



# A Web Demo of RSA Public Key Cryptography Algorithms

An accompanying learning material for students of cryptography

Student: Andy Tan Ying Kun

Supervisor: Assoc Prof Anwitaman Datta

A step-by-step visualization  
of 3 computational  
subsystem.

- Miller-Rabin Primality Test
- Multiplicative Inverse  
Computation Through  
Extended Euclidean  
Algorithm
- RSA Algorithm

Home Primality Test Multiplicative Inverse Computation

### Miller Rabin Primality Test

21

Number of repeated use of Primality test

3

21 is not a prime number

Step 1: Find Integers  $k, q$ , with  $k > 0, q$  odd, so that  $(n - 1) = 2^k q$

Show Steps  $\oplus$

\*If test return composite at any point, the number is not a prime number.

Running Miller Rabin Primality Test for 3 times.

Primality Test 1 return composite. Ending Test...

Show Steps  $\oplus$

Home Primality Test Multiplicative Inverse Computation

### RSA Encryption and Decryption

Enter plain text to be encrypted and decrypted

Enter 1st prime number [p]: 8429

Enter 2nd prime number [q]: 53

Proceed with RSA Algorithms:

Home Primality Test Multiplicative Inverse Computation

### Computation of Multiplicative Inverse Using Extended Euclidean Algorithms

Calculating Multiplicative Inverse of b

Using the Extended Euclidean Algorithm we can establish the Bézout's identity, namely:  $ax + by = d = \gcd(a,b)$

If  $\gcd(a,b) = 1$ , the Multiplicative Inverse  $b^{-1} \pmod a = y$

26   $^{-1} \pmod$  63