Solution à : R1R2.

Le script fourni par l’énoncé (encrypt.py) montre le mot de passe chiffré / encrypté à la fin.

1. **Séparation du mot de passe** : (rechargement de l’empreinte HEX\_CIPHER (HEXA)).  
   password[::2] → b (caractères d’indice pair), password[1::2] → c (indices impairs).
2. **Transformation en entiers** : b\_int, c\_int = int.from\_bytes(..., 'big') puis on impose b\_int > c\_int.
3. **Constantes utiles** :
   * d = b\_int + c\_int
   * e = b\_int \* c\_int
4. **Trois couples (x, y) sont publiés** :  
   y = x² − d·x + e.  
   Chaque couple est sérialisé dans 1023 bits via la fonction-ci (1 bit de signe, 511 bits pour |y|, 511 bits pour x) puis *padded* sur 128 octets.

Connaître trois couples (x, y) suffit donc à retrouver d et e (verrou de degré 2), puis b\_int et c\_int (via les racines d’un polynôme), et enfin le mot de passe original par un entremêlement des deux moitiés. Le flag est concaténation des 2.



