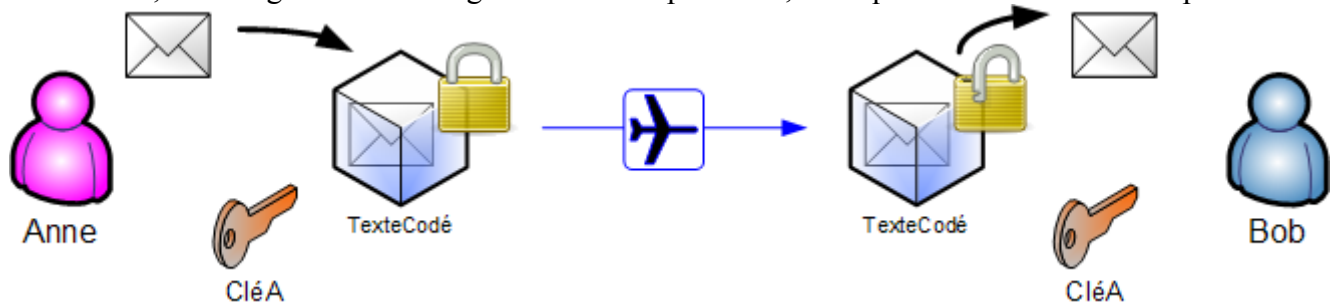
Sécurité des communications

1. Introduction

Les communications, qu'elles soient entre humains, entre humains et machines, ou entre machines, peuvent être interceptées par différents moyens, parfois surprenants[1]. Il est donc important de les protéger, que ce soit pour protéger sa vie privée ou pour éviter un piratage. Pour protéger ces communications, on chiffre[2] les messages à l'aide d'une méthode de cryptographie, comportant une ou plusieurs clés secrètes. Les deux principes de chiffrement sont le chiffrement symétrique, où la même clé est utilisée pour le chiffrement et le déchiffrement du message, et le chiffrement asymétrique, où deux clés différentes sont utilisées. Reste à assurer que les clés ne soient pas piratées, ce qui est le problème de l'authenticité des utilisateurs. La sécurité des communications dépend à la fois des méthodes de chiffrement et des protocoles d'échange des clés.

2. Chiffrement symétrique

Dans le chiffrement symétrique, la même clé permet à la fois de chiffrer et de déchiffrer le message. La clé secrète doit donc être connue préalablement par les deux entités communiquant. On peut remarquer que si la clé fait la taille du message (ou plus), alors le message ne peut pas être décrypté. Comme dit en introduction, il faut également échanger cette clé au préalable, sans qu'elles ne soient interceptées !



a. Des exemples historiques

Le chiffre de César est peut-être le plus connu. César chiffrait ces messages en décalant toutes les lettres de 3 (car C est la troisième lettre de l'alphabet). Ce chiffrement a été utilisé par les égyptiens en -2000.

Plus sophistiqué, le chiffre de Vigénère utilise un décalage alphabétique également, mais avec une clé de plusieurs lettres répétée. Si la clé est NSI, la première et la quatrième lettre du message seront décalées de 14, la deuxième et la cinquième de 19, la troisième et la sixième de 9 etc. Ce chiffre a résisté longtemps au décryptage, et a été utilisé jusque pendant la guerre de Sécession.

Enfin, le fameux code Enigma utilisé par l'Allemagne nazie pendant la deuxième guerre mondiale a été cassé par Alan Turing. Comme les alliés ne voulaient pas que les allemands changent de système, ils ont masqué leur découverte, en rajoutant du « bruit » à l'information recueillie. Par exemple, ils faisaient passer des avions de reconnaissance « par hasard » en vue d'un convoi de ravitaillement des forces de l'axe dont le trajet était connu grâce à Enigma. Et très probablement, les alliés ne ciblaient pas tous les convois repérés.

b. Méthodes actuelles

L'algorithme AES est un standard de chiffrement symétrique. Il est peu coûteux en mémoire, facile à mettre en forme, et il n'existe pas actuellement de méthode plus efficace que la force brute pour le casser.

---

[1] A l'époque des écrans cathodiques, il était possible « d'écouter » au travers d'un mur les variations de fréquence de balayage de l'écran pour trouver les caractères tapés au clavier… Seule solution, écrire dans une fenêtre cachée par une autre (cette histoire est probablement apocryphe, mais elle est très jolie ☺).

[2] Vocabulaire : chiffrer/déchiffrer s'utilise pour transformer un message clair en message codé à l'aide d'une clé. Décrypter, c'est casser le code sans connaître la clé. Crypter n'est pas du français mais du globbish.

3. Chiffrement asymétrique

Lors du chiffrement asymétrique, deux clés sont utilisées, l'une privée (secrète) et l'autre publique. La clé publique permet de chiffrer le message, et la clé privée permet de le déchiffrer. Comme leur nom l'indique, la clé privée n'est pas transmise, contrairement à la clé publique.

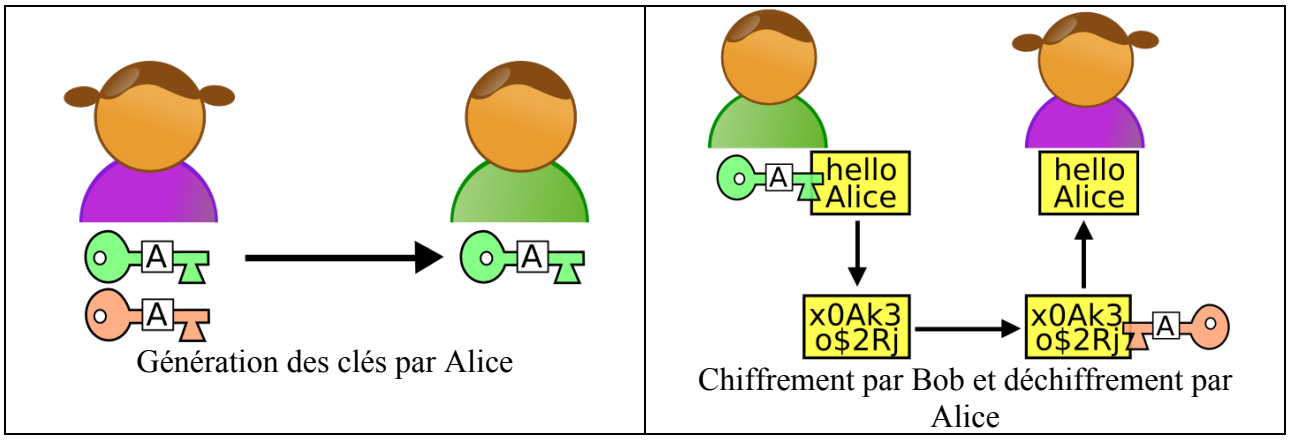
Le principe a été imaginé en 1976 par Diffie et Hellman, mais sans algorithme correspondant. En 1978 Rivest, Shamir et Adleman inventent l'algorithme RSA. Les services secrets anglais avaient déjà imaginé des concepts semblables quelques années plus tôt, mais ont gardé ces recherches secrètes jusqu'en 1997.

Ces protocoles reposent sur l'asymétrie des fonctions utilisées (fonctions dites à sens unique). Par exemple, dans RSA on utilise le produit de deux nombres premiers. Autant il est facile d'effectuer une multiplication de deux nombres premiers, autant il est difficile d'obtenir la décomposition de ce produit en les deux nombres d'origine[3].

Principe :

Alice souhaite recevoir un message secret de Bob, sur un canal susceptible d'être écouté par Ève.

- Alice génère deux clés (sa clé publique et sa clé privée).
- Elle transmet à Bob la clé publique et conserve précieusement la clé privée.
- Bob chiffre son message avec la clé publique et l'envoie à Alice.
- Alice déchiffre le message avec sa clé privée.
- Si Ève intercepte le message, elle ne peut pas le déchiffrer, ne disposant pas de la clé privée.



Génération des clés par Alice

Chiffrement par Bob et déchiffrement par Alice

On peut compléter ce protocole avec un mécanisme d'authentification (signature des messages) ou des certificats de sécurité. En effet, Alice ne peut pas savoir si un message reçu provient de Bob ou d'Ève, vu qu'Ève dispose également de la clé publique (cf. ci-après)

4. Compléments

a. Échange de clé de Diffie-Hellman

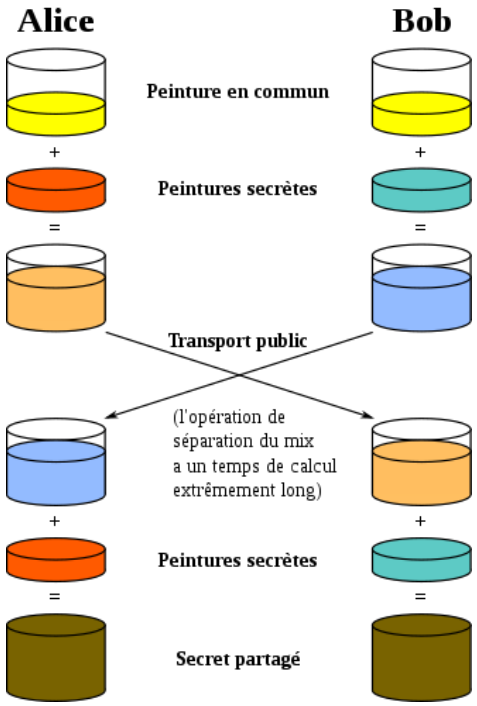
Ce protocole permet à Alice et Bob de convenir d'une clé symétrique, par un moyen de communication non sûr. Pour cela, il faut disposer d'une « fonction à sens unique » possédant certaines propriétés. Le mélange de couleurs en est une bonne métaphore : il est facile de mélanger deux couleurs, par contre retrouver les teintes d'origine est complexe. Par ailleurs cette fonction a la propriété fondamentale, qui est que le mélange de trois couleurs donne le même résultat, quelque soit l'ordre dans lequel on le fait.

Le schéma de Wikipédia (et votre livre p 412) sont très clairs :

- Alice et Bob décident d'une couleur en commun (jaune), connue de tous, y compris Eve.
- Chacun choisit une couleur secrète (Alice le rouge, Bob le vert).
- Puis mélange sa couleur secrète avec la couleur commune.

[3] Autre exemple de problème à sens unique : le problème du sac à dos. On a vu en 1ère que ce problème était de complexité exponentielle. Par contre, vérifier une solution est presque immédiat (complexité linéaire)

- Alice et Bob s'échangent leur mélange. Ève peut intercepter les mélanges, mais ne pourra que très difficilement extraire les couleurs d'origine.
- Alice et Bob mixent le mélange avec leur couleur secrète. Ils obtiennent la même teinte (kaki), inconnue d'Ève.



b. Attaque de l'homme du milieu

Cette attaque consiste à intercepter les communications entre deux entités, sans que ni l'une ni l'autre ne le réalise. Comme son nom l'indique, il suffit pour un attaquant de se placer entre les deux interlocuteurs et d'en usurper l'identité. Par exemple, dans le protocole d'échange de clés de Diffie-Hellman, Eve peut choisir aussi une peinture secrète et intercepter l'échange des mélanges. Elle créera alors deux mélanges « secrets partagés » : un pour Alice et un pour Bob. Elle pourra ainsi intercepter les messages, et par exemple dans le cas d'un message d'Alice à Bob, elle le déchiffrera avec le mélange partagé avec Alice pour le lire, puis le chiffrera avec celui de Bob, afin qu'il le reçoive bien et ne se doute de rien. Dans ce cas la puissance du chiffrement est inutile !

Pour pallier à ce problème, des procédures d'authentification sont mises en place. La plus connue sur le web est celle des certificats de sécurités (X.509 ou OpenPGP principalement). Ces certificats sont gérés par des tiers de confiance.

Remarque : sous Firefox, vous pouvez afficher le certificat de sécurité d'un site accessible en https. Cliquez sur le cadenas, puis sur « > », « plus d'information », « afficher le certificat ».

c. Protocoles hybrides

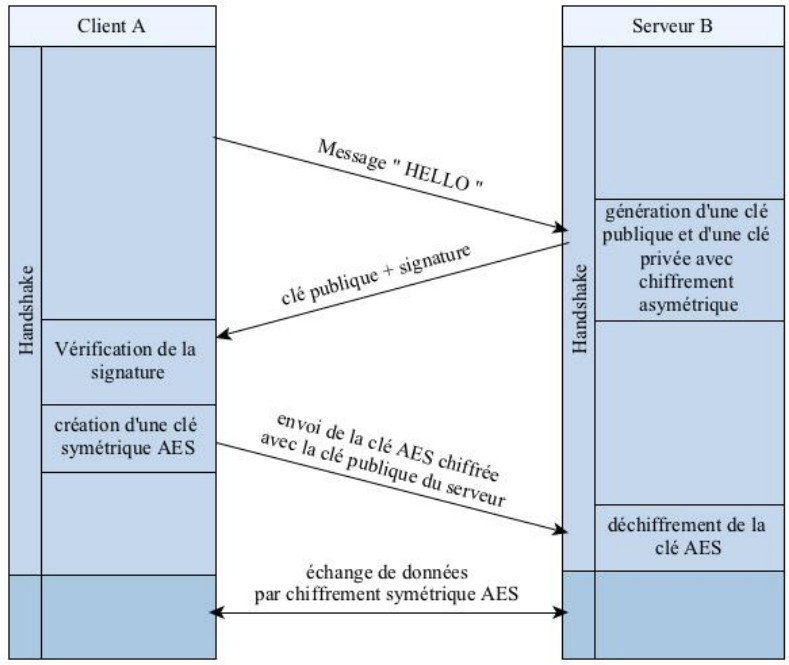
Les protocoles asymétriques sont difficiles à casser mais lents. Les protocoles symétriques sont rapides, mais nécessitent l'échange préalable des clés. Les protocoles hybrides utilisent les deux méthodes. RSA peut par exemple être utilisé pour échanger une clé de protocole symétrique.

Par exemple, TLS/SSL (le « https ») utilise en partie un chiffrement asymétrique, pour initialiser la connexion client/serveur, et créer une clé symétrique utilisée pour la suite de la session. Ce protocole mélange donc les deux types de chiffrement. Cette méthode est couplée avec un mécanisme d'authentification : l'utilisation des certificats de sécurité, confiés à un tiers de confiance.

d. https plus en détail

Le protocole http permet d'échanger des données entre client et serveur. En première, on voit deux possibilités de http avec les méthodes GET et POST. Ce protocole n'est pas sécurisé, il n'est donc pas adapté à tous les échanges de données sur le web. https rajoute à http une couche de sécurité, la couche TLS (plus sûre que SSL).

Les protocoles de communication commencent par une mise en relation des entités. On appelle souvent cette mise en relation la « poignée de mains » (handshake).



- La vérification de la signature se fait auprès d'autorités extérieures (les tiers de confiance)
- La clé symétrique est une clé AES, qui est chiffrée avec la clé publique du serveur. Elle ne sert que pour une seule session : une autre clé est générée s'il y a déconnexion et reconnexion.
- La clé symétrique est déchiffrée par le serveur avec sa clé privée : on utilise deux protocoles successivement. Protocole asymétrique pour la poignée de mains, puis protocole symétrique pour l'échange des données.

Plus de détails, tout en restant dans la vulgarisation, sur cette bande dessinée (en anglais) : https://howhttps.works/
Test des vulnérabilités de votre navigateur :
https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html

e. Le futur

Les protocoles actuels sont très solides, les coûts de décryptage étant prohibitifs. Par contre, avec un ordinateur quantique ils seront cassés très rapidement. Il faudra alors passer à des méthodes de cryptographie quantique. Notamment, lors de transmissions de paquets quantiques, une éventuelle interception est toujours détectable (elle modifie la nature du paquet transmis). Cela permet au moins de savoir que la communication a été interceptée.

EXERCICES

1. UN PROTOCOLE PAS SI SÉCURISÉ QUE CELA

Alice et Bob souhaitent communiquer, en s'envoyant des messages dans une boîte fermée à clef. Bien sûr, Eve veut les espionner. Ils utilisent le protocole suivant :

- Alice envoie à Bob la boîte ouverte, ne contenant que la clé publique d'Alice.
- Bob place le message dans la boîte puis ferme celle-ci à l'aide de la clé publique d'Alice.
- Bob envoie la boîte fermée à Alice.
- Alice utilise sa clé privée pour ouvrir la boîte.
- Alice récupère le message de Bob.

Alice et Bob sont fiers de leur protocole, mais Ève rit sous cape et lit facilement les messages de Bob. Comment fait-elle ?

2. UN EXEMPLE DE CHIFFREMENT SYMÉTRIQUE

Le XOR (ou exclusif) est très utilisé dans les protocoles de chiffrement symétrique. En effet, c'est une opération qui est sa propre réciproque, ce qui n'est pas le cas du ET ni du OU. C'est à dire que : $A \oplus B = C \Leftrightarrow A \oplus C = B \Leftrightarrow C \oplus B = A$ (1).

a. Démontrer la propriété (1) en complétant la table de vérité suivante (et en rédigeant une conclusion) :

b.

A	B	A XOR B	A XOR C	C XOR B
0	0	0		
0	1	1		
1	0	1		
1	1	0		

On va programmer un protocole de chiffrement symétrique utilisant le XOR.

c. Préliminaire : programmer une fonction qui admet deux bits en paramètres et renvoie le XOR de ces deux bits.

d. Le protocole utilisera deux listes de bits : la première contient le message proprement dit, la seconde, en général plus courte, contient la clé.
Le message chiffré est une liste de bits, de même longueur que le message originel, obtenue avec un XOR des bits du message en clair avec les bits de la clé. Comme en général la clé est plus courte, on la répète ou on utilise un modulo (opération % de Python) pour qu'elle ait la même longueur que le message.
Le protocole étant symétrique, le déchiffrement utilise le même procédé.
Ecrire la fonction de chiffrement/déchiffrement qui admet en paramètres deux listes de bits (le message et la clé), et qui renvoie le message chiffré ou déchiffré sous forme de liste de bits.

e. Compléments : écrire deux fonctions qui :
- Pour la première, étant donnée une chaîne de caractères ascii, composée uniquement de minuscules (donc non accentuées et sans espaces), renvoie le tableau de bits correspondants.
On peut faire un dictionnaire qui associe à chaque lettre un nombre sur 8 bits :
`dic_c2nbin = {chr(97 + i) : format(i, '#010b')[2:] for i in range(26)}`
Cette fonction sert à transformer un message t une clé sous forme de tableaux de bits.
- Pour la deuxième, étant donné un tableau de bits de longueur multiple de 8, renvoie un tableau ou une chaîne constituée des caractères ascii correspondants.
On peut utiliser le dictionnaire fourni par le professeur qui donne la signification des codes ascii.
Cette fonction sert à décoder le message chiffré et à le transformer sous forme de caractères ascii, qui en général ne sont pas imprimables.

Compléter alors le programme de chiffrement avec ces fonctions.

3. Un exemple de chiffrement asymétrique

Dans cet exercice, on va programmer le « RSA pour les enfants », qui est un algorithme public.
Création des clés par Alice. Elle :

- choisit quatre nombres a, b, a' et b' ;
- Calcule

$$M = a \times b - 1 \qquad e = a' \times M + a \qquad d = b' \times M + b$$

$$n = \frac{e \times d - 1}{M}$$

- La clé publique d'Alice est (n, e) et sa clé privée est (n, d)
- Le message à chiffrer doit être un entier plus petit que n, et n'ayant pas de facteurs commun avec n.

Échange des messages :

- Pour envoyer un message à Alice, Bob utilise la fonction $M_{\text{chiffré}} \equiv e \times M_{\text{clair}} \left[n \right]$, c'est-à-dire en Python : `message_chiffré = (e * message_clair) % n`
- Pour déchiffrer le message, Alice utilise sa clé privée : $M_{\text{clair}} \equiv d \times M_{\text{chiffré}} \left[n \right]$, c'est-à-dire en Python : `message_clair = (d * message_chiffré) % n`

a. Exemple
   Vérifier qu'avec les nombres $a=9, b=11, a1=5, b1=8$ et le message $M_{\text{clair}}=538$, alors le message chiffré est $M_{\text{chiffré}}=1294$. Vérifier que la méthode de déchiffrement est correcte.
b. Programmer ce chiffre en Python ; on écrira une fonction qui génère les clés étant donné les quatre nombres a, b, a' et b', et une deuxième fonction qui effectue le chiffrement d'un nombre. Il est inutile d'écrire une fonction de déchiffrement, puisque le procédé est le même, seule la clé change (ceci dit on peut le faire par souci de clarté).
c. Ève connaît la clé publique (n,e) partagée par Alice, ainsi que l'algorithme de génération des clés publiques et privées (et le message chiffré qu'elle a intercepté). Pour décrypter le message, elle cherche à trouver la clé privée par force brute, en testant toutes les valeurs de a, b, a' et b' jusqu'à retomber sur cette clé publique.
   Programmer une fonction qui permet de décrypter ce chiffre par force brute.
   Cette fonction est-elle compliquée ? Lente ? Et si on augmente la taille des nombres a, b, a' et b' utilisés ?
d. Pour ceux qui font mathématiques expertes la preuve que cela fonctionne et la méthode de décryptage « intelligente » sont résolues par les questions suivantes :
   i. Montrer que $n=a'b'M+ab'+a'b+1$; en déduire que n est entier.
   ii. Montrer que $ed\equiv 1\left[n\right]$. C'est à dire que e et d sont des inverses multiplicatifs modulo n.
   iii. En déduire que le calcul $d\times M_{\text{chiffré}}\left[n\right]$ renvoie le message en clair, lorsque le message chiffré est obtenu par $M_{\text{chiffré}}\equiv e\times M_{\text{clair}}\left[n\right]$. Ceci prouve que le système de chiffrement/déchiffrement fonctionne.
   iv. Décryptage intelligent : résoudre $ed\equiv 1\left[n\right]$, où e et n sont connus puisque publics, et où d est l'inconnue (rappel pour ce type d'équation diophantienne : on utilise l'algorithme d'Euclide et le théorème de Bézout).
   Comparer intuitivement la rapidité de calcul par rapport à la méthode en force brute. Pour une comparaison plus rigoureuse, donner la complexité de l'algorithme de la question c., et l'exercice XXXV de la page http://www.maths-info-lycee.fr/exos_arithmetique.html donne la complexité de l'algorithme d'Euclide (logarithmique pour ceux qui ont la flemme de faire l'exercice)

Conclusion : un protocole asymétrique ne suffit pas, il faut aussi un algorithme de chiffrement puissant !

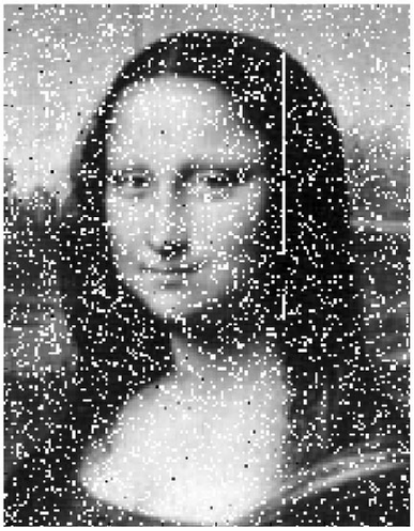
4. Le code de Reed-Solomon en version simplifiée

Un exercice tiré de quanta magazine (super magazine de vulgarisation en ligne, en anglais). Le code de Reed-Solomon est notamment utilisé par la NASA pour les missions vers la Lune et Mars et également pour la lecture des CD et DVD (et deux fois dans ce cas). C'est un code de correction d'erreur et non un algorithme de cryptographie, mais on va le dévoyer vers cet usage (à ne pas faire irl !)
Un exemple : Bob et Alice veulent s'échanger un message secret pendant le cours de NSI. Le message secret est formé de deux caractères, donnés par leur numéro dans l'ordre alphabétique. Comme il n'y a que deux lettres, ce message va être donné par les coefficients a et b d'une équation de droite : $y=ax+b$.
Alice a envoyé à Bob les valeurs 57 et 99 (la clé publique, qui sont les ordonnées y de deux points, on dit syndrome et non clé dans le cas d'un code correcteur d'erreur). Bob sait qu'il doit utiliser les abscisses x de ces deux points, c'est sa clé privée –son syndrome– 3 et 6. Pour décoder le message, Bob résout le système : $\begin{cases} 57=3a+b \\ 99=6a+b \end{cases}$. Il trouve a = 14 et b = 15 (vérifiez). Le message est donc NO.

Pour un message de 3 caractères, on utilise une parabole $y = ax^2 + bx + c$, les trois coefficients a, b, et c donnant le message, pour un message de 4 caractères une cubique $y = ax^3 + bx^2 + cx + d$ etc.

1. Déchiffrer le message de clé privée (2, 5, 6) et de clé publique (14, 59, 82) reçu par Bob. On pourra :
   - si on est quelqu'un de valeur, résoudre le système à la main ;
   - sinon, si on est un peu bourrin : écrire un programme Python qui résout le problème par force brute (réfléchir un peu sur les valeurs des coefficients) ;
   - ou si on est un moins que moins que rien : utiliser les outils de résolution de la calculatrice ou trouver un solveur en ligne.
2. Le code de Reed-Solomon offre une possibilité simple de correction d'erreur. Il suffit de rajouter un point. Dans l'exemple initial « NO » donné ci-dessus, la clé publique $y = 155$, associée à la clé privée $x = 10$, convient : le vérifier.
3. On reprend l'exemple initial, quel est le message reçu par Bob avec la clé publique (33, 57) ?
4. Comment Bob et Alice peuvent-ils être sûrs que la clé privée (3, 6) donnera toujours une solution ?
5. Bob renvoie (90, 387, 534) à Alice (exemple de la question 1). Déchiffrer le message reçu par Alice.
6. Charlie envoie un message de deux lettres + code de correction, avec la clé publique (27, 43, 90). La clé privée est (1, 3, 10). Montrer que ce message contient une erreur, essayer de trouver un moyen de la corriger (on pourra représenter les points dans un repère et faire preuve d'intuition).

Les deux images ci-dessous montrent l'efficacité du code de Solomon-Reed pour corriger les erreurs de transmissions. L'image a été transmise de la Terre vers un module lunaire, par faisceau laser.

Sans codage	Avec codage de Reed-Solomon
	

7. Exercices du livre 185 à 190 p 435

Cours de Frédéric Mandon et Romain Mallet, licence Creative Commons BY NC SA, https://creativecommons.org/licenses/by-nc-sa/3.0/fr/
Merci aux contributeurs de la liste NSI et à leurs idées toujours très riches.