Exercice

On souhaite chiffrer le mot de passe d'une application web (hébergée sur un serveur distant) à des fins pédagogiques.

Message clair (exemple) :

`P@ssw0rd`

Table de codage, à utiliser pour encoder le mot de passe :

- `a → 00, b → 01, …, z → 25`
- `A → 26, B → 27, …, Z → 51`
- `0 → 52, 1 → 53, …, 9 → 61`
- `@ → 62, $ → 63, ! → 64, - → 65, _ → 66`

Paramètres RSA:

p=101,q=103,e=7.

Travail demandé :

1. Calculer **n**, **φ(n)** et la clé privée **d**.
2. Déterminer la taille maximale k (nombre de caractères par bloc) que l'on peut encoder dans un entier M tel que M<n. Justifier.
3. Encoder le mot de passe selon la table, découper en blocs de k caractères, transformer chaque bloc en entier M, puis chiffrer chaque bloc `P@ssw0rd`
4. Déchiffrer chaque bloc avec d et reconstituer le mot de passe.

Exercice : Partage de clés secrètes par Diffie-Hellmann

On considère que deux utilisateurs, **Alice** et **Bob**, souhaitent établir une clé secrète commune grâce au protocole Diffie–Hellman.

On choisit des paramètres publics :

- Un nombre premier : p=23
- Une base (générateur) : g=5

Alice choisit un secret privé Xa=6 & Bob choisit un secret privé Xb=15b.

1. Calculer la clé publique d'Alice Ya
2. Calculer la clé publique de Bob Yb
3. En utilisant la clé publique reçue :
    - Calculer la clé commune obtenue par Alice Kab
    - Calculer la clé commune obtenue par Bob Kba
4. Vérifier que la clé partagée est identique :

Exercice : Diffie–Hellman et Attaque de type MITM

Alice et Bob veulent établir une clé secrète via Diffie–Hellman.
Les paramètres publics sont :

- Nombre premier : p=29
- Générateur :g=7

Alice choisit un secret privé Xa=6 & Bob choisit un secret privé Xb=15.

Un attaquant **Darth** intercepte les messages.

Darth va effectuer une attaque **Man-In-The-Middle** (MITM) au processus d'échange de clés (les secrets de Darth sont respectivement : d1=4 & d2=7)

1. Calculer les clés publiques de Alice, Bob et Darth
2. Calculer les clés partagées
3. Expliquer pourquoi l'attaque MITM fonctionne sur Diffie–Hellman sans authentification**.**
4. Donner au moins deux moyens de protéger Diffie–Hellman contre le MITM.