MATH/CMSC 456 (Washington) Final Exam Solutions May 14, 2009

1. (16 points = 8+8) (a) First encrypt $(x, y) = (0, 0)$. This yields (e, f). Then encrypt $(1, 0)$ and subtract (e, f) from the result. This yields (a, b). Finally, encrypt $(0, 1)$ and subtract (e, f) from the result to get (c, d).
(b) Take the product to get $(729 \cdot 42912)^2 \equiv 2 \cdot 18 \equiv 6^2$. Then compute $\gcd(729 \cdot 42912 - 6, n)$ to get a nontrivial factor of n.

2. (12 points = 6+6) (a) $m \equiv c^d$, so $m^{14} \equiv (c^{14})^d \equiv 1^d \equiv 1$.
(b) Multiply (a) by m to get $m^{15} \equiv m$. This means that $c^5 \equiv (m^3)^5 \equiv m$. So $f = 5$ works.

3. (12 points = 6+6) (a) If n is prime then $k^2 \equiv 2^{n-1} \equiv 1$ by Fermat. Therefore, if $k^2 \not\equiv 1$ then n is not prime.
(b) We have $k^2 \equiv 1^2$ but $k \not\equiv \pm 1$. Therefore, $\gcd(k - 1, n)$ is a nontrivial factor of n.

4. (8 points) First, use RSA (or some public key method) to send a key. Or use Diffie-Hellman to establish a key. Then use DES or AES with this key to transmit the gigabytes of data. Alternatively, tell them to use a shift cipher. Then break the system, steal the data and the money, and move to Tahiti.

5. (18 points = 6+6+6) (a) $u_2 \equiv (\alpha^a)^s(\alpha^k)^r \equiv \alpha^{as+kr} \equiv \alpha^{h(m)} \equiv u_1$.
(b) If $k = a$ then $r = \beta$, so Eve can notice this. From equation (3), $s \equiv a^{-1}h(m) - r$ when $k = a$, so $a^{-1}h(m) \equiv s + r \pmod{p-1}$. There are $d = \gcd(h(m), p - 1)$ solutions a^{-1} to this congruence. Test each potential value of a in the congruence $\beta \equiv \alpha^a \pmod{p}$. This yields the correct value of a.
(c) Since $h(m_0 + 100) \equiv 2^{m_0}2^{100} \equiv 2^{m_0} \equiv h(m_0) \pmod{101}$, we find that $(m_0 + 100, r_0, s_0)$ is a valid signed message.

6. (14 points = 8+6) (a) For example, let the polynomial be $f(x) = 5 + 3x + x^2 \pmod{11}$. Since $f(1) = 9$, give $(1, 9)$ to A. Give $(2, 4)$ to B. Give $(3, 1)$ to C. Give $(4, 0)$ to D.
(b) There are 11 choices for the secret.

7. (8 points) There are 2^{30} "birthdays." Eve hashes each of the 2^{20} fraudulent contracts. Eve now has two lists of hash values, each list of length much longer than $\sqrt{2^{30}}$. So there should be a match between the two lists. This means that there is a hash of a legitimate contract that matches the hash of a fraudulent contract. Alice's signature on the legitimate contract is therefore also a signature for this fraudulent contract.

8. (12 points: 6+6) (a) There are 10^{20} "birthdays," so N should be around $\sqrt{10^{20}} = 10^{10}$.
(b) p is a prime around 10^{20}. There are numbers α and β such that $\beta \equiv \alpha^k \pmod{p}$ for some k. Eve makes two lists: The first is α^j for $\sqrt{p}$ random j. The second is $\beta\alpha^{-\ell}$ for $\sqrt{p}$ random ℓ. She looks for a match.