MATH/CMSC 456 (Washington) Final Exam Spring 2018 Name: _____

This exam has 8 pages and is worth 140 points. Solve each problem in the space provided and clearly indicate your answer. If you need more space, use the reverse side of the page and indicate that you have done so. You must show your work to receive credit for a problem.

You may use calculators.

Sign the following Honor Pledge:
I pledge on my honor that I have not given or received any unauthorized assistance on this examination.
Sign here: _____

1. (10 points = 5+5) Alice uses an improvement of the Vigenère cipher: She writes all the letters in the plaintext as numbers mod 26 in the standard way (with $a = 0$ and $z = 25$) and she chooses an integer b and integers $a_1, a_2, \ldots, a_5$. She applies the affine functions $a_1x + b, a_2x + b, \ldots, a_5x + b \pmod{26}$ as in Vigenère (so a_1x+b is used on the 1st, 6th, 11th, ... letters, $a_2x + b$ is used on the 2nd, 7th, 12th, ... letters, etc.).
(a) What condition do $a_1, a_2, \ldots, a_5$ need to satisfy for Bob (who knows the key) to be able to decipher the message?
(b) Describe a chosen plaintext attack that will yield the key. You know the encryption method and you know the key length. You must *explicitly* say what plaintexts you use.

(a) $\gcd(a_i, 26) = 1$

(b) plaintext : aaaaabbbbb = 0000011111

the output is $a_1, a_2, \cdots, a_5, a_1+b_1, \cdots, a_5+b_5$.

This yields a_i's and b_i's.

2. (20 points = 5+5+5+5) At the end of the semester, the professor randomly chooses and sends one of two possible messages:
$m_0 = YOUPASSED$ and $m_1 = YOUFAILED$.
To add to the excitement, the professor encrypts the message using one of the following methods:
(a) Shift cipher
(b) Vigenère cipher with key length 3
(c) RSA with a public 300-digit modulus n and encryption exponent $e = 65537$ (the message is not padded with extra bits)
(d) One-time pad
You receive the ciphertext and want to decide (in less than one minute, but you have a computer) whether the professor sent m_0 or m_1. For each method (a), (b), (c), and (d), explain how to decide which message was sent or explain why this is impossible. (*Notes:* You may assume that you know which method is being used. For the Vigenère, do not use frequency analysis; the message is too short.)

(a) First letter determines the shift. Then decrypt.
Or, see if 6th letter = 7th letter in ciphertext.

(b) First 3 letters determine key. Then decrypt.

(c) Encrypt m_0 and m_1 and see which gives the ciphertext.

(d) Can't tell because of perfect secrecy of one-time pad.

3. (20 points = 10+5+5) Huey, Dewey, and Louie ask their uncle Donald, "Is $n = 19887974881$ prime or composite?" Donald replies, "Yes." Therefore, they decide to obtain more information on their own.

(a) Huey computes $13^{(n-1)} \equiv 16739180549 \pmod{n}$. What does he conclude?

(b) Dewey computes $7^{n-1} \equiv 1 \pmod{n}$, and he does this by computing

$$\begin{aligned} 7^{(n-1)/32} &\equiv 1992941816 \pmod{n} \\ 7^{(n-1)/16} &\equiv 19887730619 \\ 7^{(n-1)/8} &\equiv 1 \\ 7^{(n-1)/4} \equiv 7^{(n-1)/2} &\equiv 7^{(n-1)} \equiv 1. \end{aligned}$$

What information can Dewey obtain from his calculation that Huey does not obtain?

(c) Louie notices that $19857930655^2 \equiv 123^2 \pmod{n}$. What information can Louie compute? (in parts (b) and (c), you do not need to do the calculations, but you should indicate what calculations need to be done)

(a) $n \neq$ prime, by Fermat

(b) $\gcd(19887730619-1, n) =$ non-trivial factor of n

(c) $\gcd(19857930655-123, n) =$ non-trivial factor of n

4. (10 points) Suppose Eve factors Alice's RSA modulus n and obtains p and q. Eve knows Alice's encryption exponent e and has intercepted a ciphertext c that Bob has sent to Alice. Explain all of the steps that Eve uses to recover the message m that Bob encrypted ($c \equiv m^e \pmod{n}$). Indicate at each step what algorithm is used to perform the computation. (That is, if some method other than the obvious naive method needs to be used, say what it is. In particular, there are two methods that need to be mentioned.)

Eve computes d satisfying $de \equiv 1 \bmod (p-1)(q-1)$ using Extended Euclidean Algorithm.
She computes $c^d \pmod{n}$ using modular exponentiation (successive squaring).
This yields m.

5. (10 points) The Modulus Supply Company sells RSA moduli. To save money, it has one 300-digit prime p and, for each customer, it randomly chooses another 300-digit prime q (different from p and different from q supplied to other customers). Then it sells $n = pq$, along with encryption and decryption exponents, to unsuspecting customers.

(a) Suppose Eve suspects that the company is using this method of providing moduli to customers. How can she read their messages? (as usual, the modulus n and the encryption exponent e for each customer are public information)

(b) Now suppose that the customers complain that Eve is reading their messages. The company computes a set S of 10^6 primes, each with 300 digits. For each customer, it chooses a random prime p from S, then randomly chooses a 300-digit prime q, as in part (a). The 100 customers who receive moduli $n = pq$ from this update are happy and Eve publicly complains that she no longer can break their systems. As a result, 2000 more customers buy moduli from the company. Explain why the 100 customers probably have distinct primes p, but among the 2000 customers there are probably two with the same p.

(a) Eve takes 2 modali, n_1 and n_2 and computes $\gcd(n_1, n_2) = p$.
Then she can factor every n_i and read the messages.

(b) $r = 2000 > \sqrt{N} = \sqrt{10^6}$

Birthday attack $\Rightarrow$ we expect 2 to have the same p.

6. (10 points) Alice and Bob (and no one else) share a key K. Each time that Alice wants to make sure that she is communicating with Bob, she sends him a random string S of 100 bits. Bob computes $B = H(S||K)$, where H is a good cryptographic hash function, and sends B to Alice. Alice computes $H(S||K)$. If this matches what Bob sent her, she is convinced that she is communicating with Bob.
(a) What property of H convinces Alice that she is communicating with Bob?
(b) Suppose Alice's random number generator is broken and she sends the same S each time she communicates with anyone. How can Eve (who doesn't know K, but who intercepts all communications between Alice and Bob) convince Alice that she is Bob?

(a) Collision resistance: If Bob's hash is equal to $H(S||K)$, Alice assumes Bob must have hashed $S||K$. (If Bob sends a random B (≠ hash), it probably won't $= H(S||K)$.)

(b) Bob sends the same $B = H(S||K)$ each time. Eve can send this, too, since she has intercepted B.

7. (15 points = 5+5+5) **(a)** Alice claims that she knows who will win the next World Cup. She takes the name of the team, T, and encrypts it with a one-time pad K, and sends $C = T \oplus K$ to Bob. After the World Cup is finished, Alice reveals K, and Bob computes $T = C \oplus K$ to determine Alice's guess. Why should Bob not believe that Alice actually guessed the correct team, even if $T = C \oplus K$ is correct?
(b) To keep Alice from changing K, Bob requires Alice to send not only $C = T \oplus K$ but also $H(K)$, where H is a good cryptographic hash function. How does the use of the hash function convince Bob that Alice is not changing K?
(c) In the procedure in (b), Bob receives C and $H(K)$. Show how he can determine Alice's prediction, without needing Alice to send K? (*Hint:* There are fewer than 100 teams T that could win the World Cup.)

(a) Suppose T' wins. Alice chooses K' so that $C = T' \oplus K'$, and sends K' to Bob.

(b) Collision resistant: $H(K) = H(K') \Rightarrow$ probably $K = K'$.

(c) Since $K = C \oplus T$, Bob computes $H(C \oplus T)$ for each team T and sees which T yields $H(K)$.

8. (10 points) Bob has an elliptic curve E mod some prime and he has computed a secret integer n such that $nP = \infty$ for each point P on E. He chooses integers d and e such that $de \equiv 1 \pmod{n}$. He makes E and e public, and keeps d and n secret. Alice wants to send a message to Bob, and the message is represented as a point M on E. Alice computes $C = eM$, which is a point on E, and sends C to Bob. Bob computes dC. Show that dC is the original message M.

$dC = deM$

Write $de = 1 + kn$ for some k.

Then

$deM = M + knM = M + k(\infty) = M + \infty = M$ ✓

(Writing $d \equiv e^{-1} \Rightarrow deM \equiv e^{-1}eM \equiv 1$ does not explain why M is being used.)

9. (10 points) Let p be a large prime, let g be a primitive root mod p, and let $b \not\equiv 0 \pmod{p}$. Peggy claims to know an integer s such that $g^s \equiv b \pmod{p}$. Give a zero knowledge procedure for Peggy to convince Victor that she knows s (Victor does not know s). The first step should be "Peggy chooses a random integer $r_1 \pmod{p-1}$ and lets $r_2 \equiv s - r_1 \pmod{p-1}$."

(1) step given.

(2) P computes $h_i \equiv g^{r_i} \bmod p$ for $i = 1, 2$, and sends h_1, h_2 to Victor

(3) V checks that $h_1 h_2 \equiv b \pmod{p}$

(4) V chooses $i = 1$ or 2 and asks for r_i.

(5) P sends r_i and V checks that $h_i \equiv g^{r_i} \pmod{p}$.

(6) Repeat several times.

10. (10 points) Bob has a good cryptographic hash function H, but he is worried that it is not good enough. He has taken a cryptography course (it's not known whether he passed), so he knows discrete logs are hard. Therefore, he chooses a 300-digit prime p and a primitive root g mod p. He strengthens his hash function by combining it with a discrete log: $h(m) = H(g^m \pmod p)$. This yields a hash function that is slow to compute, but this is a sacrifice that Bob is willing to make, since he mistakenly thinks he has made a better hash function. Give another property of hash functions that h does not satisfy, and justify your answer.

$h(m+p-1) = H(g^m g^{p-1} \pmod p) = H(g^m \bmod p) = h(m)$

↑ Fermat

So collisions are easy to find.

11. (10 points = 5+5) In the setup of the ElGamal signature scheme, Alice chooses a prime p, a primitive root g mod p, and a secret integer a. She computes $h \equiv g^a \pmod p$. The numbers p, g, h are made public, and a is kept secret. To sign a message, Alice chooses a random integer k with $\gcd(k, p-1) = 1$ and computes

$$r \equiv g^k \pmod p, \qquad s \equiv k^{-1}(m - ar) \pmod{p-1}.$$

The signed message (m, r, s) is valid if $g^m \equiv h^r r^s \pmod p$.
(a) Why is $\gcd(k, p-1) = 1$ required?
(b) Suppose Eve finds a valid signed message $(*, r, s)$ but the message * is unreadable. How difficult is it for Eve to find a message m for which these r and s give a valid signed message (m, r, s)? Explain your answer.

(a) So that $k^{-1} \pmod{p-1}$ exists.

(b) Eve needs to find m with $g^m \equiv h^r r^s \pmod p$.
This is a discrete log problem, so it's probably hard.

12. (5 points) The following was encrypted by a shift cipher with shift of -1. Find the plaintext:
GZUDZFNNCRTLLDQ

HAVEAGOODSUMMER