CMSC/ENEE/MATH 456 (Washington) Exam 2 Fall 2019 Name: _____

This exam has 5 pages. 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) There are approximately 3×10^{147} primes with 150 digits. There are approximately 10^{85} particles in the universe. If each particle chooses a random 150-digit prime, do you think two particles will choose the same prime? Explain why or why not.

$r = 10^{85}$, $N = 3 \times 10^{147}$.
Since r is much larger than $\sqrt{N}$, we expect a match; namely, two particles with the same prime.
More precisely, the probability of a match is approximately
$1 - e^{-r^2/2N} = 1 - e^{-10^{23}/6} \approx 1.000\ldots$

2. (10 points) Suppose we design a hash function H. If we break the message into blocks as $M = M_1||M_2||\cdots||M_n$, where the M_i are blocks of length 512, then $H(M) = M_1 \oplus M_2 \oplus \cdots \oplus M_n$. Alice signs messages by signing the hash of the message. Suppose Alice signs the message

[Don't][promote][Eve;][dismiss][her.],

where each phrase in brackets is a block, padded to get 512 bits. Show how Eve can use this signature to forge Alice's signature on another document that is much more favorable to Eve.

The message
[Don't][dismiss][Eve][promote][her]
has the same hash as the original message. Therefore, Alice's signature on the hash of the original message is also valid for the hash of this more favorable message.

3. (20 points) Here is a variant of the ElGamal signature scheme. Alice chooses a prime p, a primitive root α, and a secret integer a. She computes $\beta \equiv \alpha^a \pmod{p}$. The numbers p, α, β are made public, and a is kept secret. Alice signs m as follows:

(1) She chooses k and computes $r \equiv \alpha^k \pmod{p}$, with $0 < r < p$.

(2) She computes $s \equiv ar + km \pmod{p-1}$.

The signed message is (m, r, s).

(a) Show that if Alice signs correctly, then the verification equation $\alpha^s = \beta^r r^m \pmod{p}$ is true.

$\beta^r r^m \equiv (\alpha^a)^r (\alpha^k)^m \equiv \alpha^{ar+km} \equiv \alpha^s \pmod{p}$

(b) Suppose Alice uses $k = a$. How does Eve recognize this, and how does Eve use this information to break the system (by finding a)?

If $k=a$, then $r=\beta$.

Then

$s \equiv ar + km \equiv a(r+m) \pmod{p-1}$.

There are $\gcd(r+m, p-1)$ values of a that satisfy this congruence. Try each a and see which gives $\beta \equiv \alpha^a \pmod{p}$.

(c) What theorem tells us that the congruence for s should be mod $p-1$?

Fermat's Theorem.

(d) Eve tries to forge Alice's signature on a message m. Eve chooses m and r and tries to find an appropriate s. Why does s exist and why should it be hard to find s?

Eve needs to solve $\alpha^s \equiv \beta^r r^m \pmod{p}$ for s.

This is a discrete log problem, so it's probably hard.

There is a solution s because α is a primitive root.

(it is not because we can take $s \equiv ar+km$, because then the question is why k exists: Answer: because α = prim. root).

4. (14 points) Suppose n is a large odd number. You calculate $2^{(n-1)/2} \equiv k \pmod{n}$, where k is some integer with $k \not\equiv \pm 1 \pmod{n}$.

(a) Suppose $k^2 \not\equiv 1 \pmod{n}$. Explain why this implies that n is not prime.

$2^{n-1} \equiv \left(2^{(n-1)/2}\right)^2 \equiv k^2 \not\equiv 1 \pmod{n}$.

The Fermat test says n must be composite.

(b) Suppose $k^2 \equiv 1 \pmod{n}$. Explain how you can use this information to factor n.

$k^2 \equiv 1^2 \pmod{n} \implies \gcd(k-1, n) =$ non-trivial factor of n.

$k \not\equiv \pm 1$

5. (6 points) Alice uses RSA signatures with a hash function H, so (m, s) is valid if $H(m) \equiv s^e \pmod{n}$ (where n, e are the usual RSA parameters). Eve tries to find a document m on which she can forge Alice's signature (she doesn't care what m is, even if it's meaningless). Eve chooses s and then looks for an m such that (m, s) is valid. Why will it be hard for Eve to find such an m?

Eve has chosen m. The number e is public. So Eve needs to solve

$$H(m) \equiv s^e \pmod{n}$$

for m. The preimage resisistance of H means it's hard for Eve to find an m satisfying this.

6. (10 points) You have a random 500-digit prime p, and some people want to store passwords, written as numbers. If x is the password, then the number $2^x \pmod p$ is stored in a file. When y is given as a password, the number $2^y \pmod p$ is compared with the entry for the user in the file. Suppose Eve gains access to the file. Why is it hard for her to deduce the passwords?

Eve sees a number y in the file. She needs to find the password x with $2^x \equiv y \pmod p$. This is a discrete log problem, which is probably hard.

7. (10 points) Alice's RSA public key is (n, e) and her private key is d. Recall that a document with an RSA signature (m, s) is valid if $m \equiv s^e \pmod n$. Bob wants Alice to sign a document m but he does not want Alice to read the document. Assume $m < n$. They do the following:

1. Bob chooses a random integer k with $\gcd(k, n) = 1$. He computes $m_1 \equiv k^e m \pmod n$.
2. Alice signs m_1 by computing $s_1 \equiv m_1^d \pmod n$.
3. Bob divides s_1 by k mod n to obtain $s \equiv k^{-1} s_1 \pmod n$.

(a) Show that (m, s) is valid.

(m,s) is valid if $m \equiv s^e \pmod n$, so we need to compute s^e:

$$s^e \equiv (k^{-1}s_1)^e \equiv k^{-e} m_1^{de} \equiv k^{-e} m_1 \equiv k^{-e}(k^e m) \equiv m$$

because RSA encryption-decryption works

(b) Why is it assumed that $\gcd(k, n) = 1$?

In step 3, Bob needs $k^{-1} \pmod n$.

8. (10 points) Suppose Alice signs contracts using a 30-bit hash function h (and h is known to everyone). If m is the contract, then $(m, sig(h(m)))$ is the signed contract (where *sig* is some public signature function). Eve has a file of 2^{20} fraudulent contracts. She finds a file with 2^{20} contracts with valid signatures (by Alice) on them. Describe how Eve can accomplish her goal of putting Alice's signature on at least one fraudulent document. Eve is not allowed to compute more than 2^{20} hash values.

Eve chooses 2^{19} contracts that Alice has signed,
Eve choose 2^{19} fraudulent contracts,
She makes two lists of length 2^{19}:
(1) Hash(Alice contract) for the 2^{19} chosen contracts,
(2) Hash(fraudulent contract) for the 2^{19} chosen fraudulent contracts
(This is $2^{19}+2^{19}=2^{20}$ hashes).
Since $r=2^{19}$ is much larger than $\sqrt{N}=\sqrt{2^{30}}$, we expect a match.
Alice's existing signature on the contract is also valid on the matching fraudulent one.

9. (10 points) Recall the Diffie-Hellman protocol. Alice and Bob choose a large prime p and a primitive root α. Alice chooses a secret a and Bob chooses a secret b. Alice computes $A \equiv \alpha^a \pmod{p}$ and sends A to Bob. Bob computes $B \equiv \alpha^b \pmod{p}$ and sends B Alice. Alice computes $C \equiv B^a \pmod{p}$, and Bob computes $C \equiv A^b \pmod{p}$. Eve intercepts all of these communications between Alice and Bob.

(a) Show that if Eve can compute discrete logs, then she can also compute C.

Eve sees A, B and computes b.
Then she computes $A^b \equiv C$.

(b) Suppose that Alice chooses $a = (p-1)/2$. Show how Eve can figure out C. You may assume that Eve has figured out that $a = (p-1)/2$. (You get partial credit for reducing the problem to looking at a small set of possibilities for C.)

Ignore.