MATH/CMSC 456 (Washington) Final Exam Answers May 17, 2006

1. (1) Vigenère: let the plaintext be *aaaaaaaaaaa*.... The ciphertext will be the key repeated several times.
(2) Affine: let the ciphertext be *ab*. If the affine function is $\alpha x + \beta$, the first letter of the ciphertext yields β and the second yields $\alpha + \beta$. Subtracting yields α.
(3) Hill: let the ciphertext be *baab* (Bob's favorite message, of course). The first two letters of the ciphertext are the first row of the matrix and the last two letters give the second row.

2. (a) Choose a random slope, say 5. The polynomial is $f(x) = 12 + 5x \pmod{17}$. The points are $A : (1, 0)$, $B : (2, 5)$, $C : (3, 10)$. (There are many possible correct answers for this question.)
(b) Satisfies: fast. Doesn't satisfy: preimage resistant (given y, we want x with $H(x) = y$. let $x = y$. Also: not strongly collision free: $H(x) = H(x \| 111 \cdots 111)$, where 400 1's are appended to x.
3. (a) Compute $\gcd(670705093 - 33335, 670726081)$. This gives a nontrivial factor.
(b) $1 \not\equiv k^2 \equiv 2^{n-1} \pmod{n}$. If n is prime, Fermat's theorem implies that $2^{n-1} \equiv 1 \pmod{n}$, so n cannot be prime.
4. (a) Write $a_1 a = 1 + (p-1)k$. Then Fermat implies that $x^{p-1} \equiv 1 \pmod{p}$, so $y^{a_1} \equiv x^{a_1 a} = x \cdot (x^{p-1})^k \equiv a \cdot 1^k \equiv x \pmod{p}$.
(b) Alice chooses a secret a and computes a_1 as in (a). Bob chooses b and b_1 with $b_1 b \equiv 1 \pmod{p-1}$. Let the message be x. Alice sends $x^a \pmod{p}$ to Bob. Bob sends $(x^a)^b$ back to Alice. Alice raises this to the a_1th power and sends to Bob. Bob raises to the b_1 power and gets x. Justification is as in (a).
5. (a) Eve knows kQ and needs k. Finding elliptic discrete logarithms is hard.
(b) $k\infty = \infty$ for all k, so all the entries in the file are ∞. Any password k that Eve uses will yield $kQ = \infty$, and therefore it will match what is in the file.
(c) Choose a large prime p and a primitive root α. Store a password k as $\alpha^k \pmod{p}$.
6. (a) Victor randomly chooses $i = 1$ or $i = 2$ and asks Peggy for r_i. Peggy sends r_i. Victor checks that $r_i^2 \equiv x_i \pmod{n}$. They repeat the whole procedure several times.
7. Eve chooses a plaintext-ciphertext pair (m, c). She makes two lists: The first is $E_K(m)$ for all K and the second is $D_L(c)$ for all keys L. She lists all matches. These correspond to possible pairs (K_1, K_2). She then tries encrypting some more plaintexts using each of the possibilities for (K_1, K_2). This should eliminate all of the incorrect pairs, leaving only valid pairs (more than one pair might give the correct encryption function).
8. (a) $s^e \equiv H(m)^{ed} \equiv H(m)$, since this is just an RSA encryption/decryption.
(b) Eve needs to find m_1 with $H(m_1) = s_1^e \pmod{n}$. This is hard because the hash function is preimage resistant.
(c) Eve knows $H(m)$ and needs to find s with $s^e \equiv H(m)$. Finding s is the same as decrypting the RSA "ciphertext" $H(m)$.