

Exercise Set 4.**Due in Class on Monday, April 16**

Write as if this were part of your resume for a high-paying job you really want!

1. Decipher the ciphertext message

2771 1794 3187 1013 3228 1259

given that it was enciphered using an exponential cipher with $n = 2$, $p = 3373$, and $e = 95$.

2. Encipher VEE IS FOR VICTORY using an RSA cipher with $p = 61$, $q = 47$, $pq = 2867$, and $e = 17$. [Change the plaintext into numerical equivalents (AA-00, ..., Z-25, and group the digits into blocks of size 4 (add an X at the end of the message in order to have an even number of letters).]

3. In the field $GF(2^8)$ used in the AES, compute the following sum and product where elements are represented using hexadecimal:

$$\{2b\} + \{35\}$$

$$\{2b\} \times \{35\}.$$