)x^7. \end{aligned}$$

On a donc $u(x) = x^7 + x + 1$ et $v(x) = x^6 + x^2 + x + 1$. L'inverse de x^7 modulo $m(x)$ est donc $u(x) = x^7 + x + 1$.

Pour calculer $x^{42} \bmod m(x)$, on peut commencer par calculer $x^{14} \bmod m$, par division par m : $x^14 = x^6 m + x^{10} + x^9 + x^7 + x^6 = (x^6 + x^2)m + x^9 + x^7 + x^5 + x^3 + x^2 = (x^6 + x^2 + x)m + x^7 + x^4 + x^3 + x$. Donc $x^{14} = x^7 + x^4 + x^3 + x \bmod m$. On calcule ensuite $x^{21} = x^{14} \cdot x^7 = x^5 + x^4 + x^2 + 1$, puis $x^{42} = x^{21} \cdot x^{21} = x^6 + x^5 + x^2 + x$.

Erreur à ne pas commettre : remplacer les polynômes par des entiers !

Exercice 6. Première question : Alice et Bob peuvent utiliser $a\beta = b\alpha = Nab$.

Deuxième question : ce n'est pas sûr car Charlie peut obtenir a et b par simple division de α et β par N (public).

Dans la troisième question, beaucoup sont tombés dans le piège en multipliant α par β : ce n'est pas un secret, car si Charlie intercepte α et β, il peut aussi bien faire ce calcul.

Certains proposent comme clé commune $g^{\alpha\beta}$, mais comme l'énoncé précise que α et β sont envoyés, et comme g est supposé connu, Charlie peut aussi calculer $g^{\alpha\beta}$.

Perles : a^N multiplié par b^N donne $(ab)^{N^2}\ldots$

Exercice 7. Pour un système à clé secrète, il faut autant de clés qu'il y a de couples de personnes, soit $\binom{n}{2} = \frac{n(n-1)}{2}$. Ici cela vaut $17 \cdot 8 = 136$, et non 17^{16}, ni 17! (factorielle 17). Ce n'est pas non plus $n(n-1)$ (nombre d'arrangements), car les clés sont symétriques.

Pour un système à clé publique, il faut 17 clés (autant que de participants), et non 180 clés comme l'indique une copie (pour $n = 10$).

Perles : une copie obtient par un raisonnement faux la valeur 16! (factorielle 16) puis par un calcul faux en déduit le résultat correct 136... Pour un système à clé publique, une copie propose 17 clés secrètes (ok) et une seule clé publique ! C'est ok, sauf si la clé publique est inférieure ou égale à 17 (exercice 9).

Exercice 8. La forme $2^k + 3$ n'est pas sûre car il y a très peu de nombres de cette forme, et surtout un seul de 512 bits, à savoir $2^{511} + 3$, qui est de plus divisible par 53.

Perles : $2^k + 2 = 2^{k+1}$ (sur deux copies) ! Une copie indique que l'attaque $p-1$ est possible car $p-1 = 2^k+2$ a un petit facteur, à savoir 2 : tout nombre premier impair vérifie que $p-1$ est divisible par 2 ! Il ne suffit pas que $p-1$ ait un petit facteur premier, il faut que tous ses facteurs premiers soient petits. Une copie indique que p n'est pas premier fort car $p+1 = 2^k + 2^2$ n'est pas un grand facteur premier...

Exercice 9. C'est dangereux, car si $c_1, \ldots, c_5$ sont les chiffrés envoyés à Bob, ..., Fanny, on a $c_1 = m^5 \bmod N_1$, ..., $c_5 = m^5 \bmod N_5$, donc par restes chinois on reconstruit $M = m^5 \bmod (N_1N_2N_3N_4N_5)$. Comme par hypothèse $m < N_i$, on a $M = m^5$, et on peut retrouver m par une simple racine cinquième.

Exercice 10. On peut utiliser g^n comme secret commun. Alice et Bob ne peuvent reconstruire g^n sans l'aide de Charlie, car il leur manque deux inconnues c et n dans $g^n = g^a g^b g^c$. S'ils connaissent g^c, ils peuvent retrouver c s'ils savent résoudre le problème du logarithme discret.

Perles : $g^n \equiv g^{b+c} \bmod g^a$!

Exercice 11. Le protocole est un partage de secret : ils peuvent retrouver N par restes chinois, mais $n-1$ participants ne peuvent pas. Toutefois, le partage n'est pas équitable, car le premier participant n'a qu'un bit d'information ($p_1 = 2$), alors que le dernier en a $\log_2 p_n$. Si le premier participant manque, on peut retrouver N en deux essais.