Cryptology

Read the first three sections of chapter 13. We will start with the third.

Problems

To be discussed Wednesday, May 2, 2001.

1. Do problems 6.1.a, 6.1.b, and all of 6.5 in the textbook.

2. Give an intuitive reason for believing that the verification protocol for the Chaum-Antwerpen Undeniable Signature Scheme (Figure 6.7 on page 219) is not a zero-knowledge protocol.

3. In class, we looked at a probabilistic encryption scheme whi ch had its security based on the Quadratic Residuosity Assumption, and we observed that this scheme could be used for bit commitments (blobs). User A has a public key pair (N, y), where N is the product of two large primes and y is a quadratic nonresidue with Jacobi symbol $+1$. To commit to a bit b, user A chooses a random $r \in Z_N^*$ and produces the blob $y^b r^2 \pmod{N}$. Suppose that user A has committed to two bits b_1 and b_2, producing blobs B_1 and B_2. Show how A can use the blobs B_1 and B_2 to reveal c such that $c = b_1$ XOR b_2, and to prove to another user B that $c = b_1$ XOR b_2, without revealing b_1 or b_2. (The fact that this can be done means that this system for producing blobs has what is called the *equality property*, because it can be used to show that two blobs are commitments to equal bits, showing that the XOR is zero.)