MATH/CMSC 456 (Washington) Final Exam May 15, 2014 Name:_____

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. (15 points = 6+3+6) **(a)** Suppose you use an affine cipher. The plaintext consists of two letters and the encryption function is $y \equiv 21x + 2 \pmod{26}$. The ciphertext is the first two letters of your last name (for me the ciphertext is WA). Find the plaintext.

(b) The matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is not suitable for the matrix in a Hill cipher. Why?

(c) You are told that

$$3^{675} \equiv 2071 \pmod{2701}, \quad 3^{1350} \equiv 2554 \pmod{2701}, \quad 3^{2700} \equiv 1 \pmod{2701}.$$

Use this information to factor 2701. You must use this information and show how you obtain the answer. Just giving the factorization will receive no credit.

2. (15 points) Eve loves to do double encryption. She starts with a message m. First, she encrypts it twice with a one-time pad (the same one each time). Then she encrypts the result twice using a Vigenère cipher with key $NANANA$. Finally, she encrypts twice with RSA using modulus $n = pq = 7919 \times 17389$ and exponent $e = 66909025$. It happens that $e^2 \equiv 1 \pmod{(p-1)(q-1)}$. Show that the final result of all this encryption is the original plaintext. Explain your answer fully. Simply saying something like "decryption is the same as encryption" is not enough. You must explain why.

3. (15 points = 10+5) **(a)** Alice and Bob have the same RSA modulus n. Alice has encryption exponent e_A and decryption exponent d_A, and Bob has e_B and d_B. Alice wants to send a message m to Bob. She computes $c_1 \equiv m^{e_A} \pmod{n}$ and sends c_1 to Bob. Bob computes $c_2 \equiv c_1^{e_B} \pmod{n}$ and sends c_2 to Alice. Alice computes $c_3 \equiv c_2^{d_A} \pmod{n}$ and sends c_3 to Bob. Bob computes $c_4 \equiv c_3^{d_B} \pmod{n}$. Show that $c_4 \equiv m \pmod{n}$.
(b) If Eve finds out Bob's e_B and d_B, how can she use this information to find Alice's d_A ? (Eve already knows e_A and n.)

4. (10 points = 5+5) **(a)** Suppose n is a product of two large primes. For a certain algorithm, Nelson needs to choose an elliptic curve E mod n along with a point P ($\neq \infty$) on E. He does not know p and q. Here is his strategy. He first chooses integers A and B and considers the curve $y^2 \equiv x^3 + Ax + B \pmod{n}$. He then tries $x = 1, 2, 3, \ldots$ until he finds an x such that $x^3 + Ax + B$ is a square mod n and lets y be a square root of $x^3 + Ax + B$ mod n. Why will this strategy probably not allow Nelson to find a point on E?
(b) Give a strategy that will allow Nelson to find some elliptic curve E mod n along with a point P ($\neq \infty$) on E.

5. (15 points = 5=5+5) Recall the RSA signature scheme: m is Alice's document, $n = pq$ is Alice's RSA modulus, and e and d are her RSA encryption and decryption exponents. Alice signs m by computing $s \equiv m^d \pmod{n}$, so the signed message is (m, s). Bob verifies the signature by checking that $s^e \equiv m \pmod{n}$.

(a) Eve want to produce Alice's signature on the document $m = 123456789$. Why is this difficult? Explain this by stating what difficult cryptographic problem must be solved. (Do not say that it's because Eve does not know d. Why isn't there another way to produce s?)

(b) Eve wants to produce a valid signed message with $s = 112090305$ (= ALICE, when A=01, B=02, etc.; Eve thinks this is how digital signatures work). How does Eve find an appropriate message?

(c) Recall the equations for the ElGamal signature scheme: g is a primitive root mod p, $h \equiv g^a \pmod{p}$. The signed message is (m, r, s). Bob verifies by checking that $g^m \equiv r^s h^r \pmod{p}$.

If $r \not\equiv 0 \pmod{p}$ and s are chosen randomly, explain why there is always an m such that (m, r, s) is a valid message and also explain why it is difficult for Eve to find such an m (do not say it's because Eve doesn't know Alice's secret information. Instead, state what difficult problem must be solved.)

6. (15 points = 5+5+5) Let E be an elliptic curve mod a large prime, let N be the number of points on E, and let P and Q be points on E. Peggy claims to know an integer s such that $sP = Q$. She wants to prove this to Victor by the following procedure. Victor knows E, P, and Q, but he does not know s and should receive no information about s.

1. Peggy chooses a random integer r_1 mod N and lets $r_2 \equiv s - r_1 \pmod{N}$. (Don't worry about why it's mod N. It's for technical reasons.)
2. Peggy computes $Y_1 = r_1 P$ and $Y_2 = r_2 P$ and sends Y_1 and Y_2 to Victor.
3. Victor checks something.
4. Victor randomly chooses $i = 1$ or 2 and asks Peggy for r_i.
5. Peggy sends r_i to Victor.
6. Victor checks something.
7. Step (7).

(a) What does Victor check in step (3)?
(b) What does Victor check in step (6)?
(c) What should step (7) be if Victor wants to be at least 99.9% sure that Peggy knows s?

7. (15 points = 5+5+5) **(a)** 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.
(b) Suppose a message is divided into blocks of length 160 bits:

$$m = M_1 \,||\, M_2 \,||\, \cdots \,||\, M_\ell.$$

Let

$$h(m) = M_1 \oplus M_2 \oplus \cdots \oplus M_\ell.$$

Which properties of a cryptographic hash function does h satisfy and which does it not satisfy? Justify your answers.
(c) Alice says that she is willing to sign a petition to save koala bears. Alice's signing algorithm uses a hash function H that has an output of 60 bits (so she actually signs the hash of the document). Describe how Eve can trick Alice into signing a statement allowing Eve unlimited withdrawals from Alice's bank account.