MATH/CMSC 456 (Washington) Final Exam Solutions May 14, 2015
The exam is worth 140 points.

1. (15 points = 5+10) **(a)** $\gcd(b, 26) = 1$
(b) $aaaaa = 00000$ yields the shifts $a_1, \ldots, a_5$. Then $baaaa = 10000$ yields $b + a_1, \ldots$. Subtract a_1 to get b.
2. (20 points = 5+5+5+5) **(a)** The shift can be determined from the first ciphertext letter minus Y. Then check whether this shift applied to P or F yields the fourth letter of the ciphertext.
(b) Same solution as for the shift cipher.
(c) Encrypt the two messages and see which one yields the ciphertext.
(d) With a one-time pad, the ciphertext could come from either message, so there is no way to tell which one it is.
3. (25 points = 5+5+5+10) **(a)** $\gcd(k, p-1) = 1$ because we need $k^{-1} \pmod{p-1}$.
(b) If $k_1 = k_2$ then the values of r will be the same.
(c) We have $ks_1 + ar \equiv m_1$ and $ks_2 + ar \equiv m_2 \pmod{p-1}$. Subtract to get $k(s_1 - s_2) \equiv m_1 - m_2$. Divide by $s_1 - s_2$ to get k. Then $ar \equiv m_1 - ks_1$. Divide by r to get a.
(d) By the Birthday Paradox, since $10^7 > \sqrt{10^{12}}$, we expect two values of k to be equal. Eve sees this, as in part (b), and finds a by the method of part (c).
4. (20 points = 5+5+10) **(a)** Use $n = \cdots$; PowerMod$(2, n-1, n)$. If this yields 1, then n is probably prime. If this is not 1 then n must be composite by the Fermat test.
(b) There are more than 10^{97} primes of 100 digits. There is not enough time (and not enough electrons in the universe) to do this calculation.
(c) Compute $\gcd(7961-7, 8051) = 97$ (Basic Factorization Principle), and $8051/97 = 83$.
5. (10 points) 1. Peggy chooses random integers r_1 and r_2 and lets $r_3 = k - r_1 - r_2$. She computes

$$X_1 = r_1 P, \quad X_2 = r_2 P, \quad X_3 = r_3 P$$

and sends them to Victor.
2. Victor checks that $X_1 + X_2 + X_3 = Q$.
3. Victor chooses two indices i, j (among $1, 2, 3$).
4. Peggy sends r_i and r_j.
5. Victor checks that $X_i = r_i P$ and $X_j = r_j P$.
6. They repeat 4 more times.
In this version, if Peggy doesn't know k then she has only 1/3 probability of succeeding in a round. For another version, Victor asks for only one index i in Step 3. Then Peggy has probability 2/3. This means that 12 iterations are needed.
6. (20 points = 10+10) **(a)** The method $c = E_{K_1}(E_{K_1}(E_{K_2}(m)))$ is weaker since the Meet-in-the-Middle attack can be used: Choose a pair (m, c). Make two lists:
I. $D_K(D_K(c))$ for all keys K, **II.** $E_L(m)$ for all keys L.
For each match between the lists, test the pair (K, L) on another pair (m, c). If more than one pair survives the second round, use a third pair (m, c), and so on.
(b) Collisions are easy to find: $H(x + p - 1) = 2^{x+p-1} \equiv 2^x = H(x)$ by Fermat.

Preimage resistant: given y, solving $2^x \equiv y \pmod p$ is a discrete log problem, which is probably hard.

7. (20 points = 10+5+5) **(a)** Write $ed = 1 + k(p-1)(q-1)/2$. Then

$$s^e \equiv m^{ed} \equiv m^1 (m^{(p-1)(q-1)/2})^k \equiv m^1 1^k \equiv m \pmod n.$$

(b) We have $s_1 \equiv m_1^d \equiv k^{ed} m^d$. But $k^{ed} \equiv k \pmod n$ since this is just RSA encryption and decryption of k. Therefore, $s_1 \equiv km^d$. Bob divides by k to get $s \equiv k^{-1} s_1 \equiv m^d$, which is a valid signature for m.

(c) Signing: $s \equiv H(m)^d \pmod n$. Verifying: $H(m) \equiv s^e \pmod n$.

8. (10 points = 5+5) **(a)** Use RSA, or ElGamal, or Diffie-Hellman to establish a key. Then use 3-DES or AES to send the data.

(b) If the hash of a corrupted message equals the hash of the correct message, there is a collision. If the hash function is collision free, this shouldn't happen.