MATH/CMSC 456 (Washington) Final Exam Answers May 16, 2002

1. (a) Use the Extended Euclidean algorithm: $100 = 14*7+2$, $7 = 3*2+1$, so 1 is the gcd. Working backwards yields $1 = 7-3*2 = 7-3*(100-14*7) = 43*7-3*100$. This means that $43 * 7 \equiv 1 \pmod{100}$, so $d = 43$.
(b) Decrypt: $m \equiv c^{43} \pmod{101}$. (This works because of part (a) and because we work mod $p-1$ in the exponent.)
(c) Break m into blocks, each less than 101, and encrypt each block separately.

2. (31 points=9+9+4+9) (a) Displace by 2. There is one match. Displace by 3. There are five matches. Therefore key length 3 is more likely.
(b) The affine encryption function is $y \equiv mx+n \pmod{26}$. Use the plaintext $ab = 0, 1$. The ciphertext will be U, V for some numbers U, V. Since $U = m0 + n = n$, we know m. Since $V \equiv m*1+n$, we have $m \equiv V - n \equiv V - U$. Therefore we have found the encryption function.
(c) DES uses too small a key and can be broken by brute force.
(d) Slope $= (4-2)/(1-0) = 2$. Line: $y = 2x+2$. Intersect with E: $(2x+2)^2 = x^3+4x+4$, so $x^3 - 4x^2 - 4x = 0$. The sum of the roots is minus the coefficient of x^2, so $4 = 0+1+x$. This means $x = 3$. Therefore $y = 2x+2 = 8 \equiv 1 \pmod{7}$. Reflect across x-axis: $(3,-1) \equiv (3,6)$. This is $P+Q$.

3. (a) Euclidean algorithm.
(b) Alice computes a square root of y mod p and a square root of y mod q, then combines them (Chinese Remainder Theorem) to get s. She computes the square root of y mod p as $y^{(p+1)/4} \pmod{p}$, and similarly mod q.
(c) There are four square roots of y mod n, namely, $\pm x$ and $\pm$something else. Therefore the probability is 1/2 that $s \equiv \pm x \pmod{n}$.
(d) If Bob wins, then $s^2 \equiv x^2 \pmod{n}$, but $s \not\equiv \pm x \pmod{n}$. Therefore, $\gcd(x-s, n)$ is a nontrivial factor of n.

4. (a) Eve knows P_1 and $P_2 = bP_1$. Eve solves a discrete log to find b. Similarly, Eve knows P_2 and $P_3 = a_1P_2$. Eve solves a discrete log to find a_1. She then calculates $a \equiv a_1^{-1} \pmod{n}$ to get a.
(b) Alice and Bob publicly agree on a large prime p. Alice chooses a secret integer a with $\gcd(a, p-1) = 1$ and Bob chooses a secret integer b with $\gcd(b, p-1) = 1$. Alice sends $m_1 \equiv m^a \pmod{p}$ to Bob. Bob sends $m_2 \equiv m_1^b$ to Alice. Alice computes $a_1 \equiv a^{-1} \pmod{p-1}$ and sends $m_3 \equiv m_2^{a_1} \pmod{p}$ to Bob. Bob computes $b_1 \equiv b^{-1} \pmod{p-1}$ and computes $m_4 \equiv m_3^{b_1} \pmod{p}$. It can be shown that $m_4 \equiv m \mod p$.

5. Solve $d'e \equiv 1 \pmod{12345}$. Then $d'e = 1 + 12345k$ for some k. Therefore $c^{d'} \equiv m^{d'e} \equiv m(m^{12345})^k \equiv m(1)^k \equiv m \pmod{n}$. The next to last congruence used the spy's information. This shows that d' works as a decryption exponent for this ciphertext.

6. (a) We have $\beta^{r_1} r_1^{s_1} \equiv \alpha^{ar_1}\alpha^u\beta^v)^{s_1} \equiv \alpha^{ar_1+us_1+avs_1}$. But the exponent is $ar_1 + us_1 + avs_1 \equiv ar_1 + (u+av)(-r_1v^{-1}) = -ur_1v^{-1} = s_1u = m$, so we have α^m.
(b) Eve will have a value of h_0 for which the signature is valid, and will need to find a message m with $h(m) = h_0$. This is hard to do if h is a good hash function.

7. Make a list of $E_K(m_1)$ for all keys K and a list of $D_L(c_1)$ for all keys L. Record all pairs (K, L) for which there is a match. Now check which of these pairs satisfy $E_L(E_K(m_2)) = c_2$. This should eliminate most of the pairs (K, L). Try the remaining ones on (m_3, c_3), and continue in this way until only one pair (K, L) remains. This will be (K_1, K_2).

8. (a) If Peggy uses the same r_1 and r_2 a second time, Victor will receive the same x_1 and x_2. He therefore asks for the r_i that was not asked for the first time. he then has r_1 and r_2. He thus obtains $s \equiv r_1r_2$.
(b) Peggy chooses a random r_2, computes $x_2 \equiv r_2^2 \pmod n$, and computes $x_1 \equiv yx_2^{-1} \pmod n$. She sends x_1, x_2 to Victor. When Victor asks for a square root of x_2, Peggy can provide r_2.
(c) There is $1/2$ probability in each round, so $(1/2)^{10} = 1/1024$ probability that Peggy successfully completes 10 rounds.