# Cryptology

Read sections 12.4, 6.1, 6.2, and 6.3, plus the article on probabilistic encryption.

# Problems

To be discussed Wednesday, April 18, 2001.

1. Suppose $p \equiv q \equiv 3 \pmod 4$ are both primes and $n = p \cdot q$. Suppose $x$ is a QNR modulo both $p$ and $q$. Show that $-x$ is a QR modulo $n$.

2. In the Diffie-Hellman key-exchange system (Figure 8.5), consider the possibility that the number $\alpha$ is not a generator.

a. Would a pair of users still be able to agree on a key?

b. When the two users agree on a key, what effect would the fact that $g$ is not a generator have on an eavesdropper's ability to determine that key?

3.a. Show that when two primes $p$ and $q$ are both congruent to 3 modulo 4 and $N = p \cdot q$, then every quadratic residue modulo $N$ has exactly one square root which is quadratic residue.

b. Show that this does not hold when $p$ and $q$ are congruent to 1 modulo 4. What holds here?

c. Design a probabilistic encryption scheme based on 3b. Give algorithms for encryption and decryption. Which keys are public and which are secret? What assumption do you need for securtiy?