**Exercice 1** On retrouve une bandelette de cuir sur laquelle on peut lire :

`proirotnecurdperoeusdubicevosycenetnrdnaiuirlfnaoefbmuraelette`

1. Examiner ce message puis le décrypter.
2. Proposer un moyen général de casser ce type de chiffrement.
3. Écrire les méthodes de chiffrement et de déchiffrement.

**Exercice 2** Le chiffrement de César revient à incrémenter d'un nombre fixé le code ASCII de chaque caractère du message.

1. Quel est le chiffrement du message « `unrondpastoutafaitclos` » si on incrémente de 4 ?
2. Écrire les méthodes de chiffrement et de déchiffrement.
3. Rappeler le moyen général de casser un chiffrement de César. Que se passe-t-il si l'on chiffre *La disparition* de Georges Perec ?
4. Écrire une méthode de cryptanalyse.
   Quel message correspond au chiffré « `gaiatksginotkgaiatjuiasktzvuaxrkdgsktjkvlat` » ?

**Exercice 3** Soit le message chiffré ci-contre par la méthode de Vigenère.

```
00 cliiyaatpiencueugaetkfvrr
01 dwsmreaqmsbcvlodwlyvhoijd
02 kiudpankyeytvwfdaxanoztex
03 wveepixoatzwhsaeokyebalof
04 ugeijdfltdpwrvzfdpasnvrob
05 jucpadmktredgpstvmebqlwrj
06 hosfenyiwawlwtaeoztzeidbj
07 aggenjqtyrtrifdrkhsafetbt
08 rmyodaaljsryvrokslcvddpwr
09 vjpyvkewiowbzecztkvqaxrix
10 alfvrrkazijdodpwryrddimgy
11 khsugukffdpwbveeqmksviidz
12 atv
```

1. Y repérer les répétitions de facteurs de longueur 4.
2. En déduire la longueur possible de la clé.
3. Écrire les méthodes de chiffrement, déchiffrement et cryptanalyse.

**Exercice 4** On considère la méthode suivante :

```
static String carre(String clef){
    String carre = "";
    boolean[] dejavu = new boolean[26];
    for(int k=0; k<clef.length(); k++)
        if(!dejavu[clef.charAt(k)-'A']){
            dejavu[clef.charAt(k)-'A'] = true;
            carre+=clef.charAt(k);
        }
    for(int k=0; k<dejavu.length; k++)
        if(!dejavu[k] && k!=22) % pas de 'W'
            carre+=(char)('A'+k);
    return carre;
}
```

1. Éditer ce code pour que le résultat se présente sous une forme effectivement carrée.
2. Choisir un mot de code (en majuscule et sans `'W'`) et lui appliquer la méthode `carre`.

Pour chiffrer un message avec un tel carré, on prend les lettres deux par deux et on applique ces règles :

- si les deux lettres sont identiques (ou s'il n'en reste qu'une) mettre un `'X'` après la première lettre, puis chiffrer la nouvelle paire ainsi constituée ;
- si les lettres se situent sur une même ligne du carré, les remplacer par celles qui sont immédiatement à leur droite (en bouclant sur la gauche si le bord est atteint) ;
- si les lettres se situent sur une même colonne du carré, les remplacer par celles qui sont juste en-dessous (en bouclant par le haut si le bas du carré est atteint) ;
- sinon, remplacer les lettres par celles se trouvant sur la même ligne, mais dans le coin opposé du rectangle défini par la paire originale.

3. Chiffrer le message « `AUCUNDOCUMENTAUCUNEMACHINEPOURLEXAMENDEPFUN` ».
4. Expliquer en quoi ce principe est plus robuste à la cryptanalyse que ceux des exercices **2** et **3**.
5. Écrire les méthodes de chiffrement et de déchiffrement.

**Exercice 5** On considère un système cryptographique réalisant quelques opérations élémentaires sur les bits constituant un caractère à transmettre : les bits de rangs pairs restent inchangés et les bits de rangs impairs sont mélangés à l'aide d'un *ou-exclusif* avec les bits de rangs pairs, de sorte que le bit de rang $2p+1$ du résultat est égal au ou-exclusif du bit $b_{2p+1}$ du message d'origine et du bit $b_{2p}$ à sa droite.

1. Comparer les fonctions de chiffrement et de déchiffrement.

Le message chiffré (exprimé en hexadécimale) est le suivant :

```
00ec 00eb 00ec 00ef 00d2 00e5 00dc.
```

2. Déchiffrer chacune des valeurs binaires.
   Sachant que `'a'` correspond à `0061`, donner le message en clair.
3. Écrire les méthodes de chiffrement *et* de déchiffrement.

**Exercice 6** Pour échanger via un système symétrique, Alice et Bob doivent partager une clé secrète.

1. Rappeler le principe de Diffie-Hellman (au moyen de couleurs ou d'entiers).
2. En supposant qu'elle puisse intercepter les messages entre Alice et Bob (en se faisant passer pour un routeur incontournable par exemple), expliquer comment Eve peut s'immiscer dans leur échange.

**Exercice 7** Alice et Bob s'accordent sur le système de chiffrement asymétrique RSA.

1. Alice choisit $n = 221$. Calculer $\varphi(n)$ et vérifier qu'elle peut choisir $e = 7$ comme exposant.
2. Préciser alors la clé publique que doit utiliser Bob et chiffrer le message $m = 3$ avec cette clé.
3. Calculer l'exposant $d$ et préciser la clé privée d'Alice. Déchiffrer alors le message reçu $c = 2$.
4. Proposer un moyen pour Alice de signer numériquement un message $h$ à l'attention de Bob.