1152/DCP1323 Introduction to Cryptography, Spring 2021 **Due: 2021/3/12(Friday)**

Homework 1

Instructor: Prof. Wen-Guey Tseng Scribe: Yu-Siang Chen

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. Using the extended Euclidean algorithm, find the multiplicative inverse of 7465 mod 2464
3. Use Fermat's theorem, find 4^{225} mod 13.
4. Use Euler's theorem to find a number x between 0 and 14 with x^{61} congruent to 7 modulo 15. (You should not need to use any brute-force searching.)
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.

   Warning: The resulting message is in English but may not make much sense on a first reading.

7. When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an

Australian wireless station in Playfair code.

KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBWT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

The key used was ***royal new zealand navy***. Decrypt the message. Translate TT into tt.

8. Encrypt the message “meet me at the usual place at ten rather than eight o clock”

   Using the Hill cipher with the key $\begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$. Show your calculations and the result.

9. Using the Vigenère cipher, encrypt the word “cryptographic” using the word “eng”

10. 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.

11. Use the Rabin-Miller primality test to test primality of 113 and 133.