MATH/CMSC 456 (Washington) Final Exam May 17, 2011

Do each problem on a separate sheet of paper (so you need 7 sheets). Do Problem 1 on page 1, Problem 2 on page 2, etc. Do not staple. Put your name on each sheet. The exam is worth 140 points.

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. (20 points = 10+10) **(a)** Consider an affine cipher mod 26. You do a chosen plaintext attack using *haha*. The ciphertext is *NONO*. Determine the encryption function.

(b) Suppose there is a language that has only the letters a and b. The frequency of the letter a is 0.1 and the frequency of b is 0.9. A message is encrypted using a Vigenère cipher (working mod 2 instead of mod 26). The ciphertext is $BABABAAABA$. The key length is 1, 2, or 3. Determine the key length and decrypt the message.

2. (30 points = 10+10+10) **(a)** Alice and Bob are trying to use RSA, but Bob knows only one large prime, namely $p = 1093$. He sends $n = p = 1093$ and $e = 361$ to Alice. She encrypts her message m as $c \equiv m^e \pmod{n}$. Eve intercepts c and decrypts using the congruence $m \equiv c^d \pmod{n}$. What value of d should Eve use? Your answer should be an actual number. You may assume that Eve knows n and e, and she knows that n is prime.

(b) Suppose that you have two distinct large primes p and q. Explain how to find an integer x such that

$$x^2 \equiv 49 \pmod{pq}, \qquad x \not\equiv \pm 7 \pmod{pq}.$$

(c) Suppose that you have a large number n that is a product of two distinct primes: $n = pq$. Suppose also that you have a number x such that

$$x^2 \equiv 49 \pmod{n}, \qquad x \not\equiv \pm 7 \pmod{n}.$$

Explain how to factor n.

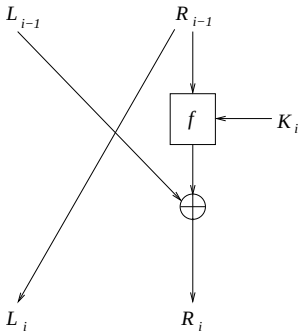
3. (25 points = 9+8+8) Suppose Alice signs a document m by signing its hash $H(m)$ using the RSA signature scheme. That is, let n, e be Alice's RSA public key and let d be her private key. The signed document is (m, s), where $s \equiv H(m)^d \pmod{n}$. Bob verifies the signature by checking that $s^e \equiv H(m) \pmod{n}$.

(a) If (m, s) is a correctly signed document, show that the verifcation congruence is satisfied.

(b) Eve has a document m and wants to find Alice's signature s for m. Why is this difficult? (do not say that it's because Eve doesn't know d. Instead, relate it to the difficulty of some problem).

(c) Eve gives up trying to sign her document. Instead, she starts with s and tries to find a message m for which s is the signature. Why is this difficult? (again, relate it to the difficulty of some problem).

4. (15 points = 5+10) **(a)** Alice constructs a 16-round Feistel system with the same key at each round (that is, $K_1 = K_2 = \cdots = K_{16}$). It starts with the plaintext L_0R_0,



and it uses some function $f(R, K)$. Eve does not know Alice's key but she obtains the ciphertext $L_{16}R_{16}$ from Alice's encryption. If Eve obtains a copy of Alice's machine, how can she recover the plaintext L_0R_0?

(b) Alice and Bob are arguing about which method of multiple DES encryption they should use. Alice wants to choose keys K_1 and K_2 and triple encrypt a message m as $c = E_{K_1}(E_{K_2}(E_{K_1}(m)))$. Bob wants to quadruple encrypt a message m as $c = E_{K_1}(E_{K_1}(E_{K_2}(E_{K_2}(m))))$. Which method is usually more secure? Describe in detail an attack on the weaker encryption method.

5. (10 points) Let P and Q be points on an elliptic curve E. Peggy claims that she knows an integer k such that $kP = Q$ and she wants to convince Victor that she knows k without giving Victor any information about k. They perform a zero-knowledge protocol. The first step is the following:

1. Peggy chooses a random integer r_1 and lets $r_2 = k - r_1$. She computes $X_1 = r_1P$ and $X_2 = r_2P$ and sends them to Victor.

Give the remaining steps. Victor wants to be at least 99% sure that Peggy knows k. (*Technical note:* You may regard r_1 and r_2 as numbers mod n, where $nP = \infty$. Without congruences, Victor obtains some information about the size of k.

Non-technical note: The "Technical note" may be ignored when solving the problem.)

6. (20 points = 10+10) **(a)** Bob signs contracts by signing the hash values of the contracts. He is using a hash function H with a 70-bit output. Eve has a document M that Bob is willing to sign and another document N that states that Bob will pay her a lot of money. Explain how Eve can trick Bob into signing a document (closely related to N) that states that Bob will pay Eve a lot of money. (*Note:* You may assume that Eve can do up to 2^{50} calculations.)

(b) Let p be a large prime and let α be a primitive root mod p. Suppose that $H(x) = \alpha^x \pmod p$. Then H is not quite fast enough to be a hash function. Which of the other two properties for a hash function does H satisfy? Explain your answers.

7. (20 points = 6+6+8) Let E be the elliptic curve $y^2 \equiv x^3 - x + 4 \pmod 5$.

(a) List the points on E (don't forget ∞).

(b) Evaluate the elliptic curve addition $(2, 0) + (4, 3)$.

(c) A bank in Alice Springs (Australia), also known as Alice, wants to send a lot of financial data to the Bank of Baltimore, also known as Bob. All of their communications will be on public airwaves. Describe how Alice and Bob can accomplish this. In particular, state two cryptosystems they should use and how these cryptosystems are used.