实验 2：RSA 加密算法实现

实现 RSA 加密算法，要求如下：

1 利用 **Miller-Rabin 测试**生成两个 256（或 512）比特的素数, p,q.

记录素数生成的时间.

2 计算 $n = pq$. 利用 **Euclidean 算法**生成与 $\phi(n)$ 互素的整数 a 作为私钥, 利用**扩展 Euclidean 算法**计算 $b = a^{-1}$ 作为公钥.

3 随机生成明文 $m \in Z_n$, 利用**平方乘积（Square and Multiply）算法**计算密文

$$c = m^b \bmod n,$$

并进行解密运算

$$m' = c^a \bmod n,$$

检验解密的正确性，即 $m = m'$ 是否成立.

4 记录一组明文的 RSA 加密和解密时间.

使用 DES 对相同的明文进行加解密，记录 DES 加密和解密时间.

（建议选取 10 组以上明文，对比这些明文加密时间**总和**.）

5 RSA 算法正确性检验：请依据下面的实验结果检验程序的正确性.

EXAMPLE

Suppose Bob chooses $p = 101$ and $q = 113$. Then $n = 11413$ and $\phi(n) = 100 \times 112 = 11200$. Bob chooses $b = 3533$. Then,

$$b^{-1} \mod 11200 = 6597,$$

and Bob's secret decryption exponent is $a = 6597$.
Bob publishes $n = 11413$ and $b = 3533$. Now, suppose Alice wants to encrypt the plaintext 9726 send to Bob. She will compute

$$9726^{3533} \mod 11413 = 5761$$

and send the ciphertext 5761 over the channel. When Bob receives the ciphertext 5761, he uses his secret decryption exponent to compute

$$5761^{6597} \mod 11413 = 9726.$$