MTH 233

Final Exam

May 11, 2021

- You have 90 minutes to work, then additional time to upload your answers. You must stop working immediately when the proctor says time is up, and if you begin uploading early, you may not change any of your answers, even if time still remains.
- You are allowed to use a basic four function calculator.
- Textbooks, additional notes, computer use besides zoom and gradescope, or communication with anyone else during the exam are not allowed.
- You must be in the zoom proctoring room with your camera on for the duration of the exam, including while uploading your work. Please stay on mute but have your volume on and chat open in case the proctor needs to reach you.
- You must write your exam on paper, not on a tablet or other device.

Before we begin, please copy the following honor pledge and sign your name. (The same honesty standards apply as detailed on the blackboard page. Cursive is not required).

I affirm that I will not give or receive any unauthorized help on this exam, and all work will be my own.

Submit your honesty pledge at the end of the exam as Question 8.

TO RECEIVE FULL CREDIT, JUSTIFY YOUR ANSWERS.

1. (12 points) Alice has just enjoyed a delicious meal, and encrypts the message

$$mmmmmmmmmmmmmmmm$$

to send to Bob. Eve knows the plaintext, and intercepts the ciphertext.

(a) If Eve knows Alice is using a Caesar cipher, can she find the key?
Yes, the first character of the ciphertext will determine the shift.

(b) If Eve knows Alice is using an affine cipher, can she find the key?
No, The plaintext would need to contain at least two different characters to determine the key.

(c) If Eve knows Alice is using a Vigenère cipher with key length 6, can she find the key?
Yes, each of the first 6 letters of the ciphertext will determine that letter of the key.

2. (14 points)

Let GF(2^4) be defined using the (irreducible) polynomial $X^4 + X + 1$.

(a) Compute $(X^3 + X^2 + 1)(X^2 + X)$ in GF(2^4). Write your answer as a polynomial of degree less than 4.

$$(X^3 + X^2 + 1)(X^2 + X) = X^5 + 2X^4 + X^3 + X^2 + X \equiv X^5 + X^3 + X^2 + X \pmod 2$$

Then dividing $X^5 + X^3 + X^2 + X$ by $X^4 + X + 1$ via polynomial long division leaves remainder X^3.

(b) Compute $(X)^{-1}$ in GF(2^4). Write your answer as a polynomial of degree less than 4.
Since $(X^3 + 1) * X = X^4 + X \equiv 1 \pmod{X^4 + X + 1}$, the inverse is $X^3 + 1$. Note that $-1 = 1$ in GF(2^4)

3. (16 points)

Alice's RSA public key is $n = 77$, and $e = 17$.

(a) Is $m = 4$, $s = 10$ a valid message and signature from Alice? Show your work.
To check, compute $10^17 \equiv 54 \neq 4 \pmod{17}$, so it's not valid. 10^17 can be computed by repeated squaring.

(b) Produce a valid signature from Alice for the message $m = 43$.
To sign, we first need Alice's private key. $77 = 7 * 11$, so we compute

$$17^{-1} \equiv 53 \pmod{(7-1)(11-1)}$$

(This can be done using the Euclidean algorithm. Then the signature is

$$s = 43^53 \equiv (43^2)^{26} \cdot 43 \equiv 43 \pmod{77},$$

Since $43^2 \equiv 1 \pmod{77}$.

4. (16 points) Let E be the elliptic curve $y^2 = x^3 + 4x + 7$ over GF(11), and let $P = (2, 1)$. Compute $4P$.
Use repeated doubling. The slope of the tangent line is $\frac{3x_0^2+4}{2y_0}$, which is $16/2 = 8$ at P. The tangent line is then

$$y = 8(x - 2) + 1.$$

Plugging this into the equation for E and computing the coefficient of x^2, we get that the x coefficient of $2P$ is $8^2 - 2 \cdot x_0 \equiv 5 \pmod{11}$. Finally, plug this into the tangent line then negate the y coordinate to reflect over the x axis, to get $2P = (5, 8)$.

To compute $4P = 2(5, 8)$, we repeat this process. The tangent slope is $\frac{3 \cdot 25+4}{16} \equiv \frac{2}{5} \equiv 7 \pmod{11}$, and the tangent line is

$$y = 7(x - 5) + 8.$$

This makes the x coordinate of $4P$ equal to $7^2 - 2 \cdot 5 \equiv 6 \pmod{11}$, and then, remembering to reflect across the x axis, $4P = (6, 7)$.

5. (16 points) Let H_1 be a hash function which produces a 256-bit message digest, and let H_2 be a hash function which produces a 160-bit message digest. Using only a brute-force attack, roughly how many computations do you expect the following to take?

(a) Finding two different messages m_1 and m_2 such that $H_1(H_2(m_1)) = H_1(H_2(m_2))$.

A birthday attack takes around $\sqrt{2^{160}} = 2^{80}$ computations to find a collision $H_2(m_1) = H_2(m_2)$, and then putting the same input into H_1 produces the same output.

(b) Finding two different messages m_1 and m_2 such that $H_2(H_1(m_1)) = H_2(H_1(m_2))$.

It takes roughly 2^{128} computations to produce a collision for H_1. But if we treat H_1 as merely producing random inputs into H_2, it will only take 2^{80} such random inputs to succeed with a birthday attack on H_1, thus 2^{80} will suffice.

(c) Finding any message m such that $H_1(H_2(m))$ has at least 60 leading zeros in binary.

(d) Finding any message m such that $H_2(H_1(m))$ has at least 60 leading zeros in binary.

For both (c) and (d), the length of the message digest doesn't matter. Exactly one in 2^{60} possible hash outputs has 60 leading zeros, so it will take on average 2^{60} tries to find such a message.

6. (10 points)

Bob's RSA public key is $n = 51$, and $e = 5$. Alice sends Bob the ciphertext $c = 9$, which you intercept. What is the message Alice intended for Bob?

We find Bob's private key: $d = 5^{-1} \equiv 13 \pmod{(3-1)(17-1)}$. Then we can decrypt by computing

$$m \equiv 9^d \equiv 9^{13} \equiv 42 \mod 51,$$

Which can be computed by repeated squaring.

7. (16 points) For each pair of computations below, state whether the second will take $0-4x$ longer than the first, or more than $1000x$ longer than the first. You do not need to explain your answers.

(a) Breaking double AES encryption —**vs**— Breaking triple AES encryption.

$> 1000x$. A meet-in-the-middle attack makes double encryption roughly as secure as single, but the same attack on triple encryption requires computing AES for all possible key pairs.

(b) Breaking triple DES encryption —**vs**— Breaking quadruple DES encryption.

$0-4x$. A meet in the middle attack on either requires computing all possible pairs of two keys, so both are about the same difficulty.

(c) Breaking triple encryption with an affine cipher —**vs**— Breaking quadruple encryption with an affine cipher.

$0-4x$. Both are equivalent to a single affine cipher, as composing affine functions just produces new affine functions.

(d) Breaking 128-bit RSA —**vs**— Breaking 256-bit RSA.

$> 1000x$. The second requires factoring a number with twice as many digits, which is much harder.

(e) Finding two different 256-bit messages with the same hash —**vs**— finding two different 256 page documents with the same hash

$0-4x$. A birthday attack on a 256-bit hash requires roughly 2^{128} Computations. This can be accomplished by finding 128 changes to make, regardless of the overall message length.

(f) Finding two different messages with the same hash —**vs**— Finding three different messages with the same hash

$> 1000x$. Suppose the hash is 256 bits (the exact length isn't important for the idea). Finding two requires $2^{256\cdot(1/2)} = 2^{128}$ computations, whereas finding three requires $2^{256\cdot(2/3)} \approx 2^{171}$

(g) Computing exponents modulo a large prime via repeated squaring —**vs**— computing ex-

ponents modulo a large prime via repeated multiplication (i.e. $a^e = \underbrace{a \cdot a \cdots a}_{e} \pmod{n}$)

$> 1000x$. Computing e^n via repeated multiplication takes $n - 1$ steps, wheras repeated squaring requires at most $2\log_2(n)$.

(h) Adding a new block to the Bitcoin blockchain in 2012 —**vs**— Adding a new block to the Bitcoin blockchain in 2021.

$0 - 4x$. The difficulty of the hash problem is adjusted so that each block takes an average of 10 minutes, no matter the computing power available.

8. (0 points) Upload your honesty statement as problem 8:

I affirm that I will not give or receive any unauthorized help on this exam, and all work will be my own.

Don't cheat, it's not worth it.