MATH/CMSC 456 (Washington) Final Exam Solutions May 14, 2007

1. (14 points = 7+7) (a) Solve $y \equiv 9x + 1 \pmod{26}$ for x to get $x \equiv 3(y-1)$ (mod 26). The ciphertext $19, 1, 16$ becomes $2, 0, 19$, which is *cat*.
(b) Use $n = 1, 2, 3$ to get the equations

$$1 \equiv 0 + 0 + c_2, \quad 1 \equiv 0 + c_1 + c_2, \quad 0 \equiv c_0 + c_1 + c_2.$$

These yield $c_2 \equiv 1,\ c_1 \equiv 0,\ c_0 \equiv 1$. The recurrence is $x_{n+3} \equiv x_n + x_{n+2}$. The next four elements of the sequence are 1, 0, 0. 1.

2. (11 points = 7+4) (a) Take any random number, for example 3, for the slope. Use the line $y \equiv 5 + 3x \pmod 7$. Give A the point $(1, 1)$, give B the point $(2, 4)$, give C the point $(3, 0)$, and give D the point $(4, 3)$.
(b) With only one share, all 7 secrets are still possible.

3. (20 points = 12+8) (a) (1) Vigenère: yes; (2) Hill cipher: yes; (3) RSA (with a 300-digit n): no; (4) DES: no
(b) $23154^2 \equiv 1234^4 \equiv 1 \pmod n$ but $23154 \not\equiv \pm 1 \pmod n$. Therefore, $\gcd(23154-1, n)$ gives a factor of n. (If you're wondering, or if you're not, $n = 137 \cdot 421$.)

4. (14 points: 7+7) (a)$x \equiv y \pmod{p-1}$ means $x = y + (p-1)k$ for some k. Therefore, $m^x = m^y (m^{p-1})^k \equiv m^y (1)^k \equiv m^y \pmod p$, by Fermat's theorem.
(b) Eve knows e and p, so she finds d with $de \equiv 1 \pmod{p-1}$. Then $c^d \equiv m^{ed} \equiv m$ (mod p), so Eve obtains p.

5. (10 points: 7+3) $v_1 \equiv \beta^{f(r)} r^s \equiv \alpha^{af(r)} \alpha^{ks} \equiv \alpha^{af(r)+m-af(r)} \equiv \alpha^m \equiv v_2$ (mod p).
(b) Eve takes $k = 1$, $r = \alpha$, $s = m_1$.

6. (11 points = 7+4) (a) $s^e \equiv k^{-e} s_1^e \equiv k^{-e} m_1^{ed} \equiv k^{-e} m_1 \equiv m \pmod n$.
(b) $\gcd(k, n) = 1$ is used because we compute $k^{-1} \pmod n$.

7. (10 points) The remaining steps are

(3) Peggy sends R_1 and R_2 to Victor.
(4) Victor checks that $R_1 + R_2 = B$.
(5) Victor asks for r_1 or r_2. Call it r_i.
(6) Peggy sends r_i to Victor.
(7) Victor checks that $r_i A = R_i$ for that i.
(8) They repeat all the above steps at least 9 more times (for a total of at least 10).

8. (10 points) Eve makes a list of the hash values of each of the 2^{20} good contracts and another list of the hash values of the 2^{20} bad contracts. Since there are 2^{30} possible hash values, 2^{20} is much larger than $\sqrt{2^{30}} = 2^{15}$, there should be a match. This means that Alice's signature on a good contract is also valid as a signature of some bad document.