Some computational problems in number theory

January 14, 2016

(1) Say that I have a 2x2 matrix of the form:

$$A = \begin{bmatrix} 3 & * \\ * & * \end{bmatrix}$$

I don't know the matrix itself, but I do know that $det(A) \equiv 17 \ (mod\ 26)$ and I also know that

$$A \begin{bmatrix} 5 \\ 19 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 9 \end{bmatrix} \ (mod\ 26).$$

Find the matrix A.

(2) Calculate the Euler phi function of 864864. Use it to calculate

$$5^{207366} \ (mod\ 864864)$$

(3) In divising the RSA system you choose a public modulus $m = 1081 = 23 \cdot 47$ and an encrypting exponent of 73. Find the decrypting exponent.

The next problem requires a computer

(4) Say that your public modulus is:

$$m = 91940503602139071156933662853049152155202746298534495 61$$

$$= (9834710928479123480819)(9348572039458723049587230496060 19)$$

and nobody else knows how your number factors. You also publish your public key to be:

$$34871928376451982734629 39$$

which you choose at random so that it is relatively prime to $\phi(m)$. I send you the message 60013421429603075773376518639013271388910603264548977 97, what does it say?