ECE 332:491/602 Information and Network Security Exam Solutions

Spring 2008

1 Short Answer

1. **(5 pts)** Draw a diagram depicting two consecutive Feistel Rounds (you may consider the subkeys to be K_1 and K_2).
2. **(5 pts)** Explain the mathematical meaning of the Euler Phi function $\phi(n)$.
3. **(5 pts)** Describe how you would apply Fermat's Little Theorem to test whether a number n is prime.
4. **(5 pts)** Explain why using two prime numbers p and q that are close to each other in value is a bad idea for RSA.

Answers: (1) See book and concatenate two rounds together.

(2) The Euler $\phi(n)$ function counts the amount of numbers relatively prime to n in the range 1 to n.

(3) Choose a random a such that $gcd(a, n) = 1$ (if you find one that is not, then you have factored n). Calculate $y = a^{n-1} \pmod{n}$ and check to see whether $y = 1$. If not then n is definitely not prime. If so, then n might be prime. Repeat the test multiple times.

(4) Choosing two primes that are close to each other is bad for RSA because it facilitates factoring. If p and q are close to each other, then the factors lie close to $\sqrt{n}$. Fermat's factorization can easily find one of the factors.

2 Calculations

1. **(5 pts)** Calculate $7^{-1} \pmod{17}$.
2. **(5 pts)** Suppose Alice chooses $n = 35$ as her RSA modulus, and chooses $e_A = 7$ as her public exponent. Hence her public key is (n, e_A). Calculate her private decryption exponent d_A.
3. **(10 pts)** Let p be a prime and n be any integer greater than p. Show that for any a and b from $\{0, 1, \cdots, p-1\}$, that $(a + b)^n = a^n + b^n \pmod{n}$. What can you say about $(a + b)^p \pmod{p}$?
4. **(10 pts)** Is $5^{57} + 1$ prime? If so, explain how you know this, if not, provide a factorization.

Answers:

(1) Observe that $7 \cdot 5 = 35$, and $35 = 1 \pmod{11}$. Hence $7^{-1} \pmod{11} = 5$.

(2) Observe that $n = 5 \cdot 7$, and hence $\phi(n) = (5 - 1)(7 - 1) = 24$. The private decryption exponent d_A satisfies

$$e_A d_A = 1 \pmod{24}$$

and hence $d_A = 7$. (So, encryption and decryption would be the same for this example!)

(3) Observe that the binomial expansion for $(a + b)^n$ has terms of the form $\binom{n}{j} a^j b^{n-j}$. All terms but a^n and b^n have a factor of n, and hence become 0 modulo n. Thus all that remains is $a^n + b^n$. By Fermat's Little Theorem $(a + b)^{p-1} = 1 \pmod{p}$ so $(a + b)^p = a + b$.

(4) Observe that $57 = 3 \cdot 19$, and that $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$. Let $x = 5^19$ and $y = 1$. Then $(5^{19})^3 + 1^3 = (x + y)(x^2 - xy + y^2)$. Thus, it is not prime and we have provided a factorization.

3 Advanced Understanding

1. **(10 pts)** Suppose $E_K(M)$ is the DES encryption of a message M using the key K. We showed in the homework that DES has the complementation property, namely that if $y = E_K(M)$ then $\overline{y} = E_{\overline{K}}(\overline{M})$, where $\overline{M}$ is the bit complement of M. That is, the bitwise complement of the key and the plaintext result in the bitwise complement of the DES ciphertext. Explain how an adversary can use this property in a brute force, chosen plaintext attack to reduce the expected number of keys that would be tried from 2^{55} to 2^{54}. (Hint: Consider a chosen plaintext set of (M_1, C_1) and $(\overline{M_1}, C_2)$). (Second Hint: This is a tough problem.)

2. **(10 pts)** The cipher block chaining (CBC) mode has the property that it recovers from errors in ciphertext blocks. Show that if an error occurs in the transmission of a block C_j, but all the other blocks are transmitted correctly, then this affects only two blocks for decryption. Which two blocks?

3. We now look at a $3-person$ group encryption scheme based on the same principle as RSA. Suppose that some trusted entity generates two primes p and q and forms $n = pq$. Now, instead of choosing e_A and d_A (as in RSA), the trusted entity chooses k_1, k_2, and k_3 such that $gcd(k_j, n) = 1$ and
$$k_1k_2k_3 = 1 \pmod{\phi(n)}.$$
The three users A, B, and C are given the following keys
$$\begin{aligned} A &: (k_1, k_2, n) \\ B &: (k_2, k_3, n) \\ C &: (k_1, k_3, n). \end{aligned}$$
   (a) **(5 pts)** Suppose user A generates a message m such that $gcd(m, n) = 1$. A wants to encrypt m so that *both* B and C can decrypt the ciphertext. To accomplish this, A forms the ciphertext
$$y = m^{k_1k_2} \pmod{n}.$$
   Explain how B would decrypt y, and explain how C would decrypt y.

   (b) **(10 pts)** Suppose A and B have been collaborating on some class project and have produced the message m (with $gcd(m, n) = 1$). They would like to create a ciphertext that they can send C so that only C can decrypt it, and such that once encrypted neither A nor B can decrypt the ciphertext to recover m. Explain how this can be accomplished.

4. **(15 pts)** Eve has captured an encryption device that she knows is an affine cipher (mod 26). She conducts a chosen plaintext attack and feeds in the letters A and B into the cipher to get the ciphertexts H and O. What was the key (α, β) for the underlying affine cipher?

Answers:

(1) This is a tricky little problem with a deceptively simple looking answer.

Let K be the key we wish to find. Use the hint. Then $C_1 = E_K(M_1)$ and $C_2 = E_K(\overline{M_1})$. Now, suppose we start a brute force attack by encrypting M_1 with different keys. If, when we use K_j we get $E_{K_j}(M_1) = C_1$ then we are done and the key we desire is $K = K_j$. However, when we use K_j we can eliminate another key. Here is how. If $E_{K_j}(M_1) = \overline{C_2}$ then we know (by complementation property) that $E_{\overline{K_j}}(\overline{M_1}) = C_2$. Hence, if this happens, we know the key is $\overline{K_j}$ since $\overline{K_j}$ would decrypt C_2 to get $\overline{M_1}$. We are effectively testing two keys for the price of one! Hence, the key space is cut in half and we only have to search an average of 2^{54}.

(2) In CBC, suppose that an error occurs (perhaps during transmission) in block C_j to produce the corrupted $\tilde{C}_j$ and that the subsequent C_{j+1} and C_{j+2} and so on are ok.

Now start decrypting. If we try to decrypt to get P_j we get $\tilde{P}_j = D_K(\tilde{C}_j) \oplus C_{j-1}$, which is corrupted since the decryption of $\tilde{C}_j$ will be corrupted. Next, try to decrypt to get P_{j+1}:

$$P_{j+1} = D_K(C_{j+1}) \oplus \tilde{C}_j$$

which, although $D_K(C_{j+1})$ is correct, when we add $\tilde{C}_j$ we get corrupted output. Now proceed to try to decrypt C_{j+2} to get P_{j+2}:

$$P_{j+2} = D_K(C_{j+2}) \oplus C_{j+1}$$

which is uncorrupted since each of the components are $D_K(C_{j+2})$ and C_{j+1} are uncorrupted.

(3)-a: B would simply do $y^{k_3} \pmod{n} = m^{k_1 k_2 k_3} \pmod{n}$. By Euler's Theorem $m^{k_1 k_2 k_3} = m \pmod{n}$. C would do the same.

(3)-b: Observe that A and B can encrypt their message successively:

$$m^{k_1 k_2} \to \left(m^{k_1 k_2}\right)^{k_2 k_3} = m^{k_2} \pmod{n}.$$

To decrypt, C needs to raise m^{k_2} to the $k_1 k_3$ power:

$$m = \left(m^{k_2}\right)^{k_1 k_3} \pmod{n}.$$

Now, if A or B loses m, then they can't recover m since neither of them, by themselves, knows *both* k_1 and k_3.

(4) Observe that $A = 0$ gets mapped to $H = 7$, so $7 = \beta$. Now, $B = 1$ gets mapped to $O = 14 = \alpha + \beta$, so $\alpha = 7$.