MATH/CMSC 456 (Washington) Final Exam Solutions May 15, 2014

1. (15 points = 6+3+6) **(a)** The inverse of 21 mod 26 is 5. Multiply by 5 to get $5y \equiv 105x + 10 \equiv x + 10 \pmod{26}$. This yields $x \equiv 5y - 10$. The decryption of $W = 22$ is $5 \times 22 - 10 = 100 \equiv 22$, which is X. The decryption of $A = 0$ is $-10 \equiv 16$, which is Q. So my plaintext is XQ.
(b) The determinant of the matrix is -2 and $gcd(-2, 26) \neq 1$, so the matrix is not invertible.
(c) Since $2554^2 \equiv 3^{2700} \equiv 1 \pmod{2701}$ and $2554 \not\equiv \pm 1 \pmod{2701}$, we compute $\gcd(2554 - 1, 2701) = 37$, so $2701 = 37 \times 73$.
2. (15 points) Let P be the one-time pad. Double encrypting m yields $m \oplus P \oplus P = m$ since $p \oplus P = 000\ldots 0$. The key $NANANA$ alternates shifts of 13 and 0. Doing this twice yields shifts of 26 and 0. Since we are working mod 26, the plaintext does not get encrypted. Finally, since $e^2 \equiv 1 \pmod{(p-1)(q-1)}$, we must have $d = e$. Therefore, double encryption is the same as encrypting and then decrypting. The final result is therefore the unencrypted plaintext.
3. (15 points = 10+5) **(a)** We have $c_4 \equiv m^{e_A d_A e_B d_B} \equiv (m^{e_A d_A})^{e_B d_B} \equiv m^{e_A d_A} \pmod{n}$, since raising to the exponent $e_B d_B$ is RSA encryption and decryption for Bob. But $m^{e_A d_A} \equiv m \pmod{n}$ since this is RSA encryption and decryption for Alice. Therefore, $c_4 \equiv m \pmod{n}$.
(b) Knowing e_A and d_A allows Eve to factor n, so then Eve solves $d_B e_B \equiv \pmod{(p-1)(q-1)}$ for d_A for get d_A.
4. (10 points = 5+5) **(a)** To find y, Nelson will need to find square roots mod n. This is equivalent to being able to factoring n.
(b) First choose the point $P = (x, y)$ and the coefficient A. Then let $B = y^2 - x^3 - Ax$.
5. (15 points = 5=5+5) **(a)** Eve needs to solve $s^e \equiv 123456789 \pmod{n}$, which is the same as decrypting the RSA "ciphertext" 123456789 to get the "plaintext" s. This is (probably) hard to do.
(b) Eve computes $m \equiv 112090305^e \pmod{n}$. Then (m, s) satisfies the verification congruence.
(c) Eve needs to solve $g^m \equiv r^s h^r \pmod{p}$ for m. Since g is a primitive root, this always has a solution. It is a discrete log problem, so it is (probably) hard.
6. (15 points = 5+5+5) **(a)** Victor checks that $Y_1 + Y_2 = Q$.
(b) Victor checks that $r_i P = Y_i$.
(c) They repeat (1) through (6) ten times.
7. (15 points = 5+5+5) **(a)** There are $N = 3 \times 10^{147}$ "birthdays" and $r = 10^{85}$ "people." Since r is much larger than $\sqrt{N}$, it is very likely that there is a match; that is, two particles should choose the same prime.
(b) h is fast. But $h(m) = m$, so it is not preimage resistant, and $h(m \oplus m \oplus m) = h(m)$, so it is not collision resistant.
(c) Eve makes 2^{30} versions of the petition and computes their hashes. She makes 2^{30} versions of the statement and computes their hashes. Since h has at most 2^{60} outputs and $2^{30} = \sqrt{2^{60}}$, we expect a match between the two lists of hashes: $H(m_1) = H(m_2)$, where m_1 is a version of the petition and m_2 is a version of the statement. Eve has Alice sign m_1 by signing $H(m_1)$. This is also a signature for m_2.