1172/DCP1323 Introduction to Cryptography, Spring 2019 **Due: 2019/3/4 (Mon.)**

Homework 1

Instructor: Prof. Wen-Guey Tseng Scribe: Hung-Yu Chiu

1. In this text, we assume that the modulus is a positive integer. But the definition of the expression a mod n also makes perfect sense if n is negative. Determine the following:
   a. 7 mod 4
   b. 7 mod -4
   c. -7 mod 4
   d. -7 mod -4

2. Find the multiplicative inverse of each nonzero element in Z_5.

3. Using the extended Euclidean algorithm, find the multiplicative inverse of 42828 mod 6407.

4. Use Fermat's theorem to find a number a between 0 and 92 with a congruent to 7^{1013} modulo 93.

5. Six professors begin courses on Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, respectively, and announce their intentions of lecturing at intervals of 3, 2, 5, 6, 1, and 4 days, respectively. The regulations of the university forbid Sunday lectures (so that a Sunday lecture must be omitted). When first will all six professors find themselves compelled to omit a lecture? *Hint*: Use the CRT.

6. The following ciphertext was generated using a simple substitution algorithm.

   hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf, wzsxz gqv zqhhnf ol ozn glco zlfnco hnlhrn; nsoznj jnrqosdnc lj fnqj kjsnfbc, wzsxz sc xnjoqsfrv gljn efeceqr. zn rsdnb qrlfn sf zsc zlecn sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb. q csfyrn blgncosx cekksxnb ol cnjdn zsg. zn pjnqmkqconb qfb bsfnb qo ozn xrep, qo zlejc gqozngqosxqrrv ksanb, sf ozn cqgn jllg, qo ozn cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznj gngpnjc, gexz rncc pjsfysfy q yenco wsoz zsg; qfb wnfo zlgn qo naqxorv gsbfsyzo, lfrv ol jnosjn qo lfxn ol pnb. zn fndnj ecnb ozn xlcv xzqgpnjc wzsxz ozn jnkljg hjldsbnc klj soc kqdlejnb gngpnjc. zn hqccnb onf zlejc leo lk ozn ownfov-klej sf cqdsrrn jlw, nsoznj sf crnnhsfy lj gqmsfy zsc olsrno.

Decrypt this message.
Hints:
1. As you know, the most frequently occurring letter in English is e. Therefore, the first or second (or perhaps third?) most common character in the message is likely to stand for e. Also, e is often seen in pairs (e.g., meet, fleet, speed, seen, been, agree, etc.). Try to find a character in the ciphertext that decodes to e.
2. The most common word in English is "the." Use this fact to guess the characters that stand for t and h.
3. Decipher the rest of the message by deducing additional words.
Warning: The resulting message is in English but may not make much sense on a first reading.

7. A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword CRYPTO, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

    plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
    cipher: C R Y P T O A B D E F G H I J K L M N Q S U V W X Z

    If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

    C R Y P T O
    A B D E F G
    H I J K L M
    N Q S U V W
    X Z

    This yields the sequence:

    C A H N X R B I Q Z Y D J S P E K U T F L V O G M W

    Such a system is used in the example in Section 3.2 (the one that begins "it was disclosed yesterday"). Determine the keyword.

8. **a**. Using this Playfair matrix:

J/K	C	D	E	F
U	N	P	Q	S
Z	V	W	X	Y
R	A	L	G	O
B	I	T	H	M

Encrypt this message:

I only regret that I have but one life to give for my country.

Note: This message is by Nathan Hale, a soldier in the American Revolutionary War.
b. Repeat part (a) using the Playfair matrix from Problem 3.10a.
c. How do you account for the results of this problem? Can you generalize your conclusion?

9. This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 . . . , then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.
a. Encrypt the plaintext sendmoremoney with the key stream

3 11 5 7 17 21 0 11 14 8 7 13 9

b. Using the ciphertext produced in part (a), find a key so that the ciphertext decrypts to the plaintext cashnotneeded.