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 =3

   b. 7 mod -4 =3

   c. -7 mod 4 =1

   d. -7 mod -4 =1

2. Using the extended Euclidean algorithm, find the multiplicative inverse of 7465 mod 2464.

   2329

3. Use Fermat's theorem, find 4^{225} mod 13.

   4^{225} mod 13 =$(4^{12})^{18}$ x 4^9 mod 13= 4^9 mod 13=2^{18} mod 13 = 2^{12} x 2^6 mod 13 =2^6 mod 13=2^4 x 2^2 mod 13=16 x 4 mod 13 =3 x 4 mod 13=12

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.)

   Since $x^{\phi(15)}$ mod 15 ≡ x^8 mod 15 ≡ 1

   $x^{(61)}$ mod 15 ≡ $x^{(7 \times 8 + 5)}$ mod 15 ≡ x^5 mod 15 = 7 mod 15

   Therefore, we can solve two simultaneous congruences and combine them using Chinese remainder theorem as follows:

   (i) $\mathbf{a}^5$ mod 5 ≡ 7 mod 5

   (ii) $\mathbf{b}^5$ mod 3 ≡ 7 mod 3

   From (i), we get **a** mod 5 ≡ 2 mod 5 ,and

   from (ii), we get **b** mod 3 ≡ 1 mod 3.

   Combining **a** and **b** using Chinese remainder theorem,

   we get **x** = (2 mod 5, 1 mod 3) = 7.

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.

   Let the day when they all have a colliding lecture be denoted by x, where we count day 1 as the first Monday, then

   x = 1 + $3K_1$ = 2 + $2K_2$ = 3 + $5K_3$ = 4 + $6K_4$ = 5 + K_5 = 6 + $4K_6$ = $7K_7$ where Ki are integers;

i.e.,

(1) $x \equiv 1 \bmod 3$

(2) $x \equiv 2 \bmod 2$

(3) $x \equiv 3 \bmod 5$

(4) $x \equiv 4 \bmod 6$

(5) $x \equiv 5 \bmod 1$

(6) $x \equiv 6 \bmod 4 \equiv 2 \bmod 4$

(7) $x \equiv 0 \bmod 7$

Of these congruences, modulo 1 congruence is trivially satisfied and can be eliminated, the modulo 2 congruence gets subsumed into modulo 4 congruence and modulo 3 congruence gets subsumed into the modulo 6 congruence, so reducing in this way gives:

(1) $x \equiv 3 \bmod 5$

(2) $x \equiv 4 \bmod 6$

(3) $x \equiv 2 \bmod 4$

(4) $x \equiv 0 \bmod 7$

Congruences (2) and (3) can be combined into 10 mod 12, leaving the remaining modulus's coprime to each other so that we can apply Chinese remainder theorem. Thus, we have

(1) $x \equiv 3 \bmod 5$

(2) $x \equiv 10 \bmod 12$

(3) $x \equiv 0 \bmod 7$

Then $m1 = 5$, $m2 = 12$, $m3 = 7$; $M = 420$ and so $M1 = 84$, $M2 = 35$, $M3 = 60$.

Then,

$x = (3 \times 84 \times 84^{-1} \bmod 5 + 10 \times 35 \times 35^{-1} \bmod 12 + 0) \bmod 420$

$= (3 \times 84 \times 4 + 10 \times 35 \times 11) \bmod 420$

$= 4858 \bmod 420$

$= 238.$

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 o clock” Using the Hill cipher with t

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	**o**	**c**	**l**	**o**	**c**	**k**	**q**		
20	15	3	12	15	3	11	17		

The calculations proceed two letters at a time. The first pair:

$$\begin{pmatrix} C1 \\ C2 \end{pmatrix} = \begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 13 \\ 5 \end{pmatrix} = \begin{pmatrix} 106 \\ 51 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 25 \end{pmatrix}$$

The first two ciphertext characters are in alphabetic positions as 2 and 25 which correspond to BY. The complete ciphertext:

BYQFBYOXHBTKNMQNRNPQLORJYJYOHBKVHBWTJCUBCKENJSXC

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

key	eng	eng	eng	eng	eng
plain	cry	pto	gra	phi	c
cipher	gee	tgu	keg	tuo	g

geetgukegtuog

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.

a. Ciphertext:

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. Finding a key:

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 113 and 133.

$113-1=2^4 \times 7$

Try a=4

$a^{112} \bmod 113 = 1$

$a^{56} \bmod 56 = 1$

$a^{28} \bmod 113 = 1$

$a^{14} \bmod 113 = 1$

$a^{7} \bmod 113 = -1$, no witness

113 is probably prime.

$133-1=2^2 \times 33$

Try a=8

$a^{132} \bmod 133 = 1$

$a^{66} \bmod 133 = 1$

$a^{33} \bmod 133 = 113$,witness

133 is composite