Cryptography: Public-key encryption activity

Activity 1: Generating keys using small integers

In Activity 1 we use modular product tables to generate our modular inverses.

1. First complete the following modular five (M-5) multiplication table:

M5	0	1	2	3	4
0					
1					
2					
3					
4					

2. Now complete this modular nine (M-9) multiplication table:

M9	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

You will first simulate public key encryption using the second table above: the modular nine multiplication table. Your first 'message' must be restricted to an integer between 1 and 8.

Choose your keys

1. Your **Public key** is the modular multiplication table used. Here it is 9.
2. Pick two integers from the table whose mod product is 1 (eg 4 and 7).
   a. Your **encryption key** is the first integer. **Encryption key**
   b. Your **decryption key**, or **private key** is the second integer. **Decryption key**

   You can tell others your public and encryption keys but your decryption key is kept private!

Sending and decoding the secret message

1. **How to encrypt:**
   a. Choose a 'message' for secret transmission (here it needs to be restricted to an integer between 1 and 8). This is the **message** which we will represent as an integer. **Message (in the form of an integer)**
   b. Using the modular multiplication table find M-product of the message integer and their encryption key. This result is the **encoded secret message**. **Encryption key**
2. **How to decrypt:**
   Use the M9 table to find the M-product of the decryption (private) key and the encrypted message. This is the decrypted message, known only to those who have the private key. **The decrypted message**

Real-life encryption with public and private keys also uses modular arithmetic. However, we know the table and we know there are very few choices for the multiplicative modular inverses.

It would not be hard for someone to guess our message. In real life, encryption used for far larger numbers would be very hard to guess.

In the next Activity we will use much larger numbers.