Baptiste Cottier
baptiste.cottier@ens.fr

TP Crypto - Python

INSA - Hauts de France
28 Septembre 2022

Le TP décrit la résolution d'un challenge RootMe. Bien que soit fourni avec ce TP un jeu d'input, libre à vous d'utiliser votre propre input afin d'obtenir le flag.

1 – Dans un premier temps, implémenter l'algorithme d'Euclide étendu décrit ci-dessous:

function extended_gcd(a, b)
  $(r', r) := (a, b)$
  $(u, s) := (1, 0)$
  $(v, t) := (0, 1)$
  while $r \neq 0$, **do**
    $q := r'/r$
    $(r', r) := (r, r' - q \times r)$
    $(u, s) := (s, u - q \times s)$
    $(v, t) := (t, v - q \times t)$
  return (u, v)

Le contexte de l'attaque est le suivant : vous venez d'intercepter trois messages c_1, c_2, c_3 chiffrés avec le cryptosystème RSA dont les clés publiques utilisées pour les chiffrer sont respectivement $(N_1, e), (N_2, e), (N_3, e)$.

2 – Réécrire l'énoncé comme un système de la forme :

$$\begin{cases} \alpha \equiv \beta_1 \mod \gamma_1 \\ \alpha \equiv \beta_2 \mod \gamma_2 \\ \alpha \equiv \beta_3 \mod \gamma_3 \end{cases} \tag{1}$$

On va à présent utiliser le Théorème des Restes Chinois pour calculer α à partir du système d'équations.

Pour convertir les fichiers `.pem` en integer, vous pouvez utiliser la libraire Crypto.PublicKey.

3 – On définit $\hat{\gamma_i} = \dfrac{\gamma_1 \times \gamma_2 \times \gamma_3}{\gamma_i}$. Utiliser l'algoritme d'Euclide éténdu afin d'obtenir u_i pour $i \in \{1, 2, 3\}$ tels que $u_i \cdot \hat{\gamma_i} + v_i \cdot \gamma_i = 1$.

4 – Calculer $\sum_{n=1}^{3} \beta_i \cdot u_i \cdot \hat{n_i}$ pour obtenir une solution du système (1).

5 – En déduire le message envoyé.