Spring 2020-2021
Home
Assignments
Discussions
Grades
People
Pages
Files
Quizzes
Modules
Collaborations
Chat
BBCollaborate Ultra
Course Summary
Course Syllabus (AEFIS)
Kaltura My Media
Kaltura Gallery

Assessment for Homework 2

Started: Feb 10 at 9:30pm

Quiz Instructions

The majority of the problems below will continue with the assumption that the set of plaintexts and ciphertexts are the uppercase Roman alphabet of 26 characters (as per the Bach course notes), and may be encoded as Z_{26}. However, observe that Problem 1 considers the case of Z_{256}.

You are not required to submit any written work for this quiz, but it is strongly encouraged to work out the problems by hand.

Questions
Question 5
Question 6
Spacer
Question 7
Question 8
Spacer
Question 9
Question 10

Time Elapsed: Hide
Attempt due: Feb 12 at 5pm
1 Hour, 25 Minutes, 38 Seconds

Problem 1

a) Identify the prime factorizations of 49 and 256. Using this result, provide a short statement to justify the conclusion that gcd(256, 49) = 1. (aside: you can certainly employ MATLAB to compute gcd(256, 49); here your goal is to provide a short justification).

b) Based on (a), you have confirmed that 49 is an element of Z_{256}^{*}. Use the extended Euclidean algorithm to compute the multiplicative inverse of 49 in Z_{256}.

Question 1 — 1 pts

Find the numerical inverse of 49 in Z_{256}.

209

Problem 2

The ciphertext 'LMNYBJQZWGN' is known to have been encoded with an affine cipher. We know that the first two characters of the plaintext are 'IL'

Question 2 — 1 pts

Identify the values of a (multiplicative coefficient) and b (additive constant) used in the affine cipher.

$e_k(x) =$ 9 $x +$ 17

Question 3 — 1 pts

Identify all the characters of the full plaintext message.

ILOVECRYPTO

Problem 3

Consider a matrix with elements in Z_{26}, given by $M_1 = \begin{bmatrix} 9 & 2 \\ 13 & 3 \end{bmatrix}$

Question 4 — 1 pts

Compute the determinant in Z_{26}.

1

Question 5 — 2 pts

Find the inverse of M_1 in Z_{26}. $M_1^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$a =$ 3

$b =$ 24

$c =$ 13

$d =$ 9

Question 6 — 1 pts

Assume the matrix M_1 has been as a Hill cipher, block size 2, to encrypt a plaintext message; the resulting ciphertext is 'TZRUOOEZBW'

Identify the plaintext message.

HELLOWORLD

Consider the matrix $MM = \begin{bmatrix} 3 & 7 & 8 \\ 15 & 4 & 23 \\ 7 & 0 & 8 \end{bmatrix}$.

Question 7 — 1 pts

Compute its determinant.

3

Question 8 — 2 pts

Compute its inverse in Z_{26}. MM^{-1}

$MM^{-1} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$

$a =$ 2

$b =$ 16

$c =$ 17

$d =$ 5

$e =$ 24

$f =$ 17

$g =$ 8

$h =$ 25

$i =$ 21

The following ciphertext was the output of a shift cipher: 'LCLLEWLJAZLNNZMVYIYLHRMHZA'

Question 9 — 1 pts

By performing a frequency count, provide your "best guess" of the value of the key in Z_{26} used for this shift (i.e., identify the value you judge as having the highest probability of being correct).

7

Question 10 — 1 pts

What is the plaintext?

EVEEXPECTSEGGSFORBREAKFA