Homework 2 – Due Tuesday

Samuel Montalbano

Mathematical Cryptography– 4/15/2025

Question 1 (1 pt)

Without using technology, compute $387 \cdot (703^{21} - 282) \mod 4$. In other words, find the smallest positive number that is congruent to the value(mod 4).

Solution:

Question 2 (2 pts)

Choose a passage of text, and encrypt it with a (nontrivial) affine cipher. In your answer, give me the plaintext, the value of the key, and the ciphertext Choose a passage of interest to you, but make sure it is appropriate to share with the class.
These will become part of a future assignment. Don't forget to post cipehrtext to the discussion.

- The plaintext
- The key (a, b)
- The ciphertext

Plaintext:

Key: ($a =$ _____, $b =$ _____)
Ciphertext:

Note: Post your ciphertext (without key or plaintext) on the class discussion board.

Question 3 (2 pts)

The following text was encrypted with an affine cipher, key(a,b) = (5,23). Decrypt it. Enter the plaintext in lowercase letters.
YRKL YLML YLHL

Ciphertext: YRKL YLML YLHL
Plaintext:

Question 4 (2 pts)

Ciphertext: NJLNRBNDBJNTDNPJJJ

- Explain why ($\alpha = 2, \beta = 1$) is a bad choice of key.
- Decipher the message.

Explanation:

Decrypted Message:

Question 5 (2 pts)

Decode the following using the affine cipher machine online:
`https://www.cs.du.edu/~ftl/affineplaintextattack.html`

Ciphertext: PAARCDJRWUDQCZKEDQVNDJHQD

Key: $(a = \_\_\_\_\_, b = \_\_\_\_\_)$

Plaintext:

Thought Process:

Question 6 (2 pts)

The word ”tiktok” encrypted using the affine cipher gives ”NWSNKS”. Find the key, then decrypt ”AKKT”.

Key: $(a = \_\_\_\_\_, b = \_\_\_\_\_)$

Plaintext of ”AKKT”:

Question 7 (4 pts)

Choose a classmate’s posted ciphertext and cryptanalyze it.

Ciphertext:

Thought Process and Steps:

Question 8 (2 pts)

Use the Extended Euclidean Algorithm iteratively to compute:

$$\gcd(a, b) \quad \text{(fill in appropriate values)}$$

Work:

You may paste an image of your handwritten work below if preferred.