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 = 1
   b. -9 mod 4 = 3
   c. 2718 mod 47 = 39
   d. 3^{17} mod 25 = 13
   e. $\text{dlog}_{7,\,25}$ 18 = 3
2. Using the extended Euclidean algorithm, find the multiplicative inverse of 7467 mod 2464.
   1347
3. Use Fermat's theorem to find 4^{225} mod 17.
   4^{225} mod 17 = $(4^{16})^{14}$ x 4^1 mod 17 = 4^1 mod 17 = 4
4. Solve the equation 5 = x^{47} mod 18 by the Euler's theorem.
   Since $x^{ø(18)}$ mod 18 ≡ x^6 mod 18 ≡ 1
   x^{47} mod 18 ≡ $x^{(7 \times 6 + 5)}$ mod 18 ≡ x^5 mod 18 = 5 mod 18
   Therefore, we can solve two simultaneous congruences and combine them using Chinese remainder theorem as follows:
   i. a^5 mod 2 ≡ 5 mod 2
   ii. b^5 mod 9 ≡ 5 mod 9
   From (i), we get **a** mod 5 ≡ 1 mod 2, and
   from (ii), we get **b** mod 9 ≡ 2 mod 9.
   Combining **a** and **b** using Chinese remainder theorem,
   we get **x** = (2 mod 5, 2 mod 9) = 11

5. Solve the system of equations:

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

By CRT, m_1 = 7, m_2 = 11, m_3 = 12; M = 924 and so M_1 = 132, M_2 = 84, M_3 = 77.
x = (3 × 132 × 132^{-1} mod 7 + 5 × 84 × 84^{-1} mod 11 + 2 × 77 × 77^{-1} mod 12) mod 924
= (3 × 132 × 6 + 5 × 84 × 8 + 2 × 77 × 5) mod 924
= 38

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.

Phileas Fogg was not known to have either wife or children, which may happen to the most honest people; either relatives or near friends, which is certainly more unusual. He lived alone in his house in Saville Row, whither none penetrated. A single domestic sufficed to serve him. He breakfasted and dined at the club, at hours mathematically fixed, in the same room, at the same table, never taking his meals with other members, much less bringing a guest with him; and went home at exactly midnight, only to retire at once to bed. He never used the cosy chambers which the Reform provides for its favoured members. He passed ten hours out of the twenty-four in Saville Row, either in sleeping or making his toilet.

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.

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION

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.

M	**e**	**e**	**t**	**m**	**e**	**a**	**t**	**t**	**h**
13	5	5	20	13	5	1	20	20	8
e	**u**	**s**	**u**	**a**	**l**	**p**	**l**	**a**	**c**
5	21	19	21	1	12	16	12	1	3
e	**a**	**t**	**t**	**e**	**n**	**r**	**a**	**t**	**h**
5	1	20	20	5	14	18	1	20	8
e	**r**	**t**	**h**	**a**	**n**	**e**	**i**	**g**	**h**
5	18	20	8	1	14	5	9	7	8
t	**a**	**m**	**z**	**z**					
20	1	13	26	26					

The calculations proceed three letters at a time. The first three ciphertext characters are in alphabetic positions as 6, 6, and 11 which correspond to FFK. The complete ciphertext:

FFKCGPYAWISXPPQXDVPNQYAWCEYSSAYEEDTXTHCCEHMMM (a-z: 1-26)

WUWTVBPPIZHJGECOSHGCCPPITTKJHMPTQUIJKWOTTTDBY (a-z: 0-25)

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

key	hello	hello	hel
plain	crypt	ograp	hic
cipher	jvjah	vkcld	omn

jvjahvkcldomn

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

s	**e**	**n**	**d**	**m**	**o**	**r**	**e**	**m**	**o**	**n**	**e**	**y**
18	4	13	3	12	14	17	4	12	14	13	4	24
3	**11**	**5**	**7**	**17**	**21**	**0**	**11**	**14**	**8**	**7**	**13**	**9**
21	15	18	10	3	9	17	15	0	22	20	17	7
V	**P**	**S**	**K**	**D**	**J**	**R**	**P**	**A**	**W**	**U**	**R**	**H**

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

c	**a**	**s**	**h**	**n**	**o**	**t**	**n**	**e**	**e**	**d**	**e**	**d**
2	0	18	7	13	14	19	13	4	4	3	4	3
19	**15**	**0**	**3**	**16**	**21**	**24**	**2**	**22**	**18**	**17**	**13**	**4**
21	15	18	10	3	9	17	15	0	22	20	17	7
V	**P**	**S**	**K**	**D**	**J**	**R**	**P**	**A**	**W**	**U**	**R**	**H**

The key is: 19 15 0 3 16 21 24 2 22 18 17 13 4

11. Use the Rabin-Miller primality test to test primality of 151 and 161.

$151 - 1 = 150 = 2^1 \times 75$

Try a = 4

$a^{150} \bmod 151 = 1$

$a^{75} \bmod 151 = 1$, no witness

Try a = 11

$a^{150} \bmod 151 = 1$

$a^{75} \bmod 151 = 1$, no witness

Try a = 23

$a^{150} \bmod 151 = 1$

$a^{75} \bmod 151 = 1$, no witness

151 is probably prime.

$161 - 1 = 160 = 2^5 \times 5$

Try a = 8

$a^{160} \bmod 161 = 36$, witness

161 is composite