Note: this exam was an open-book and open-notes take-home exam.

1. [12 points] Alice and Bob wish to establish a shared secret. They partly remember how Diffie-Hellman key exchange works, but end up doing something not nearly as secure. In this problem, you will break their protocol and extract their secret key. **In this problem, you should use a computer only for basic arithmetic ($+, -, *, //$, and $\%$), and clearly show the result of your arithmetic in your written solution.**

   Alice and Bob's protocol is as follows. They work modulo the prime $p = 1009$, and share a public parameter $g = 523$. Alice will choose a secret number $a \in \mathbb{Z}/p\mathbb{Z}$, compute $A \equiv a \cdot g \pmod{p}$, and transmit A to Bob. Bob similarly will choose a secret number $b \in \mathbb{Z}/p\mathbb{Z}$, compute $B \equiv b \cdot g \pmod{p}$, and transmit B to Alice. Then Alice will compute $a \cdot B \pmod{p}$, and Bob will compute $b \cdot A \pmod{p}$; both will arrive at the same shared secret $S \equiv abg \pmod{p}$.

   You (in the role of Eve) know the public parameters $p = 1009$ and $g = 523$, and intercept the two numbers $A = 236$ and $B = 750$. Determine the shared secret S.

2. [12 points] Recall that the Chinese Remainder Theorem asserts in part that if a_1, a_2, m_1, m_2 are four integers such that $\gcd(m_1, m_2) = 1$, then there exists an integer x such that

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \text{ and} \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

   The following function is a fairly concise way to find such an integer x. It makes use of a helper function `bezout(a,b)`, which returns three integers g, u, v such that $g = \gcd(a, b)$ and $au + bv = g$.

```
def crt(a1, m1, a2, m2):
    g, u, v = bezout(m1, m2)
    return (m1*u*a2 + m2*v*a1) % (m1*m2)
```

   Prove that this function indeed returns an integer x satisfying the two desired congruences, assuming that $\gcd(m_1, m_2) = 1$.

3. [12 points] Read the description of the Menezes-Vanstone cryptosystem, on page 365 of the textbook. This system is an Elliptic Curve version of the Elgamal cryptosystem. In this problem, you will reduce breaking Menezes-Vanstone to the Elliptic Curve Discrete Logarithm problem (ECDLP).

   Suppose that Eve has succeeded in solving the ECDLP. That is, she has implemented an efficient function `ecdlp(P,Q,A,B,p)` which returns an integer n such that $n \cdot P = Q$, assuming that P and Q are points on the elliptic curve defined by $y^2 \equiv x^3 + Ax + b \pmod{p}$ for which such an integer n exists.

   Making use of this function, write a function `breakMZ(P,A,B,p,QA,R,c1,c2)`, which takes as arguments the public parameters and Alice's public key, as well as a ciphertext from Bob, and returns Bob's plaintext as a a pair of integers `m1,m2`.

   You may use all standard built-in Python functions in your solutions, and you may also assume that you've already implemented functions `ecAdd` and `ecMult` for Elliptic Curve arithmetic, and `modinv` to compute modular inverses. Any other helper functions should be implemented if needed. Your solution should be fast enough to return an answer in less than a second when the prime p is several thousand bits long.

4. [12 points] Note (2024): this problem concerns material we did not cover this semester. Let A, B be two integers, p and q two different prime numbers, and $N = pq$. Define the following three sets.

$$\begin{aligned} E_N &= \{(x,y) : \ x,y \in \mathbb{Z},\ 0 \le x,y < N,\ y^2 \equiv x^3 + Ax + B \pmod{N}\} \\ E_p &= \{(x,y) : \ x,y \in \mathbb{Z},\ 0 \le x,y < p,\ y^2 \equiv x^3 + Ax + B \pmod{p}\} \\ E_q &= \{(x,y) : \ x,y \in \mathbb{Z},\ 0 \le x,y < q,\ y^2 \equiv x^3 + Ax + B \pmod{q}\} \end{aligned}$$

These sets may be regarded as the non-infinite points on an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/q\mathbb{Z}$, respectively.

Prove that given $x, y \in \mathbb{Z}$ such that $0 \le x, y < N$, we have $(x, y) \in E_N$ if and only if *both* $(x\%p, y\%p) \in E_p$ and $(x\%q, y\%q) \in E_q$.

5. [12 points] Consider again the variant of DSA discussed in Problem 3 of the second midterm exam. For convenience, the description of that system is reproduced below.

The system uses the same public parameters p, q, g as DSA (notation as in Table 4.3 of the textbook). Rather that publishing a single verification key A, Samantha chooses *two* secret signing keys a_1, a_2, and publishes two verification keys A_1, A_2 such that

$$\begin{aligned} A_1 &\equiv g^{a_1} \pmod{p}, \text{ and} \\ A_2 &\equiv g^{a_2} \pmod{p}. \end{aligned}$$

A signature on a document D consists of a pair of integers (S_1, S_2). When he receives a document D with signature (S_1, S_2), Victor will use the following verification procedure.

- Compute $V_1 \equiv DS_2^{-1} \pmod{q}$ and $V_2 \equiv S_1 S_2^{-1} \pmod{q}$ (as in DSA).
- Verify that
$$\left((A_1^{V_1} A_2^{V_2})\%p\right)\%q = S_1.$$
(If this equation is false, the signature is considered invalid.)

Now suppose that Eve wishes to produce a *blind signature* for this system. That is, she will create a document D and valid signature (S_1, S_2) (but she will not be able to choose the document in advance; this is why it is called a "blind" signature). She begins by creating the number S_1 as follows: she chooses two random integers i, j with $1 \le i, j \le q - 1$, and then she computes

$$S_1 = (A_1^i A_2^j)\%p\%q.$$

Describe a procedure Eve could now follow to *efficiently* find integers D and S_2 such that (S_1, S_2) satisfies the verification equation for document D. Prove that the procedure you describe will indeed satisfy the verification equation. You need not write your solution as code, but it should be clear that this can be done in an efficient way.

6. [12 points] Samantha and Victor are using DSA for digital signatures. The smaller prime q from the public paramters is $q = 1009$. Samantha has published the following two documents with valid signatures.

D	S_1	S_2
930	142	492
648	142	330

Eve examines these two signatures and observes that both have the same value of S_1, and on this basis she correctly guesses that Samantha reused the same ephemeral key to make both signatures. Exploit this blunder and determine Samantha's secret signing key a. **In this problem, you should use a computer only for basic arithmetic ($+, -, *, //$, and %), and clearly show the result of your arithmetic in your written solution.**

Note: the parameters p, g and Samantha's public key A have not been provided in this problem, even though of course Eve would normally have access to them. This is done so that the numbers can be small enough to solve the problem on paper (using a computer for arithmetic) without making a brute-force attack possible.

7. [12 points] Suppose that p is a prime number, g and h are units modulo p, and M, N are two positive integers. Define a "baby step list" as follows.

$$\texttt{bslist} = \left[1,\ g,\ g^2\%p,\ g^3\%p,\ \cdots, g^{M-1}\%p\right]$$

Also define a "giant step list" as follows.

$$\texttt{gslist} = \left[h,\ hg^{-M}\%p,\ hg^{-2M}\%p,\ \cdots,\ hg^{-(N-1)M}\%p\right]$$

Prove that `bslist` and `gslist` have an element in common if and only if there exists an integer x such that $0 \le x < MN$ and $g^x \equiv h \pmod{p}$.

8. [12 points] Note (2024): this problem concerns material that we mentioned only briefly this semester, so I would not ask a question like this on our exam. Suppose that a prime number q has been chosen, and we now wish to select a second prime number p such that $p \equiv 1 \pmod{q}$ (this is done in DSA parameter creation, for example). To do so, we will select an integer k at random, compute $n = 1 + kq$, check whether or not it is prime, and keep trying new values of k until we succeed. This problem attempts to estimate the probability of success with one randomly chosen k. To make the situation more specific, suppose that we will first choose an integer N, and select k at random from the set $\{k \in \mathbb{Z} :\ N \le k \le 2N\}$. For any integer N, define

$$P(q, N) = [\text{Probability that } 1 + kq \text{ is prime if } k \text{ is chosen at random subject to } N \le k \le 2N]\,.$$

Find, with proof, a simple function of q and N that can be filled into the box below so that the following statement is true.

$$\lim_{N\to\infty} \frac{P(q,N)}{\boxed{}} = 1$$

You should use the "Prime number theorem, congruence version" stated in class on 3/24 (this theorem was stated without proof, and you do not need to prove it. To prove it is far beyond

the scope of this course, but you may see a proof if you take a course in Analytic Number Theory, e.g. Math 460 in the Fall).