Final Exam

Practice Test with some answers

December 11, 2006

I have left out some answers for the questions that just ask, “what is a QPRNF?” Those can be found in your notes or in the course material.

1. (a) Explain how the RSA algorithm works.

   (b) Show an example of RSA using primes $p = 19, q = 11$. This means

   - Choose an encryption key and the corresponding decryption key.
   - Encrypt the plaintext number $P = 2$.

   The trick here is choosing a nice, small value e so encrypting is easy.

   First, you need e and d with $ed \equiv 1 \pmod{\phi(N)}$, with $\phi(N) = (p-1)(q-1) = 180$. Pick a random e. How about 3? No, because it isn't invertible mod 180. Neither is 2, or 4, or 5, or 6. 7 is the smallest possible exponent.

   So if $e = 7$, What is d? Using the Euclidean algorithm:

$$\begin{array}{rcrcr} \phi & & & = & 180 \\ & & e & = & 7 \\ \phi & - & 25e & = & 5 \\ -\phi & + & 26e & = & 2 \\ 3\phi & - & 77e & = & 1 \end{array}$$

   Always check: $77e = (77)(7) = 539 \equiv 179$ — wait, that's not 1. Of course, the inverse of e is *negative* 77. Careful with those signs. $-77 \equiv 103$, and $(103)(7) = 721 \equiv 1$. So $e = 7, d = 103$.

   To encrypt, compute $c = 2^7 \pmod{N} = 128 \pmod{209} = 128$. We chose e small enough that we didn't even have to mod anything.

2. (a) What is a group?

   (b) Prove: in a group, if $ab = ac$, then $b = c$.

   Proof: a has an inverse a^{-1} due to property 4. So $a^{-1}(ab) = a{-}1(ac)$. Thanks to associativity (property 2), we can rearrange the parentheses: $(a^{-1}a)b = (a{-}1a)c$, so $1b = 1c$ and $b = c$.

   (c) Provide an example of arithmetic mod N, where $ab = ac$ but $b \neq c$.

   Wait, we just proved this, and now we want to provide a counterexample? Not exactly: we proved something was true *in a group*.

   $\mathbb{Z}_n$ is not a group under multiplication. To get a group you must strike out a bunch of numbers. For example, $\mathbb{Z}_n = \{0, 1, 2, 3, 4, 5\}$ while $\mathbb{Z}_n^\times = \{1, 5\}$.

   For a counterexample, try $\mathbb{Z}_6$ with some of these unwanted numbers: $3 \times 2 \equiv 3 \times 4 \equiv 0 \pmod 6$, and yet $2 \not\equiv 4$.

3. (a) Explain the ElGamal encryption algorithm.

   (b) Provide an example using the prime $p = 19$, and generator $g = 2$ That means: generate a public key, and use it to encrypt the plaintext $P = 3$.

   We choose h_A (secret,) then public $H_A = 2^{h_A} \pmod{19}$. That's part one. If we do not choose h_A carefully, then we cannot compute part two all the way.

   Encryption means choosing a random r and computing $P(H_A)^r$. That part has to be easy, so we want a small H_A. How to get a small H_A? Trial and error is one possibility. Look at the powers of 2 mod 19: $1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1$. Okay, so $2^13 \equiv 3$, and 3 is small.

   Great, we choose $h_A = 13$, so $H_A = 3$. Encryption is $P \times 3^r$, and let's choose a small $r = 2$. $C = 3^3 = 27 \equiv 8$.

4. Write out the elements of the group $\mathbb{Z}_{30}^\times$. Name three elements of $\mathbb{Z}_{30}^\times$ equal to their own inverses.

   The wrong way to do this is to compute the inverse of each element of $\mathbb{Z}_{30}^\times$. The right way is to observe that if $a = a^{-1}$, then $a^2 \equiv 1$.

   So first compute the elements of $\mathbb{Z}_{30}^\times$, then write out their squares:

a	1	7	11	13	17	19	23	29
a^2	1	19	1	19	19	1	19	1

...so 1, 11, 19 and 29 are self-inverses.

5. Compute:

   - $\phi(50) = 50(1-1/2)(1-1/5) = 20$
   - $\phi(1024) = 1024(1-1/2) = 512$
   - $\phi(77) = 77(1-1/7)(1-1/11) = (7-1)(11-1) = 60$
   - The last 3 digits of $7^{5122005}$

     3 digits means mod 1000. $\phi(1000) = 400$, and so we reduce the exponent mod 400:

     $$7^{5122005} \equiv 7^4 \pmod{1000}$$

     ...so take the last 3 digits of 49^2.

6. Compute the following inverses:

   - $16^{-1} \pmod{31}$

     $$\begin{array}{rcrcl} N & & & = & 31 \\ & & a & = & 16 \\ N & - & a & = & 15 \\ -N & + & 2a & = & 1 \end{array}$$

     Check: $2(16) = 32 \equiv 1 \pmod{31}$.
   - $7^{-1} \pmod{100}$

     $$\begin{array}{rcrcl} N & & & = & 100 \\ & & a & = & 7 \\ N & - & 14a & = & 2 \\ -3N & + & 43a & = & 1 \end{array}$$

     Check: $43(7) = 301 \equiv 1$.

7. (a) Suppose you have a large number $n = pq$. Now suppose I have the job of computing $3^{2^M} \pmod{n}$. That is, I have to start with the number 3, then square it M times.

   This requires M squarings. Explain how I could do it faster if I knew the factorization of n.

   (b) An example: suppose I take the number 3 and square it 15 times. What is this number modulo 100?

The trick is to use Fermat's Little Theorem. To compute $3^{2^M} \pmod{n}$, reduce the exponent $2^M \pmod{\phi(n)}$.

For example, $3^{2^{15}} \pmod{100}$: we take $2^{15} = 32768 \pmod{40}$. This is easy, because $32768 = 32000 + 600 + 160 + 8 \equiv 8$. So $3^{2^{15}} \equiv 3^8 \pmod{100}$. The last two digits are 61.