CSE 590 YA: Practical Aspects of Modern Cryptography
Winter 2002

Assignment #1

Due in class: Tuesday, January 15

1. Describe (or draw) a protocol flow tree for the "first heads lose" game presented in class. Is this the only possible tree that cannot be reduced or are there others?

2. Describe (or draw) a protocol flow tree for the "working" remote coin flip protocol presented in class. Why does this tree not get reduced in practice?

3. Suppose that two 1024-bit integers are represented using 32-bit blocks. Determine the number of 32-bit multiplications required to produce the product of the large integers using standard multiplication. Repeat the calculation using Karatsuba multiplication (recursively).

4. Suppose that a 1024-bit integer is represented using 32-bit blocks. Determine the number of 32-bit multiplications required to square the large integer using the trick for efficient squaring described in class. How does this compare with using Karatsuba? Is squaring any easier than general multiplication when Karatsuba is available (don't neglect overhead)?

5. What is the asymptotic complexity of raising an n-block integer to an n-block exponent modulo an n-block modulus? What is the asymptotic complexity of raising an n-block integer to a constant exponent modulo an n-block modulus?