ECE: Advanced Information and Network Security
Homework 2
Fall 2012

1. The ciphertext 75 was obtained using RSA with n = 437 and e = 3. You know that the plaintext is either 8 or 9. Determine which it is without factoring n.

Solution: The two possible plaintexts are 8 and 9. Encrypt each to get $8^3 (mod 437) = 75$ and $9^3 (mod 437) = 292$. Hence, the correct plaintext is 8.

2. Naive Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve sends him the ciphertext $2^e c \pmod n$. Show how this allows Eve to find m.

Solution: Nelson decrypts $2^e c$ to get $2^{ed} c^d = 2c^d = 2m (mod n)$, and therefore sends 2m to Eve. Eve divides by 2 mod n to obtain m.

3. Suppose that there are two users on a network. Let their RSA moduli be n_1 and n_2, with n_1 not equal to n_2. If you are told that n_1 and n_2 are not relatively prime, how would you break their systems?

Solution: Take the gcd and you get a factor.

4. Suppose two users Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e_A and e_B are relatively prime. Charles wants to send the message m to Alice and Bob, so he encrypts to get $c_A = m^{e_A}$ and $c_B = m^{e_B} \pmod n$. Show how Eve can find m if she intercepts c_A and c_B.

Solution: Since $\gcd(e_A, e_B) = 1$, there are integers x and y with $e_A x + e_B y = 1$. Therefore, $m = m^1 = (m^{e_A})^x (m^{e_B})^y = c_A^x c_B^y (mod n)$. Since Eve can calculate this last quantity, she can calculate m.