HW 6 CMSC 456. Morally DUE Oct 14
SOLUTIONS
NOTE- THE HW IS FOUR PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? What is the day and time of the midterm?

2. (25 points) Alice wants to speed up and simplify RSA. She tells Bob "lets ALWAYS use $e = 2^{2^4} + 1$". Let $e = 2^{2^4} + 1$ for the rest of this problem.

   (a) (5 points) Write $e-2, e-1$, and e in both decimal and binary.

   (b) (5 points) If Bob computes m^e using repeated squaring then how many operations will it take? If Bob computes m^{e-1} using repeated squaring then how many operations will it take? If Bob computes m^{e-2} using repeated squaring then how many operations will it take?

   Express answers as ACTUAL NUMBERS like 81 or π. So I don't want things like *The eth Fibonacci Number*. (*Warning:* The answer is NOT π, or the eth Fib number, or even the πth Fib number.)

   (c) (5 points) If you did part 1 right, then using $e-1$ is the best (though not by much), then e, then $e-2$ (and $e-2$ is much worse than e). So why not use $e-1$ for RSA?

   (d) (5 points) Give two PROS to using this value of e.

   (e) (5 points) Give two CONS to using this value of e.

   (f) (0 points but look into and think about) Do people really use this value of e? Is using this value of e a good idea?

SOLUTION TO PROBLEM TWO

(a) Write $e-2, e-1, e$ as both decimal and binary.

ANSWER:

$e-2 = 65535$ in base 10

$e-2 = 1111111111111111$ in base 2.

$e-1 = 65536$ in base 10

$e-1 = 10000000000000000$ in base 2.

$e = 65537$ in base 10

$e-1 = 10000000000000001$ in base 2.

(b) If Bob computes m^e using repeated squaring then how many operations will it take? If Bob computes m^{e-1} using repeated squaring then how many operations will it take? If Bob computes m^{e-2} using repeated squaring then how many operations will it take? Express answers as ACTUAL NUMBERS like 81 or π. So I don't want things like *The eth Fibonacci Number*. (*Warning:* The answer is NOT π, or the eth Fib number, or even the πth Fib number.)

ANSWER:

Recall that repeated squaring for m^n takes

$\lfloor \lg(n) \rfloor$ + (Number of 1's in n) -1.

$\lfloor \lg(e-2) \rfloor = 15$. Number of 1's in $e-2$ is 16. So 30 operations.

$\lfloor \lg(e-1) \rfloor = 16$. Number of 1's in $e-1$ is 1. So 16 operations.

$\lfloor \lg(e) \rfloor = 16$. Number of 1's in e is 2. So 17 operations.

(c) If you did part 1 right, then using $e-1$ is the best (though not by much), then e, then $e-2$ (and $e-2$ is much worse than e). So why not use $e-1$ for RSA?

ANSWER: $e-1$ would need to be rel prime to $(p-1)(q-1)$. But $(p-1)(q-1)$ is even since either p or q is odd. Hence, $e-1$ cannot work.

(d) Give two PROS to using this value of e.

ANSWER: I'll give three:

Computing m^e takes only 17 operations (as seen above even a slight change might increase the number of operations by a lot).

This e is known to be prime so easy to test if rel prime to $(p-1)(q-1)$.

e is big enough to thwart attacks in 2019.

(e) Give two CONS to using this value of e.

ANSWER: I'll give three:

If keep using the SAME e then Eve could preprocess stuff.

If keep using the SAME e then — who knows — maybe number theorists will find out something special about that e that makes it easy to find the inverse of mod $(p-1)(q-1)$.

This e thwarts the low-e attack TODAY, but what about Tomorrow, tomorrow, is always another day!

(f) Do people really use this value of e? Is using this value of e a good idea?

ANSWER: People really do use it. This makes me nervous.

END OF SOLUTION TO PROBLEM TWO
GOTO NEXT PAGE

3. (25 points)

   (a) (10 points) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

   (b) (15 points) Give an algorithm that does the following: Given primes p, q and $1 \leq a \leq pq - 1$ such that a is rel prime to pq, and n (which could be VERY LARGE!) return

$$a^n \pmod{pq}.$$

   We assume that any operation with numbers less than pq takes 1 step, but any operation with a number BIGGER than pq, of length L, takes L steps. Give an upper bound on the number of operations in terms of n, p, q. The answer should be of the form $O(f(n, p, q))$.

SOLUTION TO PROBLEM THREE

(a) Compute the following:

$$30^{123,456,789,111,213,141} \pmod{1001}.$$

ANSWER:

$1001 = 7 \times 11 \times 13$

Hence

$\phi(1001) = 6 \times 10 \times 12 = 720$

So we need to compute

$123, 456, 789, 111, 213, 141 \pmod{720}$ which is 501

So we just need

$$30^{501} \pmod{1001}$$

We omit the rest but it's done by repeated squaring.

(b) **ANSWER:**

i. Input(a, n, p, q)

ii. Divide n by $(p-1)(q-1)$ and take the remainder r. (This takes length n which is $\lg(n)$ steps.)

iii. We compute $a^r \pmod{pq}$ with repeated squaring. Since $r \leq pq$ this takes $\leq 2\lg(pq)$ steps.

This takes $\lg(n) + 2\lg(pq)$ steps.

END OF SOLUTION TO PROBLEM THREE

GOTO NEXT PAGE FOR NEXT PROBLEM

4. (25 points) Alice and Bob are going to do RSA with $p = 31$, $q = 37$, $N = pq = 1147$, $R = (p-1)(q-1) = 30 * 36 = 1080$, $e = 77$ (one can check that 77 is rel prime to 1080), and $d = 533$ (one can check that $ed \equiv 1 \pmod{R}$). Recall that (N, e) are public, but only Alice knows d.

   They operate in Base 10. So messages are in $\{0001, \ldots, 1146\}$ and are only 4-digits long (we pad with 0's).

   They want to avoid the NY,NY problem. They will now send only 3-digit messages and add a random digit on the RIGHT of the message. If Bob wants to send 107 he generates a random digit r and sends $107r$.

   (a) (10 points) Bob wants to send 107. The random r he picks is 8. What does Bob send? Show how Alice decodes it.

   (b) (10 points) Bob wants to send 107 again. The random r he picks is 5. What does Bob send? Show how Alice decodes it.

   (c) (5 points) Bob has another idea: Hey Alice, let's add a random digit to the LEFT instead of to the RIGHT. This is a terrible idea. Why?

SOLUTION TO PROBLEM FOUR

(a) Solution Omitted

(b) Solution Omitted

(c) Message have to be in $\{0001, \ldots, 1146\}$. Hence the only random digits you can append on the right are 0 or 1. If you send NY,NY,NY then at least two of the three will be identical.

END OF SOLUTION TO PROBLEM FOUR

GOTO NEXT PAGE

5. (25 points) Zelda does RSA with Alice1 and Alice2. With Alice1 she uses $N_1 = 91$ and $e = 2$. With Alice2 she uses $N_2 = 187$ and $e = 2$. Hence this is just the right setting for a low-e attack.

   (Note that $e = 2$ cannot actually be used in RSA since e is not coprime to $\phi(N_1)$ and $\phi(N_2)$, but we use it here to make the problem easier.)

   Eve sees Zelda send Alice1 43.

   Eve sees Zelda send Alice2 185.

   Eve knows that Zelda send the SAME message to both Alice1 and Alice2.

   Use the low-e attack to find the message. Show all of your steps. (ADVICE: write a program or use the web to find inverses of x mod y. You can use that and not have to show work. Everything else you do.)

SOLUTION TO PROBLEM FIVE

Let m be the message. We know $m \leq 90$.

We know

$m^2 \equiv 43 \pmod{91}$

$m^2 \equiv 185 \pmod{187}$

So we first seek an x such that

$x \equiv 43 \pmod{91}$

$x \equiv 185 \pmod{187}$

$0 \leq x < 91 \times 187$.

$$x = 43 \times 187 \times (187^{-1} \pmod{91}) + 185 \times 91 \times (91^{-1} \pmod{189}).$$

187 (mod 91) = 5. Need inverse of 5 mod 91 which we do by hand (even though you didn't have to)

$$91 = 5 \times 18 + 1$$

Mod both sides by 91

$$0 \equiv 5 \times 18 + 1 \pmod{91}$$

$$5 \times -18 \equiv 1 \pmod{91}$$

$$5 \times 73 \equiv 1 \pmod{91}$$

SO inverse of 187 mod 91 is 73.

We need inverse of 91 mod 187.

$187 = 2 \times 91 + 5$

$91 = 18 \times 5 + 1$

So

$$1 = 91 - 18 \times 5 = 91 - 18(187 - 2 \times 91) = 37 \times 91 - 18 \times 187.$$

Take this mod 187 to get

$$1 \equiv 37 \times 91 \pmod{187}.$$

So the inverse of 91 is 37. SO

$$x = 43 * 187 * 73 + 185 * 91 * 37 = 1209888$$

We now mod this down by $187 \times 91 = 17017$ to get 1681.
So we have

$$m^2 \equiv 1681 \pmod{17017}.$$

Let's see if 1681 has a real square root- it does, it's 41. . SO $m = 41$
END OF SOLUTION TO PROBLEM FIVE