Rules: Students should work alone. Always show your work; if you use a programming platform (Python, Mathematica, etc) for a computation, write the set of commands that produced the result. Upload a SINGLE PDF file using the Dropbox link. Make sure it is easily readable.

The deadline for uploading via Dropbox: **10:00pm Monday, March 16**

1. (2 pts) Use the extended Euclidean algorithm to compute the GCD$(150, 211)$ and the inverse of 150 mod 211. Show the steps and all temporary values.
2. (2 pts) Use the Fermat's Little Theorem to compute the inverse of 17 modulo 2017. Show the steps and all temporary values.
3. (2 pts) Use Euler's Theorem to compute the inverse of 81 modulo 323. Show the steps and all temporary values.
4. (4 pts) List Fermat's liars for the composite number 2431. What is the probability that a randomly selected $a < 2431$ is a witness?
5. (2 pts) Use Miller-Rabin to prove that 8911 is a composite number. Show the steps and all temporary values.
6. (6 pts) Consider the prime $p = 9973$ and the primitive element $g = 11$.
   (a) Show the steps of the Diffie-Hellman between Alice and Bob such that they select the secret values as $a = 4096$ and $b = 8192$. What are the values of g^a and g^b? What is the value of the agreed secret key?
   (b) Assume the adversary captures $y = 1985$ for an unknown x such that $y = 11^x \pmod p$. How many such x exist and why so? How many values of x you must (exhaustively) search to find x?
   (c) Assume the adversary captures $y = 1985$ for an unknown x such that $y = 2^x \pmod p$. How many such x exist and why so? How many values of x you must (exhaustively) search to find x?
7. (2 pts) Consider the RSA modulus $n = 98563159$. Since n is small, we can easily factor it by trial division. However, there is a faster way to factor n with the knowledge of $\phi(n)$. Given $\phi(n) = 98543304$, factor n.
8. (6 pts) Let p a prime of length k bits. Consider the following hash function $H(x) = x^2 \pmod p$ which maps the message x (unlimited length) to a k-bit hash value $H(x)$.
   a) Is this hash function one way (pre-image resistant)? Explain.
   b) Is it second pre-image resistant? Compute a second pre-image, if it is not.
   c) Is it collision resistant? Obtain two colliding messages, if it is not.
9. (6 pts) Consider the ElGamal public-key encryption parameters $(g, p) = (11, 9973)$ and the private key $x = 2014$.
   a) Compute the public key.
   b) Encrypt $m = 1000$ with the random number $r = 997$ and obtain the ciphertexts (c_1, c_2).
   c) Decrypt the ciphertext to obtain the message back.
10. (10 pts) Given the 3-digit prime $q = 991$, perform the DSA setup/sign/verify.
    a) Generate the 6-digit prime p ($> 10^5$) such that $q|(p-1)$.
    b) Find the qth root of unity mod p, denoted as g.
    c) Generate the random private key x and compute the public key y.
    d) Sign the message $H(m) = 10$ and obtain (s_1, s_2)
    e) Verify the signature on the message.