

## **Worksheet 5: RSA Public Key Encryption**

Name:	
Class:	

**Please complete this worksheet and print it out.**

**Author:** J.Jackson/W.Buchanan

### Objectives

This exercise is based on a simple calculation aid for the RSA algorithm. Use the supplied program to do some calculations which would be time consuming with a calculator.

### Practical

<b>a) Choose a pair of prime numbers (a, b)</b>
-------------------------------------------------

<p>Use the &lt;P&gt; option of the program to search for a prime number. For this exercise the primes should not be too large (say &lt;500). When two suitable primes have been found enter the values of a (p), b (q), n and x (PHI) below.</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Prime number $a$ ( $p$ )=	
Prime number $b$ ( $q$ )=	
Product of primes $n=a \times b$ =	
$x$ ( $PHI$ )= $(a-1) \times (b-1)$ =	

**b) Choose a Public Key Exponent (E)**

Choose a number which is not a factor of  $x$  and is not in common with  $x$ . For example, if  $x=10948$  then 52 would not be a suitable value for  $E$  since both 10948 and 52 are divisible by 4. For ease of calculation here, choose a small number ( $<100$ ) for which all the factors are known.

Public Key $(E,n)=$		
---------------------	--	--

**c) Find the Private Key Exponent (D)**

Use the program to calculate the value for the Private Key Exponent.

Private Key $(D,n)=$		
----------------------	--	--

Try out some more values, and complete the table below:

Prime number $a=$			
Prime number $b=$			
Product of primes $n=a \times b=$			
$x=(a-1) \times (b-1)=$			
Public Key $(E,n)=$			
Private Key $(D,n)=$			

**References**

Program can be downloaded from:

[http://www.dcs.napier.ac.uk/~jimj/course\\_notes/ee42001/rsademo.exe](http://www.dcs.napier.ac.uk/~jimj/course_notes/ee42001/rsademo.exe)

or

[http://www.dcs.napier.ac.uk/~bill/c\\_rsa.htm](http://www.dcs.napier.ac.uk/~bill/c_rsa.htm)