MATH/CMSC 456, Jeffrey Adams FINAL May 18, 2005
Put your name on each page, and do one problem per page
For full credit you must show your work.

1. [25 points] Which of the following can be broken quickly (i.e. the key found), in less than ten minutes on a small computer, if a sufficiently long plain text/cipher text pair is known? Simple yes/no answers are sufficient.

   (a) Hill Cipher
   (b) RSA
   (c) Affine Cipher
   (d) DES
   (e) Vigenère

2. [30] I have an alphabet with 50 letters. I try to use an affine cipher, with encryption function $f(x) = 4x + 20 \pmod{50}$.

   (a) [10] What is wrong with this affine cipher? Explain.
   (b) [10] Find the two solutions to $f(x) = 28$.
   (c) [10] How many solutions to $f(x) = 17$ are there?

3. [30] I want to make a cryptosystem like RSA with $n = pqr$ where p, q and r are distinct primes. So the encryption function is $c = m^e \pmod{n}$.

   (a) [15] What should e satisfy? Be explicit.
   (b) [15] The decryption function is $m = c^d \pmod{n}$ for some d. How do I choose d?

4. [30] Let $p = 3221225473$ and $q = 1628161$, and $n = pq = 5244673687345153$. Note that p, q are prime and $p - 1 = 2^{30} \times 3$; also $53 | q - 1$. In both parts (a) and (b) provide an argument, not a calculation.

   (a) [15] Show that $2^{35!} = 1 \pmod{p}$.
   (b) [15] Suppose you didn't know the factorization of n. Show how you could use the fact in (a) to factor n.

5. [30] Recall the ElGamal signature scheme. Alice chooses (p, α, β) with α a primitive root $\pmod{p}$, and $\beta = \alpha^a$ for some a. She publishes (p, α, β) but keeps a secret. To sign a message m she chooses a random integer k satisfying $(k, p-1) = 1$. The signed message is then (m, r, s) with $r = \alpha^k \pmod{p}$ and $s = k^{-1}(m - ar) \pmod{p-1}$. A message (m, r, s) is valid if $\alpha^m = \beta^r r^s \pmod{p}$.

Eve tries to forge a message. She chooses u, v with $(u, p-1) = 1$. She then takes $r = \beta^v \alpha^u \pmod{p}$, $s = -rv^{-1} \pmod{p-1}$, and $m = su \pmod{p-1}$.

(a) [10] Show that (m, r, s) is a valid signature.

(b) [10] Is it likely that she can make m a meaningful message? Why or why not?

(c) [10] Suppose instead there is a hash function h and the signature is supposed to be $(h(m), r, s)$. Explain why it is hard for Eve to find a valid signature.

6. [15] Alice and Bob exchange a key using Diffie Hellman key exchange. They take $p = 29$ and $\alpha = 2$. Alice takes $x = 3$ and Bob takes $y = 7$. Compute the key.

7. [40] Consider the elliptic curve E: $y^2 = x^3 + 2x + 4 \pmod{31}$.

(a) [8] Compute $(9, 10) + (9, -10)$ on E.

(b) [8] Compute $\infty + (9, 10)$ on E.

(c) [8] Compute $(2, 4) + (7, 12)$ on E.

(d) [8] Find all points of the form $(8, y)$ on E.

(e) [8] Find b so that there is a point of the form $(5, y)$ on the elliptic curve $y^2 = x^3 + 2x + b \pmod{223676221}$. What is y?

You may use the addition formulas on the curve $y^2 = x^3 + ax + b$: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

where

$$m = \begin{cases} (3x_1^2 + a)/(2y_1) & x_1 = x_2, y_1 = y_2 \\ (y_2 - y_1)/(x_2 - x_1) & else \end{cases}$$

There are additional special cases when P and/or $Q = \infty$, and when $m = \infty$.