

MATH 470 Homework 5

1. Show that $\sqrt{2} = 1 + 1/x$ where $x = 1 + \sqrt{2} = 1 + \frac{1}{x}$ and so $x = 2 + \frac{1}{x} = 2 + \frac{1}{2 + \frac{1}{x}} = \dots$

Use this idea to compute the continued fraction expansion of $\sqrt{6}$.

Write $\sqrt{6} = 2 + \frac{1}{x}$. Then $x = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} = 1 + \frac{1}{2}\sqrt{6}$. Also, $x = 1 + \frac{1}{2}(2 + \frac{1}{x}) = 2 + \frac{2}{x}$. Thus iteratively replacing x by $2 + \frac{2}{x}$ gives

$$\sqrt{6} = 2 + \frac{1}{x} = 2 + \frac{1}{2 + \frac{1}{4 + \frac{1}{2 + \frac{1}{4 + \frac{1}{2 + \dots}}}}}$$

$$\sqrt{6} = [2 : 2, 4, 2, 4, 2, 4, \dots]$$

2. Compute the gcd of 12345 and 98765 using the extended Euclidean algorithm.

Compute the continued fraction expansion of $\frac{98765}{12345}$.

Show the relationship between your two calculations.

3. Bob has published RSA parameters of $n = 26069$ and $e = 22063$. From the large value of e Eve suspects that Bob may have used a low value of d to make decryption faster. Use the continued fraction expansion attack to determine the factors of n . Show all your work.

[For your convenience: the continued fraction expansion of $\frac{e}{n}$ is $[0; 1, 5, 1, 1, 32, 1, 7, 1, 1, 3]$

and the subsequent fractions are: $1, \frac{5}{6}, \frac{6}{7}, \frac{11}{13}, \frac{358}{423}, \frac{369}{436}, \frac{2941}{3475}, \frac{3310}{3911}, \frac{6251}{7386}, \frac{22063}{26069}$.]

4. Bob spent some time making sure he had a selection of “strong primes” for his RSA parameters. Since Alice and Bob are very friendly, Alice decided to use some of this research. Now having just taken the exam in Math 470 they knew that using different moduli n 's that shared a common prime was a total disaster, so she decided to use both his primes to get the same modulus n . Of course, she used a different (prime) value for her exponent e .

If, for example, Eve intercepted the same message m encrypted as c_A and c_B using Alice and Bob's RSA public keys would this help to determine m ?

If the two exponents were e_A and e_B , since these are public, Eve (or anyone else) could run the Euclidean algorithm on them to find integers s and t such that $e_A s + e_B t = d = \gcd(e_A, e_B) = 1$. Eve has intercepted the codetexts $c_A = m^{e_A} \pmod{n}$ and $c_B = m^{e_B} \pmod{n}$. Now $(c_A^s)(c_B^t) = m^{e_A s} m^{e_B t} = m^{e_A s + e_B t} \pmod{n} = m \pmod{n}$. Since the message must be less than the modulus, Eve has obtained m by just one run of the Euclidean algorithm and two equally fast

modular exponentiations.

Note: we don't need the two exponents to be prime numbers, just to be relatively prime.

Moral of story for Bob: don't share your primes with even you best girlfriend.

5. Bob was worried that Eve might be reading his RSA-encrypted e-mail. So he decided to "double encrypt"; that is he chose two exponents e_1 and e_2 and used the following scheme: The message m was first encrypted by $b \equiv m^{e_1} \pmod{n}$ and then again by $c \equiv b^{e_2} \pmod{n}$. The final ciphertext c was then transmitted. Did this process strengthen the cipher or in fact weaken it?

We have $c \equiv b^{e_2} \equiv (m^{e_1})^{e_2} \equiv m^{e_1 e_2} \pmod{n}$. Thus the effect here is to run a single RSA cipher with the same n but exponent $e = e_1 e_2$. If the e_1 and e_2 are prime then there should be no issue in computing a decryption exponent d , but the net effect has been to double the computational effort.

[We say here that RSA forms a group: $E_{e_1} E_{e_2} = E_{e_1 e_2}$.]

6. Dave Dim thought he had invented a novel system: a combination of RSA and *Vigenere*. He took each character of the message (with *space* = 00, *a* = 01, *b* = 02, ... *z* = 26) and encrypted it using RSA separately; the first letter using an encryption exponent e_1 , the second letter using an encryption exponent e_2 and so on up to e_{10} when the same e 's were used again in order. Dave published n and the exponents e_j , $1 \leq j \leq 10$. The modulus n was the same in all cases and just to make sure he used a super industrial grade pair of primes that gave an n with 1,000 digits. In addition, since the plaintexts were small he chose large exponents; each e_j was a prime with at least 500 digits. Of course each letter produced a ciphertext c of roughly 1,000 digits, and so the transmission was much longer, but to Dave that wasn't as important as security.

Was this a good idea, or did it just make extra computation over using a large message blocksize (which given the size of the modulus could have been up to 1,000 digits or 500 characters) and a (much) smaller exponent e ? Or is it worse and actually cryptographically insecure?

This is amazingly stupid. What would Eve do? Just make up a table of the cipher texts obtained with the published n and each published e_i for each letter. For each e_i there are only 26 possibilities of c . Since these are about 1,000 digits long the chance of any two being the same is effectively zero. Since we know each e_i is being used in sequence, we simply do table-lookup to find the correct letter. In other words dave has simple set up an amazingly long-winded substitution cipher (where each letter gets replaced by a very large digit) and *published the key that lets everyone know what corresponds to which!!*. It isn't even a cipher in any sense of the word.