1. Recall the Hill cipher from class. Mallory steals Alice’s Hill cipher machine, which uses a 2 X 2 matrix \( M \mod 26 \). He uses a chosen plaintext attack and finds that the plaintext ba encrypts to DF and the plaintext zz encrypts to QI. What is the matrix \( M \)?

2. Calculate using repeated squaring method \( 13^{2014} \mod 23 \). Show all steps.

3. Compute the multiplicative inverse of 101 modulo 33 using the theorem given in class, i.e., the Extended Euclid algorithm. Show all steps. Explain also how do you know that it exists.

4. A gardener plants oak trees in rows of 5 and there is one left over. When he plants the same number of trees in rows of 7, three are left over. When he plants them in rows of 13, two are left over. What is the smallest number of oak trees possible. Solve using both methods explained in class.

5. Every pair of a group of \( n \) people wants to communicate confidentially using DES. How many total keys would have to be created? Suppose instead of DES, they switch to RSA. How many total keys would have to be created? Carefully derive your answers and explain the implications of the numbers.


7. A substitution cipher was used to produce the following ciphertext:

\[ XTHQTXJSTRFYJWMTBKFW \]

Can you decrypt the message? Explain your reasoning and the key drawback of the substitution cipher used.

8. Encrypt the plaintext message 01000100 twice, first with just the first stage of SimpleDES and then with the first four stages of SimpleDES. Use the key 10110100. Show all steps. Compare the two ciphertexts with respect to the confusion and diffusion criteria of Shannon.

Academic Honesty Policy: No collaboration with anyone or anything in or outside the course is allowed on any homeworks, exams and programming assignments (yes, that excludes the internet as well) except if it is explicitly allowed on a problem. The appropriate help of the instructor and (if applicable) the TA is of course allowed and encouraged.