

Hand in a stapled, printed copy with your answers.

Homework: /SI110/Models and Tools/Asymmetric Cryptography

1. What is the problem with symmetric (secret key) encryption that asymmetric (public key) encryption solves?

2. Alice wants to send a message only Bob can read, so Alice encrypts her message with (Circle the correct answer):

- a. Alice's Public Key
- b. Alice's Private Key
- c. Bob's Public Key
- d. Bob's Private Key

3. Alice wants to send a message only Bob can read, and which Bob will know could only have come from Alice. So Alice first encrypts the message with ___ and then encrypts the result with ___. (Fill in the blanks from the choices below)

- a. Alice's Public Key
- b. Alice's Private Key
- c. Bob's Public Key
- d. Bob's Private Key

4. Your public key is: (47619e21,a8cb571dc35f824cb8d4020cd4a838a7)
Your private key is:(9c2cee3afecbf23d6f9b8d8af18a8439,a8cb571dc35f824cb8d4020cd4a838a7)

Using <http://rona.cs.usna.edu/~sil10/resources/rsa/index.html>, decrypt the following secret message I've encrypted just for you:

574d151839ce74586ff340c7354ab624748bdd688731491a4ba1f643ecd3e994

Message is:

5. My public key is (a7d7,75dda50d2af8a490a7ccf56fde44cf6d), yours the same as problem 4. Decrypt the following message, which I've encrypted (following the scheme from the notes) so that only you can read it, and so that you'll know that only I could've sent it.

3a3d8897f0c45c4b9c08bcc36e74297a7cd9b4ec4c445ba66fe5677fda59bfde173fbfdc9ce29825919163b0ef099464

Message is:

How do you know that it had to come from me?

6. If you see "1024-bit RSA", what does the "1024-bit" refer to?