Asymmetric cryptography & large-number algorithms homework

This homework is ungraded. Its purpose is to help you understand course material. Doing these problems may help you with your graded homework and quiz. Problems like these may appear on the midterm or final. You should attempt to complete them before the end of the module (time permitting), and at a minimum study them and their provided solutions.

1. Recall that the extended GCD algorithm goes like this.

   ```
   When calculating the GCD of a and b, repeatedly do the following:
      Rewrite egcd(x, y) as egcd(y, r) where x = qy + r for some 0 <= r < y
      Solve for r: r = x + (-q)y
      Substitute combinations of a and b for x and y, and simplify
   ```

   At each iteration of the algorithm, you get a new r as a combination of a and b, which can be used in later iterations for substitution. The algorithm terminates when r=0, meaning that y is the GCD.

   Follow this process to find egcd(59,55) and format your intermediate results as seen in class.

2. Compute 55^{-1} mod 59 using the result of Problem 1. Explain.
3. Let p=367 and q=373 be randomly chosen primes. Use them to produce a public and private RSA key. When it comes time to pick e, choose the smallest value greater than 1 that qualifies. When it comes time to find an inverse, use the extended GCD algorithm to find it. Use your public key to encrypt 5, and show that your private key returns 5 when decrypting the result.
4. In class we saw an exponentiation algorithm that runs in time proportional to the length of the exponent. Follow that algorithm to compute 12^{13} mod 13. Mod each of your intermediate values to keep them from getting too big. Format your computation similar to the following example which computes 3^5 mod 10:

   Exponent 5 in binary is 101 indicating (from left-to-right) SQ-MULT / SQ / SQ-MULT.

Next step	=	Value (mod 10)	=	As exponent (in binary)
initial value	=	1	=	3^{0}
$1^{2} \cdot 3$	=	3	=	3^{01}
3^{2}	=	9	=	3^{010}
$9^{2} \cdot 3$	=	3	=	3^{0101}

   The first line shows the identity equal to the base raised to 0. Each subsequent line shows on the left the prior value squared or squared and multiplied by the base, as appropriate, and then the result modulo the modulus. This is followed by the base to the current exponent in binary. On a quiz, you may be asked to express the SQ/SQ-MULT sequence in text without spaces, placing a close parentheses after each SQ or SQ-MULT. For 3^5 the answer would be `(((1^2*3)^2)^2*3)`. Write 12^{13} as a similar sequence.

5. GCD can be computed in Gallois fields too. The algorithm is the same: repeatedly rewrite gcd(x,y) as gcd(y, x mod y) until you get a remainder of 0. (The "mod" here is remainder after dividing polynomial y into polynomial x, so do long division to find the remainder.) It does require greater attention to avoid mistakes though. Compute $(x^3+x^2+x+1)^{-1}$ in GF(2^4) using the egcd algorithm learned last week. Do all your additions and multiplications using x^4+x+1 as the modulus you use whenever you multiply and the result becomes degree 4 or more.
6. Find a random prime number in the range 1000 - 9999 by picking a random four-digit odd number and performing the probable prime test from class enough times that you're pretty sure it's prime. If it turns out not to be prime, try a new number. Ultimately verify your number is prime by going to WolframAlpha and checking there (for example, "531 prime?" reports that 531 is not prime).
7. Every element of a group generates a subgroup, and the size of the group is always a multiple of the size of the subgroup. For Z_7 and Z_8 determine the subgroups generated by each of its elements.
8. Let's say Diffie-Hellman key-exchange is being done with generator g=4 and modulus p=467. Note that g generates a subgroup of size 233. What is the key produced when the exponents chosen by the two parties are 400 and 134? What is the key produced when the exponents chosen by the two parties are 167 and 134? Why are the keys identical?
9. A small elliptic curve group has elements from $\{(x,y) \in Z_p \times Z_p \mid y^2=x^3+ax+b \bmod p\} \cup \{0\}$ where a=1, b=6 and p=11. Let's say you choose 6 as your multiplier in a Diffie-Hellman key exchange and you receive (5,9) as your communication partner's contribution. What is the shared key generated?

Ungraded homework solutions

These are best studied after completing the homework or after struggling with it for a while.

Solutions PDF.