|  |
| --- |
| **Github（或者Coding）账号：https://github.com/eric-huyl** |
| **个人博客关于密码学实验的链接：crypto repo的GitHub pages，待建** |
| **实验题目（中文）：密码学实验三** |
| **实验摘要（中文）：**  关于密码学实验的说明   1. 密码学实验将进行四次，每次实验，需按要求上传提交代码截图、相关结果等。 2. 请建立自己的技术博客或者其它记录载体，简单记录每次实验内容，所遇到的问题以及心得（建议）。 3. 因学校要求提交实验报告以给出成绩，我们只交一次纸质版实验报告，内容4次实验任选。 4. 最终提交时间11月30日晚23:00前。 5. 请建立自己的代码托管账号，Github或Coding或其他托管平台均可，建立合理的文件目录托管代码，请清晰命名，给出必要注释； 6. 电子版提交学在西电，提交pdf版附件命名“姓名\_学号\_密码学实验”。   用代码实现RSA的部分数学过程 |
| **题目描述（清楚描述题目中文，写出自己的理解，请勿复制原题目）**   * + - 1. **PE p182**   **给定pq，选定e，找出对应的未加密消息的数量，在所有e中找出这样的e并求和。**   * + - 1. **Implement RSA Cryptopals 39**   **实现自己的模逆运算，最后逐步实现整个RSA的加解密过程** |
| **过程（包括背景，原理：必要的公式，图表；步骤，如有必要画出流程图，给出主要实现步骤代码）**  **PE**  **直接暴力搜索e，然后对于e暴力搜索未加密消息数量即可。**  **import math**  **import sys**  **P = 1009**  **Q = 3063**  **N = P \* Q**  **A = (P - 1) \* (Q - 1)**  **def find\_coprimes():**  **coprimes = []**  **for e in range(1, A):**  **if math.gcd(e, A) == 1:**  **print(f'Find e:{e}')**  **coprimes.append(e)**  **return coprimes**  **def check\_non\_encrypted(e) -> int:**  **sum = 0**  **for m in range(0, N - 1):**  **if pow(m, e, N) == m:**  **print(f'Find non-encrypted: m:{m} e:{e}')**  **sum += 1**  **return sum**  **def main():**  **e\_list = find\_coprimes()**  **with open('p3\_1.out', 'w') as f:**  **for e in e\_list:**  **sum = check\_non\_encrypted(e)**  **f.write(f'e: {e},sum: {sum}')**  **main()**  **Cryptopals Set 5 Challenge 39**  **不难，按步骤实现即可**  **def extended\_gcd(a, b):**  **# 扩展欧几里得算法，返回 (gcd, x, y)，使得 a \* x + b \* y = gcd(a, b)**  **if b == 0:**  **return a, 1, 0**  **gcd, x1, y1 = extended\_gcd(b, a % b)**  **x = y1**  **y = x1 - (a // b) \* y1**  **return gcd, x, y**  **def mod\_inverse(e, phi\_n):**  **gcd, x, y = extended\_gcd(e, phi\_n)**  **if gcd != 1:**  **raise ValueError(f"{e} 和 {phi\_n} 不是互质的，无法求模逆")**  **else:**  **return x % phi\_n # x 可能是负数，取模确保结果为正数**  **# 示例**  **e = 17**  **phi\_n = 40 # 假设某个 n 的欧拉函数值**  **d = mod\_inverse(e, phi\_n)**  **print(f"e = {e} 的模逆 d = {d}（mod {phi\_n}）")** |
| **总结（完成心得与其它，主要自己碰到的问题和解决问题的方法）**  **不太难，比之前几次好多了** |
| 参考文献（包括参考的书籍，论文，URL等，很重要）<https://chatgpt.com/?model=auto> |