MATH/CMSC 456 (Washington) Final Exam Spring 2017

You may use calculators.

1. (10 points) Explicitly describe how to do a chosen plaintext attack on an affine cipher.
2. (10 points) Suppose you modify the LFSR method to work mod 5 and you use a (not quite linear) recurrence relation

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} + 2 \pmod 5,$$

with $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0$. Find the coefficients c_0 and c_1.
3. (10 points) You are trapped on a desert island and have only a four-function calculator. Use the information that $1208^2 \equiv 1 \pmod{2201}$ to factor 2201. You must use the given information, and you must obtain explicit factors. You cannot use gcd or factor commands on your calculator. You must give all the steps that are not simply $+, \times, -$, and dividing.
4. (10 points) Let E_K denote DES encryption with key K. Suppose there is a public database Y consisting of 10^{10} DES keys and there is another public database Z of 10^{10} binary strings of length 64. Alice has five messages $m_1, m_2, \ldots, m_5$. She chooses a key K from Y and a string B from Z. She encrypts each message m by computing $c = E_K(m) \oplus B$. She uses the same K and B for each of the messages. She shows the five plaintext-ciphertext pairs (m_i, c_i) to Eve and challenges Eve to find K and B. Alice knows that Eve's computer can do only 10^{15} calculations, and there are 10^{20} pairs (K, B), so Alice thinks that Eve cannot find the correct pair. However, Eve has taken a crypto course. Show how she can find the K and B that Alice used. You must state explicitly what Eve does. Statements such as "Eve makes a list" are not sufficient; you must include what is on the lists and how long they are.
5. The operator of a Vigenère cipher is bored and encrypts a plaintext consisting of the same letter of the alphabet repeated 300 times. The key is a 5-letter English word with distinct letters. Eve knows that the key is a word but does not yet know its length.
(a) (5 points) What property of the ciphertext will make Eve suspect that the key length is five?
(b) (5 points) Suppose Eve does not notice the property in part (a) and therefore she uses the method of displacing and then counting matches for finding the length of the key. What will the number of matches be for the various displacements from 1 up to a displacement by 6? (Your answers can vary by a small amount depending on whether or not you wrap around when counting displacements; either way is ok.)
6. (10 points) Suppose a message m is chosen randomly from the set of all 5-letter English words and is encrypted using an affine cipher mod 26, where the key is chosen randomly from the 312 possible keys. The ciphertext is $HHGZC$. Compute the conditional probability $\text{Prob}(m = HELLO \mid c = HHGZC)$. Use the result of this computation to determine whether of not affine ciphers have perfect secrecy.
7. (10 points) The Prime Supply Company has a collection of 10^8 primes, each with 400 digits. When a customer needs a prime, the company randomly chooses a prime from their collection and sells it to the customer. If 10^5 customers buy primes, determine whether or not it is likely that two customers buy the same prime.
8. You are possibly graduating from crypto school. At the ceremony, you are handed a certificate, but it is encrypted. Of course, you have partially hacked their system, so you know the certificate says one of two things:
ZEROKNOWLEDGE or YOUHAVEPASSED
(a) (5 points) Suppose the certificate was encrypted by a Vigenère cipher with key length 3, and the diploma reads ZQXICYFRDTUHE. Determine what the plaintext is.
(b) (5 points) Suppose the certificate was encrypted using the basic RSA method: $c \equiv m^e \pmod n$, where n and e are public. How can you decide which is the message ?
(c) (5 points) Describe how the crypto school can modify the RSA encryption method so that you cannot tell which message was encrypted (but so that the school, which knows the decryption exponent d, can decrypt the certificate for a small fee)?
9. (10 points) Suppose Alice's RSA public key is $(n, e) = (221, 7)$. Find her decryption exponent d. You may use the fact that $221 = 13 \cdot 17$.
10. Let E be an elliptic curve mod n (where n is some integer) and let P and Q be points on E with $2P = Q$. The curve E and the point Q are public and are known to everyone. The point P is secret. Peggy

wants to convince Victor that she knows P. They do the following procedure:
1. Peggy chooses a random point R_1 on E and lets $R_2 = P - R_1$.
2. Peggy computes $H_1 = 2R_1$ and $H_2 = 2R_2$ and sends H_1, H_2 to Victor.
3. Victor checks that $H_1 + H_2 = Q$.
4. Victor makes a request and Peggy responds.
5. Victor now does something else.
6. They repeat steps 1 through 5 several times.

(a) (5 points) Describe what is done in steps 4 and 5.
(b) (5 points) Give a classical (non-elliptic curve) version of this protocol that yields a zero-knowledge proof that Peggy knows a solution x to $x^2 \equiv s \mod n$.

11. (10 points) Suppose a message is divided into blocks of 256 bits: $m = M_1||M_2||\cdots||M_n$. Let

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

Which of the three properties of a cryptographic hash function does h satisfy, and which does it not satisfy? Justify your answers.

12. Consider the following signature scheme (it is similar to the ElGamal scheme). Alice chooses a large prime p and a primitive root g mod p. She chooses a secret random integer a and computes $h \equiv g^a \pmod p$. The numbers p, g, h are made public, but a is kept secret. To sign a document m, Alice chooses a random integer k and computes $r \equiv g^k \pmod p$ and $s \equiv kr - am \pmod N$, for some N. The signed document is (m, r, s). The verification congruence is $r^r \equiv h^m g^s \pmod p$.
(a) (10 points) Give an appropriate value of N and show that if the signing procedure is followed then the verification congruence holds.
(b) (5 points) Suppose Eve wants to forge Alice's signature on a certain document m. Eve chooses $r = 5$ and needs to find s such that $(m, 5, s)$ is a valid signed document. Why will it be difficult for Eve to find s?
(c) (5 points) The signing procedure is much more efficient if Alice signs the hash of m. Let H be a hash function. Give the congruences that are used to sign m using the hash function H:

13. An unenlightened professor asks his students to memorize the first 1000 digits of π for the exam. To grade the exam, he uses a 100-digit hash function H. Instead of carefully reading the students' answers, he hashes each of them individually to obtain binary strings of length 100. Your score on the exam is the number of bits of the hash of your answer that agree with the corresponding bits of the hash of the correct answer.
(a) (7 points) If someone gets 100% on the exam, why is the professor confident that the student's answer is correct?
(b) (3 points) Suppose each student gets every digit of π wrong (a very unlikely occurrence!), and they all have different answers. Approximately what should the average on the exam be?

14. (5 points) The following was encrypted by a shift cipher with shift of -1. Find the plaintext:
GZUDZFNNCRTLLDQ