1154/DCP1323 Introduction to Cryptography, Autumn 2021 **Due: 2021/10/5, 5pm (Tuesday)**

Homework 1

Instructor: Prof. Wen-Guey Tseng Scribe: Yi-Ann Chen

1. Compute the following:
   - **a.** 9 mod 4
   - **b.** -9 mod 4
   - **c.** 2718 mod 47
   - **d.** 3^{17} mod 25
   - **e.** $\text{dlog}_{7,25}\,18$
2. Using the extended Euclidean algorithm, find the multiplicative inverse of 7467 mod 2464.
3. Use Fermat's theorem to find 4^{225} mod 17.
4. Solve the equation $5 = x^{47} \bmod 18$ by the Euler's theorem.
5. Solve the system of equations:

$$\begin{cases} 3 = x \bmod 7 \\ 5 = x \bmod 11 \\ 2 = x \bmod 12 \end{cases}$$

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 am"

Using the Hill cipher with the key $\begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \\ 7 & 5 & 4 \end{pmatrix}$. Show your calculations and the result.

9. Using the Vigenère cipher, encrypt the word "cryptographic" using the word "hello".
10. Consider a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 25. 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 151 and 161.