1. This Exam requires you to answer 4 questions. You must answer questions 1-2, and you are free to choose 2 from 3-5 to answer.
2. There are no trick questions on this exam.
3. Answer everything as clearly and straightforwardly as possible.
4. You have 1.5 hours for the exam, to take and then upload the results to bCourses; unlike homework you can upload as many files as needed.
5. You may handwrite OR electronically type the answers to the questions.

Problem 1. RSA (see accompanying jupyter notebook; do NOT copy-paste from the PDF)

(a) Alice sends an encrypted message to Bob. What is the ciphertext?
message = "HOW CRUEL IS THIS CRYPTO TEACHER, SCALE OF 1 - 10?"

(b) Bob replies with an unencrypted message: message = "99 mod 10"
However, Bob adds a digital signature. What is Bob's signature for this message?

(c) Bob receives the following message-signature pair from Alice, but is suspicious. Test if the signature is correct!
message = "I THINK CRYPTO IS MY FAVORITE CLASS EVER!
signature = 22758888000085724193852691178893114717312693301645350699939721514298501021678832 04

(d) Bob sends teh following message to Alice. What does it say?
ciphertext = 553242337544063901938127359395637158513623766616486868415966831881895343037509070852715754516660796643459927023214167860984456386209932686119230048500010949158231629897969516946873139268010257138003318776564784220934759350732335449187088499877444803783201883429469687709570074659216567896983389298930493828326312256223473195182706856201050541673671710116516211075959267762 99

Problem 2. Short Answer (1-3 sentences each)

(a) Explain how digital certificates (issued by Certificate Authorities) help to stop man in the middle attacks.

(b) When making an RSA key pair, the process is to choose e, then calculate d. What is the algorithm used to calculate d?

(c) In Shamir Secret Sharing, why do we need at least q (quorum) many people to come together to determine the secret?

(d) What is one reason Rabin signatures use $N = pq$ (where p and q are primes), and not $N = pqr$?

(e) What are the 3 computationally intractible problems we have studied?

(f) Which computationally intractible problem gives non-elliptic curve Diffie Hellman its security?

(g) Why is the point at infinity important for Elliptic Curves?

Taken from Hoffstein 3.12

Choose 2 of the remaining problems to answer (for a total of 4).

Problem 3. Square Roots (*mod* N)

Find two square roots of 400 (*mod* 437), using the Chinese Remainder Theorem.
Note: $437 = 19 \times 23$
Note2: There are 4 square roots; we're just asking to find two of them.

(a) Find the square roots of 400 (*mod* 19).

(b) Find the square roots of 400 (*mod* 23).

(c) Combine using Chinese Remainder Theorem to find the first root (*mod* 437).

(d) Combine using Chinese Remainder Theorem to find the second root (*mod* 437).

Problem 4. Generators (*mod* p)

(a) What calculations would you need to show that 5 is a generator (*mod* 10223)?

(b) Why is 317 not a generator (*mod* 10223)?

(c) What is the discrete log base 5 of 3529?

Problem 5. Elliptic Curve Diffie-Hellman

We'll use the following non-singular Elliptic Curve: $y^2 \equiv x^3 + 3x - 2$ (*mod* 11).
Here's a list of all the points on the curve for reference:

$$\{(0,3),(0,8),(2,1),(2,10),(3,1),(3,10),(6,1),(6,10),(10,4),(10,7)\}$$

Alice picks $a = 2$, and Bob picks $b = 3$. They use $P = (6,1)$ as a starting point.

(a) Calculate Alice's transmitted point $2P$.

(b) Alice receives $3P$ from Bob, and computes $2(3P)$ to get the point $(10,7)$.
Show the calculation of $3(2P)$ for Bob.
Does Bob's calculation match Alice's point $(10,7)$?