資訊安全導論 HW4

B10815057 廖聖郝

產生key

首先生成兩個在bit範圍內的隨機質數p q

用p q算出n與phi\_n

公鑰e是隨機的從範圍(2~phi\_n)內挑出一個與phi\_n互質的數字

挑法: 1.生成隨機數 2.若為偶數 +1變奇數 3.判斷是否互質 不互質找下一個奇數

私鑰d是公鑰e在模phi\_n下的模反元素，因此解此式 (e\*d) mod phi\_n == 1，我使用python的pow函式內建的模反計算(第二個參數設為-1)



質數生成: 1.生成隨機數 2.若為偶數 +1變奇數 3.判斷是否為質數 不是的話往下一個奇數找



判斷質數: miller robin演算法 [米勒-拉賓質數判定法 - 維基百科，自由的百科全書 (wikipedia.org)](https://zh.wikipedia.org/zh-tw/%E7%B1%B3%E5%8B%92-%E6%8B%89%E5%AE%BE%E6%A3%80%E9%AA%8C)



判斷互質: 1.判斷輸入ab大小 大的放第一個參數 2.求ab最大公因數 若為1則互質



加密

輸入一訊息，與n和公鑰，回傳加密後數字的base64編碼



RSA加密，輸入一待加密數字與n和公鑰，回傳加密後數字

求: (plain\_num ^ 公鑰) mod n



fast\_power\_mod即為square and multiply演算法

將次方數轉為二進制，掃過所有bit，遇0則square，遇1則square與multiply



解密

輸入加密後的base64編碼，與n和私鑰，回傳解密後原始訊息



RSA加密，輸入一加密後數字與n和私鑰，回傳原始數字

求: (cipher\_num ^ 私鑰) mod n



CRT解密

輸入加密後的base64編碼，與p與q和私鑰，回傳解密後原始訊息



RSA加密，輸入一加密後數字與p與q和私鑰，回傳原始數字

採用中國剩餘定理加速



結果

Key gen:

一張含有 文字 的圖片

自動產生的描述

加密:

一張含有 文字 的圖片

自動產生的描述

解密:

一張含有 文字 的圖片

自動產生的描述