Homework 16, due October 30

(1) Let $n = 1042387$. Factor $t^2 - n$ for

$$t = 1021, 1027, 1030, 1061, 1112, 1129, 1148, 1175, 1217, 1390, 1520.$$

Make a matrix (as in section 6.4.1) and find at least two linear dependencies $\pmod 2$ among the rows. Use this information to factor n. Explain your work.

(2) Let $n = 527773$. Calculate the values of the polynomial $f(x) = (x + \lfloor\sqrt{n}\rfloor)^2 - n$ for x from -17 to 17 and factor them. (Remember that primes p with $\left(\frac{n}{p}\right) = -1$ will never divide $f(x)$.) Use this information to find some squares that factor into small primes $\pmod n$, and use this information to factor n. Explain your work.

(3) Bob's public RSA key is $(n, e) = (47198353746711821023370804532488820972149852741 3, 37)$. You have reason to believe that Bob has a fairly weak RSA key. You intercept a message intended for Bob:

`275978703881445420068277310027406516799428995 36`

Decrypt. Explain how you did it.

(4) Alice, Bob, and Eve use a public key cryptosystem; they have keys k_A, k_B, k_E respectively. (Thus Alice has encryption and decryptions functions E_{k_A} and D_{k_A}, etc.) Alice proposes that to send messages, they use the following protocol for user X to send message M to user Y (messages are of the form (sender's name, text, receiver's name), and $M|X$ is the concatenation of the strings M and X):

- X sends Y the message $(X, E_{k_Y}(M|X), Y)$.
- Y's computer decrypts $M|X$ by applying D_{k_Y}, and acknowledges receipt by automatically sending X the message $(Y, E_{k_X}(M|Y), X)$.

Eve claims that this protocol is too complicated, and that it would be easier to do the following:

- X sends Y $(X, E_{k_Y}(M), Y)$.
- Y acknowledges receipt by sending X $(Y, E_{k_X}(M), X)$.

If Eve can intercept Alice and Bob's encrypted messages, how could she use this simplified protocol to read a message M that Alice has previously sent (encrypted) to Bob?