Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Arithmétique modulaire et R.S.A

Exercice 1 :
1) Ecrire la table de multiplication dans $\mathbb{Z}/\mathbb{Z}_{26}$.
2) Quels sont les chiffrements linéaires inversibles dans $\mathbb{Z}/\mathbb{Z}_{26}$?

Exercice 2 :
Utiliser l'algorithme d'Euclide étendu pour calculer les inverses suivantes :

1. $17^{-1} \bmod 101$
2. $357^{-1} \bmod 1234$
3. $7690^{-2} \bmod 9987$

Exercice 3 :
Des personnes sont sur un bateau de croisière. Pour déjeuner, elles sont groupées par table de 25 et douze personnes se retrouvent sur la dernière table. Dans les canots de 26 places, neuf personnes seules se répartissent dans le dernier canot. Pour les visites par groupe de 27, vingt-trois personnes forment le dernier groupe. Quel est le nombre de personnes sur le bateau (au minimum)?

Exercice 4 :
Résoudre le système suivant :

$$\begin{cases} 13x & \equiv & 4 & (\text{mod } 99) \\ 15x & \equiv & 56 & (\text{mod } 101) \end{cases}$$

Indication : Utiliser d'abord l'algorithme d'Euclide étendu, puis le théorème des restes chinois.

Exercice 5 :
Retrouver l'inverse modulo 26 de la matrice

$$\begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}$$

Exercice 6 : Chiffrement de Hill
Le chiffrement de Hill est basé sur le produit d'une matrice-clef K par un vecteur clair M : $C = K \cdot M \pmod{26}$. Le vecteur clair sera de taille fixe n (on prend les lettres du clair par bloc de n lettres représentées par les nombres de 0 à 25). La matrice carrée de la taille du vecteur clair sera secrète. Le produit obtenu sera un bloc de taille n du vecteur chiffré.

1. Chiffrer le texte 'JOUR' avec la matrice $\begin{pmatrix} 1 & 4 \\ 5 & 3 \end{pmatrix}$.
2. Déchiffrer le texte 'PVGT' avec cette même matrice.
3. Supposons que l'on sache que le texte clair

   `conversation`

   donne le texte chiffré

   `SUDOOLOSZHIB`

   par le chiffrement de Hill (dont la taille de la matrice n'est pas spécifiée). Déterminer la clé utilisée.

Exercice 7 : RSA [Stinson 5.15]
Cet exercice présente un exemple d'*échec de protocole*. Il montre un exemple dans lequel un texte chiffré peut être décrypté par un opposant sans déterminer la clef, à cause d'une mauvaise utilisation du système cryptographique. La morale est qu'il n'est pas suffisant d'avoir un système cryptographique "sûr" pour garantir la confidentialité de la communication. Supposons que Bob utilise le chiffrement RSA avec n (modulo) assez grand pour qu'il soit impossible de le factoriser.

Supposons qu'Alice envoie à Bob un message, dans lequel chaque caractère alphabétique, représenté par un nombre de 0 à 25 (avec `A` correspondant à 0, `B` à 1, etc), est chiffré séparément.
a) Décrire comment Oscar peut facilement décrypter un message chiffré de cette façon.
b) Illustrer l'attaque en décryptant le texte chiffré suivant (qui a été chiffré avec RSA avec $n = 18721$ et $e = 25$) sans factoriser le modulo :

```
365,0,4845,17173,1437,1437,0
```

Quelle(s) lettre(s) allez-vous calculer en premier?

Exercice 8 : Exponentiation rapide
a) Déterminer le nombre maximal de multiplication qu'il faut effectuer avec cette méthode pour calculer x^n.
b) Calculer $3^{5032} \bmod 50$.

Exercice 9 :(Attaque cyclique)
Soit (n, e) une clef publique RSA. Pour un message clair $m \in \{0, 1, \ldots, n-1\}$, soit $c = m^e \bmod n$ le chiffré correspondant. Prouver qu'il existe un entier positif k avec

$$m^{e^k} \equiv m \bmod n.$$

Pour un tel entier k, prouver que

$$c^{e^{k-1}} \equiv m \bmod n.$$

Est-ce dangereux pour RSA? Soient $n = 493$ et $e = 3$. Déterminer la plus petite valeur de k pour laquelle l'attaque cyclique marche.

Exercice 10 : On construit un système RSA à partir de deux nombres premiers jumeaux $(p, q = p + 2)$.
1) Peut-on trouver un couple de nombres suffisamment grands pour assurer la sécurité du système?
2) Quelle attaque peut-on effectuer sur le module sachant que sa décomposition est à base de nombres jumeaux? Essayer avec $n = 4112783$.