|  |
| --- |
| **Step 1:** go to <https://mathymcmatherson.github.io/RSA_Activity/rsa.html> . Give it 30 seconds to load (there are lots of prime numbers less than 10,000 – it takes a while to load all of them) |
| **Step 2:** Choose two Prime Numbers from the dropdown menus. The website will automatically tell you your **Public Modulus**  **My Public Modulus:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Note: your public modulus must be at least 4 digits for the activity we’re doing today) |
| **Step 3:** Choose your **Public Key**, but don’t pick any of the numbers in the list. If your public key is accepted, some green text will appear.  **Your Public Key:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Step 4:** The website will *also* automatically generate your **Secret Key** (you need to hover over a button to see it). Write this below, but keep it a secret! Don’t let anyone else see it!  **My Secret Key:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Right Now:** Write your public information on this Padlet site: *[[Replace this with your Padlet site]]* . |
| Use the space below to record your list of contacts from people who have also posted on the Padlet website. You must fill every box, even if you don’t get a chance to send a message to everyone  **My Contact List**   |  |  |  | | --- | --- | --- | | **Name** | **Public Key** | **Public Modulus** | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |
| **Step 5:** Use the public information to send the first 3 digits of your phone number to each of the people above.  Use the Python Program to do this calculation and generate your *encrypted* number. Once you have your encrypted number, write it on an index card and deliver it to this person. You should write *your name* on the index card too so they know who it came from.  **Example**  To: Schneider  From: [Your Name] Secret Message: 381723  When you are done, you should have several messages of your own to decrypt… |
| **Receiving Messages** |
| Hopefully you were also sent some messages during this activity. Time to decrypt them!  **To Decrypt:** Use the Python program to decrypt the messages  Record all of your messages here:   |  |  |  | | --- | --- | --- | | **From** | **Public Message** | **Decrypted Message** | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |