HW 3 CMSC 456. Morally DUE Sep 23
SOLUTIONS
NOTE- THE HW IS FOUR PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. READ my NOTES on ciphers and on English. What is your name? What is the day and time of the first midterm?

2. (25 points) (This problem is based on material that you will see on Wed Sept 18.)

   (a) (5 points) Alice wants to compute $7^{81} \pmod{101}$. Do this using repeated squaring. Show all work. How many multiplications does it take?

   (b) (5 points) Alice notices that $81 = 3^4$. So instead of using repeated *squaring* she decides to use repeated *cubing*. Each cubing takes two multiplications but there are less iterations. Compute 7^{81} using this. Show all work. How many multiplications does it take?

   (c) (8 points) Give an algorithm that does the repeated cubing method for the problem: given a, n, p, find $a^n \pmod{p}$. Give a good upper bound on how many multiplications it takes as a function of n. You CANNOT use O-notation at all. You CAN upper bound something like $\lfloor BLAH \rfloor$ by BLAH.

   (d) (7 points) Recall that for repeated squaring the number of multiplications is

   $$\leq \lg(n) + (\text{ Number of 1's in binary rep of } n\ ) - 1.$$

   Give three examples of an $n \geq 99$ where the repeated-cubing algorithm takes less mults than the repeated-squaring algorithm.

   (e) (0 points) Why isn't repeated cubing used more often?

SOLUTION TO PROBLEM TWO

(a) Alice wants to compute $7^{81} \pmod{101}$. Do this using repeated squaring. Show all work. How many multiplications does it take?
ANSWER: all arithmetic is mod 101.

$7^2 \equiv (7^1)^2 = 49$
$7^4 \equiv (7^2)^2 = 49^2 \equiv 78$
$7^8 \equiv (7^4)^2 = 78^2 \equiv 24$
$7^{16} \equiv (7^8)^2 = 24^2 \equiv 71$
$7^{32} \equiv (7^{16})^2 = 71^2 \equiv 92$
$7^{64} \equiv (7^{32})^2 = 92^2 \equiv 81$

Each of the above took one mult for a total of 6 mults so far.

$7^{81} = 7^{64} \times 7^{16} \times 7^1 \equiv 81 \times 71 \times 7 \equiv 59$ (2 mults)

TOTAL: 8 mults.

(b) Alice notices that $81 = 3^4$. So instead of using repeated *squaring* she decides to use repeated *cubing*. Each cubing takes two multiplications but there are less iterations. Compute 7^{81} using this, show your work. How many multiplications does it take?

ANSWER

$7^3 \equiv 40$
$7^9 \equiv (7^3)^3 \equiv 40^3 \equiv 67$
$7^{27} \equiv (7^9)^3 \equiv 67^3 \equiv 86$
$7^{81} \equiv (7^{27})^3 = 86^3 \equiv 59$

Each of the above took two mult for a total of 8 mults.

TOTAL: 8 mults.

(c) Give an algorithm that does the repeated cubing method for the problem: given a, n, p, find $a^n \pmod p$. Give a good upper bound on how many multiplications it takes as a function of n.

ANSWER

All arithmetic is mod p.

i. Input (a, n, p)
ii. Convert n to base 3: $n = \sum_{i=0}^{L} n_i \times 3^i$. ($n_i$'s are in $\{0, 1, 2\}$, $L = \lfloor \log_3(n) \rfloor$.)
iii. $x_0 = a$
iv. For $i = 1$ to L, $x_i = x_{i-1}^3$. (Note that $x_i = a^{3^i}$.)
v. (Now have $a^{n_0 3^0}, \ldots, a^{n_L 3^L}$) Answer is $a^{n_0 3^0} \times \cdots \times a^{n_L 3^L}$

Number of operations:

Number of iterations: L. Number of mults in each iteration: 2. So there are $\leq 2L \leq 2\lfloor \log_3(n) \rfloor \leq 2\log_3(n)$ mults.

Number of iterations after iteration: $\leq L = \lfloor \log_3(n) \rfloor \leq \log_3(n)$.

So total is $\leq 3\log_3(n)$ mults.

(d) Recall that for repeated squaring the number of multiplications is

$$\leq \lg(n) + (\text{ Number of 1's in binary rep of } n\ ) - 1.$$

Give three examples of an $n \geq 99$ where the repeated-cubing algorithm takes less mults than the repeated-squaring algorithm.

ANSWER

We look at powers of 3.

7^{3^5}.

First do by repeated cubing:

$x_0 = 7$

$x_1 \equiv x_0^3$ (which is 7^3)

$x_2 \equiv x_1^3$ (which is 7^{3^2})

$x_3 \equiv x_2^3$ (which is 7^{3^3})

$x_4 \equiv x_3^3$ (which is 7^{3^4})

$x_5 \equiv x_4^3$ (which is 7^{3^5})

Each line takes 2 mults, so 10 mults total.

We now look at repeated squares.

Need to look at 3^5 in binary:

$3^5 = 243 = 11110011$ in binary.

$$11110011 = 2^7 + 2^6 + 2^5 + 2^4 + 2^1 + 2^0$$

$x_0 = 7$

$x_1 \equiv x_0^2$ (which is 7^2)

$x_2 \equiv x_1^2$ (which is 7^{2^2})

$x_3 \equiv x_2^2$ (which is 7^{2^3})

$x_4 \equiv x_3^2$ (which is 7^{2^4})

$x_5 \equiv x_4^2$ (which is 7^{2^5})

$x_6 \equiv x_5^2$ (which is 7^{2^6})

$x_7 \equiv x_6^2$ (which is 7^{2^7})

This took 7 multiplications so far.

$$7^{3^5} = 7^{2^0} \times 7^{2^1} \times 7^{2^4} \times 7^{2^5} \times 7^{2^6} \times 7^{2^7}$$

This is 5 mults

SO 12 mults total- MORE than the 10 doing it with repeated cubing.

We OMIT the other two examples, but they are both powers of 3.

(e) Why isn't repeated cubing used more often?

Sometimes it takes more steps. But even when it takes less, multiplying by powers of 2 is a very easy shift of bits, so the type of mult is easier for powers of 2.

GO TO NEXT PAGE

3. (25 points) Alice and Bob are going to use the Affine Cipher. They get to choose their alphabet size! If the alphabet size is n then they will pick a number $a \in \{1, \ldots, n\}$ at *random* and then test if a will work to be the coefficient of x. If not, then try again. If so then they will use a as the coefficient for x. (We are not concerned with the picking of b.)

   (a) (10 points) Assume the alphabet size is 1000. What is the probability that the a they pick will work? Call this p_{1000}. (Think about but do not hand in: what is the expected number of times they will need to pick an a?)

   (b) (10 points) Assume the alphabet size is 1001. What is the probability that the a they pick will work? Call this p_{1001}. (Think about but do not hand in: what is the expected number of times they will need to pick an a?)

   (c) (5 points) Which of p_{1000} and p_{1001} is bigger? Based on this give some general advice on what alphabet size to use if a prime size is not available.

SOLUTION TO PROBLEM THREE

(a) Assume the alphabet size is 1000. What is the probability that the a they pick will work?

ANSWER: We need to know how many elements of $\{1, \ldots, 1000\}$ are rel prime to 1000. This is $\phi(1000) = \phi(2^3 \times 5^3) = \phi(2^3) \times \phi(5^3) = (2-1)2^2 \times (5-1)5^2 = 4 \times 100$. Hence the probability is

$$p_{1000} = \frac{400}{1000} = 0.4.$$

(b) Assume the alphabet size is 1001. What is the probability that the a they pick will work?

ANSWER: We need to know how many elements of $\{1, \ldots, 1001\}$ are rel prime to 1001. This is $\phi(1001) = \phi(7 \times 11 \times 13) = \phi(7) \times \phi(11) \times \phi(13) = 6 \times 10 \times 12$. Hence the probability is

$$p_{1001} = \frac{6 \times 10 \times 12}{1001} = \frac{720}{1001} \sim 0.72.$$

(c) Which of p_{1000} and p_{1001} is bigger? Based on this give some general advice on what alphabet size to use if a prime size is not available.

ANSWER: p_{1001} is bigger. Good to pick an alphabet size that has no square factors.

GO TO NEXT PAGE

4. (25 points) We describe the *Randomized Affine Cipher*. ALL arithmetic is mod 26.

   Let

   $$S = \{(a, b) \mid 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$$

   The key is a function f from $\{0, \ldots, 25\} \times \{0, \ldots, 25\}$ to S. To send message $(m_1, \ldots, m_L)$ (each m_i a character) Alice does the following:

   - Pick random $r_1, \ldots, r_L \in \{0, \ldots, 25\} \times \{0, \ldots, 25\}$.
   - For $1 \leq i \leq L$ let compute $f(r_i) = (a_i, b_i)$.
   - Send $(r_1, a_1 m_1 + b_1), \ldots, (r_L, a_L m_L + b_L)$.

   (a) (15 points) Describe how Bob will, given

   $$(r_1, c_1), \ldots, (r_L, c_L),$$

   decode the message. (Note that Bob has the key f.)

   (b) (10 points) Alice and Bob are using the following key: $f(x, y) =$
   - The first coordinate is the first number AFTER x that is rel prime to 26 with the exception that $x = 25$ yields 1.
   - The second coordinate is $y + 1$ (all mod 26).

   Alice want to send the message *clyde*.

   Alice generates the following five random pairs to help her do this. They are

   (2,5), (3,6), (10,2), (15,7), (25,0).

   What does Alice send to Bob?

SOLUTION TO PROBLEM FOUR

(a) Describe how Bob will, given $(r_1, c_1), \ldots, (r_L, c_L)$, decode the message. (Note that Bob has the key f.)

ANSWER:

To decode $(r_1, c_1), \ldots, (r_L, c_L)$ Bob does the following.

i. For $1 \leq i \leq L$ compute $f(r_i) = (a_i, b_i)$.

ii. For each a_i find a_i^{-1} mod 26. It exists since a_i is rel prime to 26.

iii. Decode as $(a_1^{-1}(c_1 - b_1), \ldots, a_L^{-1}(c_L - b_L))$

(b) $f(x, y)$ = The first coordinate is the first number AFTER x that is rel prime to 26 with the exception that $x = 25$ yields 1. The second coordinate is $y + 1$ (all mod 26).

Alice wants to send *clyde*

She generate the following five random pairs: (2,5), (3,6), (10,2), (15,7), (25,0).

What does Alice send to Bob? Show all of your steps.

ANSWER: Omitted.

GO TO NEXT PAGE

5. (25 points) Alice and Bob are using the cipher on the Sept 9 slides, title *Awesome Vig or Psuedo One-Time Pad* EXCEPT that the mod is 2 digits long instead of 4 digits long.

   Eve is sure that the word ERIK will be in the plaintext.

   Eve looks at every 4-long sequence in the ciphertext and guesses that they decode to ERIK and sets up equations.

   Eve sees ABCD.

   (a) (7 points) Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

   (b) (7 points) What are the bounds on M?

   (c) (11 points) Find the values of M that could possibly work, or show there aren't any.

   The following table will help you:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

SOLUTION TO PROBLEM FIVE

(a) We convert both ERIK and ABCD into sequences of 2-digit long numbers.

ERIK is (05,18,09,11)

ABCD is (01,02,03,04)

Here is how Eve finds her guess for the key:

The first two digits:

$0 + x \equiv 0 \mod 10$

$5 + y \equiv 1 \pmod{10}$

Hence $x = 0$ and $y = 6$.

Keep doing this to find that the guess for the key is

$(06, 94, 04, 93)$

Just for my own sanity I'll rewrite this to check it.

ERIK	05	18	09	11
KEY	06	94	04	93
ABCD	01	02	03	04

SO the equations are:

$$\begin{aligned} 94 &\equiv 6A + B \pmod{M} \\ 4 &\equiv 94A + B \pmod{M} \\ 93 &\equiv 4A + B \pmod{M} \end{aligned}$$

(b) The largest element of the key was 94. We know that M is 2 digits. Hence $95 \leq M \leq 99$.

(c) Subtract the second from the first equation to get

EQ1: $90 \equiv -88A \pmod{M}$

Subtract the third from the first equation to get

EQ2: $1 \equiv 2A \pmod{M}$

Multiply EQ2 by 44 to get

EQ3: $44 \equiv 88A \pmod{M}$

Add EQ1 and EQ3 to get

$134 \equiv 0 \pmod{M}$

Hence we know that M divides 134. So M has to be one of

$$1, 2, 67, 134.$$

NONE of these are in the range from 95 to 99 so NO value of M works.