Exercice 11 Chiffrement RSA
Alice publie sa clé publique n = 187 et e = 7.

(a) Encoder le message m = 15 avec la clé publique d' Alice.

- Formule du Chiffrement: $C \equiv m^e (\mod n)$
  - Message en clair: $m = 15$
  - Message Chiffré: $C =?$ (à déterminer)
  - $e = 7$
  - $n = 187$
- Application numérique: $C \equiv 15^7 (\mod 187) \rightarrow \mathbf{C = 93}$

(b) En utilisant le fait que $\varphi(n) = 160$, retrouver la factorisation de n, puis la clé privée d'Alice.

- On utilise **le Théorème de Bezout**:

Théorème 1. Deux entiers relatifs a et b sont premiers entre eux (si et) seulement s'il existe deux entiers relatifs x et y tels que $a \times x + b \times y = 1$

- On transpose dans notre problème: $e \times u + \varphi(n) \times v = 1 \rightarrow 7 \times u + 160 \times v = 1$
- Méthode de Résolution : **Division Euclidienne** !
  - $160 = 7 \times 22 + 6$
  - $7 = 6 \times 1 + 1 \rightarrow (1 = ax + by) \rightarrow 1 = 7 - (6 \times 1)$
    - ∗ On isole le **1** et on retrouve l'equation : $\mathbf{1} = 7 \times u + 160 \times v$ (Bezout)
- Il suffit de reprendre notre division à partir de $1 = 7 - (6 \times 1)$:
- $1 = 7 - (6 \times 1)$
  - sachant que $6 = [160 - (7 \times 22)]$
- $1 = 7 - [160 - (7 \times 22)] \rightarrow 1 = (7 \times 23) - (160 \times 1)$
- $(7 \times 23) - (160 \times 1) \rightarrow$ equation du théorème de Bezout retrouvée
  - Si u = d alors $d.e \equiv 1 \mod \varphi(n)) \rightarrow d \times 7 = 1 + k \times 160$ (k entier)
  - u respecte cette condition donc d=23
- Verification: en utilisant la formule du Déchiffrement: $m \equiv C^d (\mod n)$
  - Message en clair: $m =?$ (à déterminer)
  - Message Chiffré: $C = 93$
  - $d = 23$
  - $n = 187$
- Application numérique: $C \equiv 93^{23} (\mod 187) \rightarrow m = 15$
- On retrouve bien la valeur de m donnée dans la question a)

Exercice 12 Chiffrement/Attaques RSA

(a) Le pirate peut-il pirater la clé d'Alice
- Oui, il suffit de chercher les nombres premiers entre 2 et $\sqrt{1073}$
  - Message en clair: $m = 15$
  - Message Chiffré: $C =?$ (à déterminer)
- Réponse: p = 37 et q = 29
- $e.d \equiv 1(\mod 1008)$
  - $e = 73$
  - $\varphi(n) = 1008$
- On a : $73 \times d \equiv 1(\mod 1008)$
  - $d =?$ (à déterminer)
- On utilise **le Théorème de Bezout**:
- On obtient : $73 \times u + 1008 \times v = 1$
- Méthode de Résolution: Division Euclidienne !
  - $1008 = 73 \times 13 + 59$
  - $73 = 59 \times 1 + 14$
  - $59 = 14 \times 4 + 3$
  - $14 = 3 \times 4 + 2$
  - $3 = 2 \times 1 + 1 \rightarrow (1 = a \times x + b \times y) \rightarrow 1 = 3 - (2 \times 1)$
    - ∗ On isole le 1 et on retrouve $1 = 73 \times u + 1008 \times v$ (Bezout)
- Il suffit de reprendre notre division à partir de $1 = 3 - (2 \times 1)$:
- $1 = 3 - (2 \times 1)$
  - sachant que $14 = 3 \times 4 + 2 \rightarrow 2 = [14 - 3 \times 4]$
- $1 = 3 - 1 \times [14 - (3 \times 4)] \rightarrow 1 = (3 \times 5) - 14$
- $1 = (3 \times 5) - 14$
  - sachant que $59 = 14 \times 4 + 3 \rightarrow 3 = [59 - (14 \times 4)]$
- $1 = [59 - 14 \times 4)] \times 5 - 14 \rightarrow 1 = (5 \times 59) - (14 \times 21)$
- $1 = (5 \times 59) - (14 \times 21)$
  - sachant que $73 = 59 \times 1 + 14 \rightarrow 14 = [73 - 59]$
- $1 = (5 \times 59) - ([73 - 59] \times 21) \rightarrow 1 = (26 \times 59) - (21 \times 73)$
- $1 = (26 \times 59) - (21 \times 73)$
  - sachant que $1008 = 73 \times 13 + 59 \rightarrow 59 = [1008 - (73 \times 13)]$
- $1 = (26.[1008 - (73 \times 13)]) - (21 \times 73) \rightarrow 1 = (26 \times 1008) - (73 \times 359)$
- $1 = (26.1008) - (73 \times 359) \rightarrow u = (-359) et v = (26)$
  - Si u = d alors $d \times e \equiv 1 \mod \varphi(n)) \rightarrow d \times e = 1 + k \times 1008$ (k entier)
  - De plus, il faut $0 < d \leqslant \varphi(n) - 1$
  - L'astuce consiste à résoudre $d \equiv u \mod \varphi(n) \rightarrow d = -359 + k.1008$
- Avec k=1, nous avons **d=649** tout en respectant $d.e \equiv 1 \mod \varphi(n))$

(b) Le pirate a sniffé le réseau et a trouvé le texte chiffré: 423 (Hex). Quel est le message échangéé entre Alice et Bob?
- Conversion de $C = (423)_{HEX}$ en base 10 (décimale) : $\boldsymbol{C = (1059)_{DEC}}$
- Verification en utilisant la formule du Déchiffrement: $\boldsymbol{m \equiv C^d(\mod n)}$
  - Message en clair: $\boldsymbol{m =?}$ (à déterminer)
  - Message Chiffré: $\boldsymbol{C = 1059}$
  - Message Chiffré: $\boldsymbol{d = 649}$
  - Message Chiffré: $\boldsymbol{n = 1073}$
- Application numérique: $\boldsymbol{m \equiv 1059^{649}(\mod 1073) \rightarrow m = 97}$
- 97 en ASCII correspond à la lettre $\boldsymbol{a}$.

The End.