1. [20 pt] Security has become an important topic. Explain how we expect better security to improve our interaction with others over the Internet.

2. [20 pt] Explain what each of the 4 steps in each round of AES does to the input message. How does each of those transformations work to hide the plaintext?

3. a. [15 pt] Bob wants to do RSA encryption. He has chosen his favorite primes 7 and 13, and the public exponent 5. Alfred wants to send the message 4 to Bob; find the ciphertext.

   Answer:
   \[ n = 7 \times 13 = 91, \quad \phi(n) = (p - 1)(q - 1) = 6 \times 12 = 72 \]
   \[ c = 4^5 \mod 91; \text{ note that } 4^4 = 256 \mod 91 = 74 \]
   \[ \text{So } c = 4^5 = 4^4 \times 4 = 74 \times 4 = 296 \mod 91 = 23 \]

3. b. [15 pt] Alfred has sent Bob a new message. The ciphertext is 3. Now find Bob’s secret key and use it to decrypt the ciphertext.

   Answer:
   We know that \( e \times d \equiv 1 \mod 72 \) so that 5d must be in the set 1, 73, 145, 217, \ldots;
   easily \( 5d = 145 \) and \( d = 29 \)
   Hence \( p = c^d = 3^{29} \mod 91 \)
   Note that \( 3^2 = 9; \quad 3^4 = (3^2)^2 = 9^2 = 81 = -10 \mod 91, \quad 3^8 = (-10)^2 = 100 = 9 \mod 91 \) and \( 3^{16} = 9^2 = 81 = -10 \mod 91 \)
   Thus \( p = 3^{29} = 3^{16+8+4+1} = 3^{16} \times 3^8 \times 3^4 \times 3^1 = (-10 \times 9) \times (-10 \times 3) = -90 \times -30 = 1 \times 61 = 61 \mod 91 \)


   Answer:
   Bob forms \( \beta = g^d = 6^5 \mod 13 \). Note that \( 6^2 = 36 = 10 \mod 13 \) and
\(6^4 = 10^2 = 100 = 9 \mod 13\). Hence \(\beta = 6^4 \times 6 = 9 \times 6 = 2 \mod 13\).

Bob’s public key is \((13, 6, 2)\).

4. b. [15 pt] Alice has sent Bob the ciphertext \((7, 8)\). What (numeric) message did she send?

Answer:
Bob forms \(m = 7^{-5} \times 8 = 7^{12-5} \times 8 \mod 13\) by Fermat’s Little Theorem. Hence \(m = 7^7 \times 8 = 7^4 \times 7^2 \times 8 = 9 \times 10 \times 8 = 90 \times 8 = 12 \times 8 \ 96 \mod 13 = 5\).