My public key is $n = 47,880,953$ and $e = 24,523$. I am encrypting text using groups of three letters encoded by `01=A`, `02=B`, `03=A`, and so on up to `26=Z`, and `27`=space. I use only letters and spaces (no distinction between uppercase and lowercase, and no punctuation). The "groups of three letters" is important; see the example, below.

An Example

This is an example of how one would encrypt a message using my public key $(e, n) = (24523, 47880953)$.

1. **The message in text:** We start with a phrase. For this example, we'll encrypt the phrase `CAT IN A HAT`. I first break it into managable chunks of three letters: `CAT`, `_IN`, `_A_`, and `HAT`.
2. **The message as a number:** These are converted to (unencrypted) numbers as `030120`, `270914`, `270127`, and `080120`. Thus the *plaintext* (unencrypted message) is:
$$\{030120, 270914, 270127, 080120\}$$
3. **The encrypted message as a number:** These are then *encrypted* using the RSA scheme:
$$\begin{aligned} 030120^e = 030120^{24523} &\equiv 5570542 \bmod n \\ 270914^{24523} &\equiv 8898498 \bmod n \\ 270127^{24523} &\equiv 2834110 \bmod n \\ 080120^{24523} &\equiv 22663854 \bmod n \end{aligned}$$
Thus the encrypted message or *cyphertext* is
$$\{5570542, 8898498, 2834110, 22663854\}.$$
4. **Decryption of the encrypted text:** I can recreate the plaintext from the cyphertext, since I know my private key (d, n). In order for you to recover the plaintext, you would either need to guess d (ha!), guess $m = \phi(n) = (p-1)(q-1)$ (ha! again), or factor $n = pq$. (This is simplifying things, of course. These are the *straightforward* options you have.)

Text To Decrypt

I have encrypted a short message using my private key. Use my public key (given above) to decrypt it. (This is part of homework 6; see that page for more information and challenges.) The encrypted text is:

$$\{20892288, 21817312, 9196332\}$$