Math/CS/ECE 435 Spring Semester 2000-01

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 $e = 95$.

THE END IS NEAR.

(The end of the semester, that is!)

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).]

2458 0300 0778 2732 1827 2608 2732 0129

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

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

In bytes this becomes 001011011+00110101 which, adding coefficients in $Z/2$ equals 00011110 or $\{1e\}$

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

Here we have $(x^5 + x^3 + x^2 + x) \times (x^5 + x^4 + x^2 + 1)\%(x^8 + x^4 + x^3 + x + 1)$ with coefficients in $Z/2$. The answer is

$x^4 + x^2 + x$ or in hexadecimal $\{16\}$.