School of Computer Science
University of Guelph

CIS*4110 Computer Security

Winter 2018 Instructor: Dr. Charlie Obimbo Assignment 2 Due: February 9th, 2018

Name: Matthew Blatz **Max Marks: 40**

PLEASE ENSURE YOU THE WHOLE ASSIGNMENT IS TYPED AND PRINTED!

1. **(Hill-Cipher)** Bob sends Alice the following code, in which the Hill-Cipher has been used, modulo 31. The key matrix used is:

$$K = \begin{pmatrix} 5 & 30 & 23 \\ 6 & 30 & 20 \\ 26 & 1 & 9 \end{pmatrix}$$ and The Ciphertext A is:

$$\begin{pmatrix} N & V & I & M & F & T & U & F & Z \\ V & F & I & F & R & 1 & Y & K & V \\ G & S & E & X & N & P & L & I & Y \end{pmatrix}$$

If Bob used the following decimal encoding:

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Code	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Letter	Q	R	S	T	U	V	W	X	Y	Z		1	2	3	4	
Code	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	

(a) Compute the inverse of the matrix K (mod 31). (3 marks)

Determinant $= (5\cdot30\cdot9)+(30\cdot20\cdot26)+(23\cdot6\cdot1)-(23\cdot30\cdot26)$
$-(5\cdot20\cdot1)-(30\cdot9\cdot6) = -2572$

$-2572 \bmod (31) = 1$

$1^{-1} \bmod 31 = 1$

Transpose $= \begin{bmatrix} 5 & 6 & 26 \\ 30 & 30 & 1 \\ 23 & 20 & 9 \end{bmatrix}$

minor

$a_{11} = (30\cdot9)-(20) = 250$

$a_{12} = (30\cdot9)-23 = 247$

$a_{13} = (30\cdot20)-(30\cdot23) = -90$

$a_{21} = (6\cdot9)-(20\cdot26) = -466$

$a_{22} = (5\cdot9)-(23\cdot26) = -553$

$a_{23} = 100-(23\cdot6) = -38$

$a_{31} = 6-(26\cdot30) = -774$

$a_{32} = 5-(30\cdot26) = -775$

$a_{33} = (5\cdot30)-(6\cdot30) = -30$

$\longrightarrow \begin{bmatrix} 250 & 247 & -90 \\ -466 & -553 & -38 \\ -774 & -775 & -30 \end{bmatrix}$

$\downarrow$ cofactor

$\begin{bmatrix} 250 & -247 & -90 \\ 466 & -553 & 38 \\ -774 & 775 & -30 \end{bmatrix}$ (mod 31)

Inverse of k mod 31

$$= \begin{bmatrix} 2 & 1 & 3 \\ 1 & 5 & 7 \\ 1 & 0 & 1 \end{bmatrix}$$

(b) Find the plaintext M. (Remember to remove the gibberish & punctuate it correclty.) [3]

$$= \begin{bmatrix} 2 & 1 & 3 \\ 1 & 5 & 7 \\ 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 13 & 21 & 8 & 12 & 5 & 19 & 20 & 5 & 25 \\ 21 & 5 & 8 & 5 & 17 & 27 & 24 & 10 & 21 \\ 6 & 18 & 4 & 23 & 13 & 15 & 11 & 8 & 24 \end{bmatrix}$$

$$= \begin{bmatrix} 65 & 101 & 36 & 98 & 66 & 110 & 97 & 44 & 143 \\ 160 & 172 & 76 & 198 & 181 & 259 & 217 & 111 & 298 \\ 19 & 39 & 12 & 35 & 18 & 34 & 31 & 13 & 49 \end{bmatrix} \bmod 31$$

$$= \begin{bmatrix} 3 & 8 & 5 & 5 & 4 & 17 & 4 & 13 & 19 \\ 5 & 17 & 14 & 12 & 26 & 11 & 0 & 18 & 19 \\ 19 & 8 & 12 & 4 & 18 & 3 & 0 & 13 & 18 \end{bmatrix}$$

$$= \begin{bmatrix} D & I & F & F & E & R & E & N & T \\ F & R & O & M & \sqcup & L & A & S & T \\ T & I & M & E & S & D & A & N & S \end{bmatrix}$$

DIFFERENT FROM LAST TIME.

2. The following Message has been encoded using Substitution Cipher. Decode them: [2]

Note: The first student to decode this and send Dr. Obimbo the solution and how (s)he broke the code will get 4 bonus marks, the next 4 students (giving plaintext & explanations) will get 2 bonus marks each.

(a) NWZ BPM NQZAB BQUM, AKQMVBQABA AIG BPMG KZMIBML KTWVML XZQUIBMA CAQVO BPM AIUM KWUXTQKIBML KTWVQVO BMKPVQYCM BPIB UILM LWTTG BPM. APMMX QV VQVMBG AQF.
KVV RIVCIZG..

Decoding Key: ----------

FOR THE FIRST TIME SCIENTISTS SAY THEY
CREATED CLONED PRIMATES USING THE SAME
COMPLICATED CLONING TECHNIQUE THAT
MADE DOLLY THE. SHEEP IN NINETY SIX.
CNN JANUARY

3. (a) Use Euclid's Algorithm to find gcd(103 107, 1133).
[No Partial Marks] (2 Marks)

103107/1133 = 91 remain 4

103107 = 1133 · 91 + 4

gcd (1133, 4)

1133 = 4 · 283 + 1

gcd (283, 1)

~~remainder~~ = 1

(b) Find the inverse of 1133 (mod 103 107). [No Partial Marks] (2 Marks)

1 = 1133 − 283(4)

= 1133 − 283[103107 − 1133(91)]

= 25754(1133) − 283(103107)

= 1133^{-1} mod (103107) = 25754

(c) Show that 13 is a prime number using the fast-exponentiation algorithm and Fermat's little Theorem [for only the primes below 13]. [3]

	1	1	0	0
$2^i \pmod{13}$	2	8	12	1
$3^i \pmod{13}$	3	1	1	1
$5^i \pmod{13}$	5	8	12	1
$7^i \pmod{13}$	7	5	12	1
$11^i \pmod{13}$	11	5	12	1

(d) From (c) what is $7^6 \pmod{13}$. [1]

Take the first 2 $\qquad 11 = 6$ in binary.

$7 + 5 = \underline{12}$

(e) Use the steps from your answer in (c) to evaluate $7^{11\,403} \pmod{13}$. [2]

$= (7^{12})^{950} \cdot 7^3 \pmod{13}$

$= 1^{450} \cdot 7^3 \pmod{13}$

$343 \pmod{13} = 5$

(f) Also find $105\,305^{5225} \pmod{13}$. [2]

$= 105\,305^{5225} \pmod{13}$

$= (8100 \cdot 13 + 5)^{5225} \pmod{13}$

$= 5^{5225} \pmod{13}$

$= (5^{12})^{435} \cdot 5^5 \pmod{13}$

$= 1^{435} \pmod{13} \cdot 5^5 \pmod{13}$

$= 5^5 \pmod{13}$

$= 3125 \pmod{13} = 5$

4. Use the Fast Exponentiation Algorithm to determine $97^{147} \pmod{200}$. [3]

$\varnothing(200)$

20 10

10 2 2 5

2 5

$\varnothing(200) = 200\left(\frac{2-1}{2}\right)\left(\frac{5-1}{5}\right)$

$= 200\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$

$= 80$

$97^{147} \pmod{200} = 97^{67} \pmod{200}$

64	32	16	8	4	2	1
1	0	0	0	0	1	1
97	9	81	161	121	177	113

$= 113$

5. **Find all solutions (between 1 & 265) to the equation $45x \equiv 15 \pmod{265}$. [4]**

$9x = 3 \pmod{53}$

$53 = 9 \cdot 5 + 8$

$9 = 8 \cdot 1 + 1$

$1 = 9 - 8$

$1 = 9 - (53 - (9 \cdot 5))$

$1 = 6 \cdot 9 - 53 \cdot 1$

$x = 6(3) \pmod{53}$

$x = 18 \bmod 53m$ → where $m = \{0, 1, 2, 3, 4\}$

because 45, 15, 265 are divisible by 5.

$\therefore$ $x = 18$

$x = 71$

$x = 124$

$x = 177$

$x = 230$

6. **[CRT] Find x, if $x = (1, 2, 3)$ S $(2, 3, 7)$** [4]

$x = 1 \pmod 2$

$x = 2 \pmod 3$

$x = 3 \pmod 7$

$m = 2 \cdot 3 \cdot 7 = 42$

$m_1 = 42/2 = 21$

$m_2 = 42/3 = 14$

$m_3 = 42/7 = 6$

$y_1 = \text{Inv } 21 \pmod 2 = 1$

$y_2 = \text{Inv } 14 \pmod 3 = 2$

$y_3 = \text{Inv } 6 \pmod 7 = 6$

$x = (1 \cdot 21 \cdot 1) + (2 \cdot 14 \cdot 2) + (3 \cdot 6 \cdot 6)$

$x = 185 \bmod (42)$

$= 17$

7. The prime number theorem asserts that the number of prime numbers smaller than n is approximately $\frac{n}{\ln n}$. (You may use this one or a better one). Write a Program to list the first 990,000th prime number, and compare the value you get from this program, with the one obtained using the prime number theorem. [9]

[Note that you are to print only the 990,000th prime, of course you will be expected to hand in your program. Also you will be expected to determine the time it takes your program to find this number, and then analyze the number with the approximate number you get by solving the nonlinear equation.]

[Program Due: Wed., February 9th, 2018 at Midnight.] The program should be uploaded to course-link, along with a document indicating the asked for prime number, and a brief description of the algorithm used to calculate it.