

Fall 2019 CIS 3362 Exam #1: Classical Cryptographic Schemes

Date: 9/23/2026

Name: _____

1) (8 pts) The ciphertext "XIRTVWLC" was encrypted via the shift cipher using an encryption key of 17. What is the corresponding plaintext?

2) (2 pts) What is the index of coincidence of the set of letters in the ciphertext from question #1? **Please answer as a fraction in lowest terms.** (This can be solved with almost no work.)

3) (6 pts) The encryption keys for an Affine Cipher are $a = 17$ and $b = 5$, what are the corresponding decryption keys. (Note: Please use the formula sheet to reduce the amount of manual computation as necessary.)

$a =$ _____ $b =$ _____

4) (10 pts) Determine the value of $83^{-1} \bmod 177$ via the Extended Euclidean Algorithm. (**Note: 1 pt for the correct answer, 9 points for the work using the steps shown in class.**)

5) (10 pts) The ciphertext "DNSKTXVYJVZVISBNLOZX" was encrypted via the Vigenere Cipher with the keyword "KNIGHTS". What is the corresponding plaintext?

6) (8 pts) The set X contains 10 As, 20 Bs, 50 Cs and 20 Ds. The set Y contains 30 As, 5 Bs, 10 Cs and 5 Ds. What is the mutual index of coincidence between the set X and the set Y. Please express your answer as a fraction in lowest terms.

7) (10 pts) Use the Hill cipher with the key $\begin{pmatrix} 11 & 4 \\ 7 & 5 \end{pmatrix}$ to encrypt the plaintext "HORSESHOES".

8) (4 pts) In every Enigma message, the day code was used to encrypt several characters.

(a) (2 pts) How many characters of every message were encrypted with the day code?

(b) (2 pts) What characters were encrypted in each message with the day code?

9) (10 pts) Decrypt the following ciphertext, which was created via column transposition with the keyword "VIGENERE". A grid is provided to help you out. **Note: There are 70 characters total (so you don't have to count); you need this information to decrypt.**

A T I W I I E D E T F W R E T H N S E I S T S E N D W S S E T H
S A K T E E H F C A E C S O T O M S W I N H T A S S H E G I B M
T O U C R I

10) (6 pts) The Navajo Code Talkers used one of three strategies to encrypt each word in a message, in a preferential order. (If possible, strategy #1 was used. If not, then strategy #2 was used. If not, then strategy #3 was used.) List each of the three strategies in the order that they were applied.

1. _____
2. _____
3. _____

11) (1 pts) What type of sweet treat can you buy at Night Owl Cookies? _____

Scratch Page – Please clearly mark any work on this page you would like graded.