# Problem Set 2

Due in class on Thursday, February 17, 2005.

## Problem 5: Number theory review

Do the following number theory problems (a little bit mathematical):

(a) Express 1 as a linear combination of 2058 and 1019. What is $1019^{-1}$ modulo 2058?

(b) Calculate $2^{5^{49}} \bmod 29$.

(c) Compute $\gcd(6188, 4709)$.

(d) Show that 1234 and 357 are relatively prime. Find the multiplicative inverse of 357 in $\mathbf{Z}_{1234}$.

## Problem 6: Number theory on computer

(a) Use Erathostenes's Sieve to count the exact number of primes less than one million. What is the estimate given by the Prime Number Theorem for this number? What is the relative error of the estimate?

(b) Get a ball-park figure of the time it takes to generate 1024-bit (308 decimal digits) and 2048-bit RSA keys on a modern PC by implementing RSA key generation using ln3 or any other big number package. Submit both the answer to this question and also the documented code that you wrote.

## Problem 7: RSA: Theory and Practice

Both mathematical and practical:

(a) (With pen) My toy RSA key is $N = 187$, $e = 107$. You observe a ciphertext $c = 5$. What is the plaintext?

(b) (With computer) Consider this RSA key

$N$ : 120457322460183418712065226069810172366048205604752299621042894
39770697900429359585533767395421537426263779452427204581821790 8
22947852658450047816163958146531233838578299654147720502711130 4
59462312186809271138496279782427321976078144123995378177130091 3
27992893347504900757047650844010384728900224247825638890 9.

$e$ : 108320892662862955596302357470782070713553067937889499942447147
35596865669435990346286776488201251207385336570154952160651134 8
71410417277032505133515738726875481503727456543694453486715313 2
29268413374246402921464854075018217158897213837803675005544643 8
69807629707802724827418271187297432607642943850779427095 1.

Suppose you manage to obtain the decryption key

$$d : 870778041505896784929057064247111975431088041103712624121674096$$
$$250991494449208495397081617394569729997785285908978755792242047$$
$$951504608606471891232362973145723219036260087876400092012690445$$
$$506827289066083911176383869641400399764707038140971639114758576$$
$$803956361759865393827611426273085021285958953198368839 91.$$

Factor $N$. (These numbers will be placed in the file /c/cs467/assignments/ps2/rsakeys.txt on the Zoo so that you don't need to copy them by hand.)