

Sample problems - Prelim 1 - Math 1350 - Fall 2010

Note: A list of the letters and their numerical translations (A=0, B=1, ... , Z=25) will be on the exam.

1. You discover a cipher which you know is a shift cipher. However, all of it has faded with time and is unreadable, except a single two letter word. The two letter ciphertext is EZ. Is this enough to determine the shift? Explain.
2. Decipher the ciphertext

FALL

using an affine cipher with key $a = 3, b = 6$.
3. An affine cipher enciphers E as F and enciphers T as G. What letter does it encipher O as?
4. Find the indicated multiplicative inverse, or explain why it is not possible.
 - (a) $(5)^{-1}(\text{mod } 24)$
 - (b) $(8)^{-1}(\text{mod } 34)$
 - (c) $(-3)^{-1}(\text{mod } 26)$
5. Use a mixed alphabet keyword substitution cipher with keyword COCACOLA to decrypt the ciphertext ZGERC.

YUENO NPTUD LEFTA XOHIT
6. The following ciphertext was produced using a columnar transposition cipher. Decipher it.

TTOEW HTRSE IAIBM PSEEP NSFLO
7. Encipher the plaintext WHERE ARE YOU GOING using a keyword

columnar transposition with keyword BLUE.
8. Decipher the ciphertext LOGHNQLW using a Vigenère cipher with key WORD.

9. Two distinct whole numbers from 1 to 7 (inclusive) are chosen at random. What is the probability that their sum is congruent to 3 modulo 8?

10. Four friends compare what day of the week, Sunday, Monday, etc., their birthday is in 2011. Assuming that for any individual each of the seven days of the week is equally likely, what is the probability that at least two of them will be celebrating their birthday on the same day of the week? (You need only write down an arithmetic expression for your answer - do not compute it exactly.)

11. The following ciphertext was produced using a Vigenère cipher, with a key of length less than ten. Find the length of the key used. (You do not need to recover the plaintext.)

JGJBT QTIJN KXQEI DFIVF PIETI KCAUZ YVWQE HHSXL MQBDY
KXPDJ GJBTQ TIJNK XQEIN RVMGX URKRB JD

12. Write down a sentence with at least 10 letters and index of coincidence at most 0.02.

13. You are given a 200 letter cipher and told it is either a simple substitution, columnar transposition or Vigenère. Give a specific method for determining which type of encryption method was used that does NOT involve decrypting the cipher. Vague descriptions will get a vague amount of credit.