Homework 1  ICS 247 Security Algorithms
Due: Friday, January 23, 2004, in class

Please answer the following questions, each of which is worth 10 points.

1. Show how a man-in-the-middle attack can defeat the Diffie-Hellman method for establishing a shared secret key between two parties (Alice and Bob).

2. Decrypt the following cipher text, which was generated from English text using a substitution cipher:

   ZLFIF ADVZ RF W BWH PDZ, YPF ZLPDOLZ. PJ UPDIVF, SJ LF LWG IFARFIFG
   ZP RISNO LSV IDRRFI ULSUMFN, SZ BPDQG RF FWVH. RDZ SN ZLSV IPPA WQQ
   YPF UPDQG VFF BWV W ZWRQF, W ZPH XWNGW, WNG W LWAAFI. PDZ PJ
   JIDVZIWZSPN, YPF LSZ ZLF XWNGW BSZL ZLF LWAAFI. ZP LSV QIFWZ
   VDIXISVF, ZLF XWNGW RIFMF PXFN WNG IFARFQFG LSV BWH PJ FVUFQF--W
   HFQQPB, IDRRFI ULSUMFN!

3. In a public-key system using RSA, you intercept the ciphertext $C = 10$, sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext $M$?

4. In a public-key system using RSA, the public key of a certain user is $e = 31$, $n = 3599$. What is the private key $d$? Hint: you may use the Unix program `factor`.

5. In a public-key system using RSA, the public key of a certain user with public key $e, n$ leaks his private key $d$. Being lazy, he recomputes a new $e$ and $d$ using the same $n$. Is this safe? Why or why not?