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.** $dlog_{7,25}$ 18 = 3+4k, $\forall k \in R$

2. **Using the extended Euclidean algorithm, find the multiplicative inverse of 7467mod 2464.**

   7467 = 2464*3 + 75

   2464 = 75*32 + 64

   75 = 64*1 + 11

   64 = 11*5 + 9

   11 = 9*1 +2

   9 = 2*4 +1

   ➔

   1 = 9 – 2*4

   = 5*9 + (-4)*11

   = 5*(64-11*5) + (-4)*11

   = …… = (-1117)*7467 + 3385*2464

   Mod 2464 both side of equal sign

   (-1117)*7467≡1 mod 2464

   So, the multiplicative inverse of 7467mod 2464 is -1117 + 2464*k, $\forall k \in Z$

3. **Use Fermat's theorem to find 4^{225} mod 17.**

   By Fermat's thereom, $4^{16} \equiv 1$ mod 17

   ➔$(4^{16})^{14} * 4 \equiv 1*4$ mod 17

   ➔$4^{225} \equiv 4$ mod 17

   Ans: 4

4. **Solve the equation 5 = x^{47} mod 18 by the Euler's theorem.**

   $\emptyset(18) = 18*(1-1/2)(1-1/3) = 6$

   $x^{47} \equiv x^{(6*7+5)} \equiv x^5 \equiv 5$ mod 18

   take the fifth power, we obtain

   $x^{25} \equiv x^{(6*4+1)} \equiv x \equiv 5^5 \equiv 3125 \equiv 11$ mod 18 so, x=11

5. **Solve the system of equations:**

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

Since 7, 11 ,12 are both relatively prime, we can use Chinese remainder theorem to solve these equations.

let n1=7, n2=11, n3=12,

r1=3, r2=5, r3=2, n=n1n2n3=7*11*12=924,

N1=n/n1=132, N2=n/n2=84, N3=n/n3=77

Next we need to find

$M1 \equiv N1^{-1} \bmod 7$

$M2 \equiv N2^{-1} \bmod 11$

$M3 \equiv N3^{-1} \bmod 12$

132*(-1) ≡ 1 mod 7, pick M1=-1

84*(-3) ≡ 1 mod 11, pick M2=-3

77*5≡ 1 mod 12, pick M3=5

Pick x ≡ r1M1N1 + r2M2N2 + r3M3N3 ≡ 3*(-1)*132 + 5*(-3)*84 + 2*5*77

≡ -886 ≡ 38 mod n (n=N1N2N3=924)

x = 38 + n*k, $\forall k \in Z$

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 afirst reading.

I use some frequency analysis and first try to decrypt vowels and then the others.

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 TTinto tt.

r	o	y	a	l
n	e	w	z	d
v	b	c	f	g
h	i/j	k	m	p
q	s	t	u	x

Above is the key matrix of this playfair cipher.

With it, we can easily decipher the ciphertext to the following plaintext.

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.**

The first three letters are m =12, e=4, e=4, (I use a=0, b=1, c=2.....)

[12 4 4] [1 3 5] mod 26 w u w

[2 4 6] = [48 72 100] =======> [22 20 22]

[7 5 4][

So, the first three encrypted letters will be wuw. Because the length of this string is not the multiple of 3, I add 'z' as padding. Continuing this process, we can get our final ciphertext:
wuwtvbppizhjgecoshgccppittkjhmptquijkwotttdby

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

KEY: h e l l o h e l l o h e l

PLAIN: c r y p t o g r a p h I c

CIPHER: 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

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

   a. Ciphertext:

Plain text	s	e	n	d	m	o	r	e	m	o	n	e	y
Origin	18	4	13	3	12	14	17	4	12	14	13	4	24
Shift amount	3	11	5	7	17	21	0	11	14	8	7	13	9
After shift	21	15	18	10	3	9	17	15	0	22	20	17	7
Cipher text	v	p	s	k	d	j	r	p	a	w	u	r	h

b.Find a key:

Plain text	c	a	s	h	n	o	t	n	e	e	d	e	d
Origin	2	0	18	7	13	14	19	13	4	4	3	4	3
Need to shift	19	15	0	3	16	21	24	2	22	18	17	13	4
After shift	21	15	18	10	3	9	17	15	0	22	20	17	7
Cipher text	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 = 2 * 75

try a = 3

a^{150} mod 151 = 1

a^{75} mod 151 = -1

next try a = 4

a^{150} mod 151 = 1
a^{75} mod 151 = 1

next try a=5
a^{150} mod 151 = 1
a^{75} mod 151 = 1

next try a=7
a^{150} mod 151 = 1
a^{75} mod 151 = -1
no witness has found,
151 is probably prime.

161 – 1 = 2^5 * 5
Try a=3
a^{160} mod 161 = 39, witness find
161 is composite.