EXERCISES ON CRYPTOGRAPHY

YANG WANG

Problem 1 In class we have discussed $a^{-1} \pmod N$, which exists and is unique if a and N are coprime. But we had not mentioned how to find $a^{-1} \pmod N$ given two coprime integers a and N. One fast way to find it is to use the so-called *Euclidean Algorithm.*

(A) Find out what the Euclidean Algorithm is and how it works. It can be found on the web or in any standard text in number theory.
(B) Illustrate how the Euclidean Algorithm allows you to solve for integers x, y such that $137x + 1000y = 1$. You must show all the steps to demonstrate the use of the Euclidean Algorithm.
(C) Illustrate how the above allows you to find $137^{-1} \pmod{1000}$.
(D) Let $a = 9923$ and N be the first 4 digits of your MSU student ID number. Use the Euclidean Algorithm to compute $a^{-1} \pmod N$ by hand (you may use a calculator to compute some routine multiplications only). Again you must show all the steps to demonstrate the use of the Euclidean Algorithm. (The purpose of this exercise is to show you that even for very large a, N one can compute $a^{-1} \pmod N$ rather efficiently.)

Problem 2 We discussed the invertibility of a square matrix in modular arithmetic. To find $A^{-1} \pmod N$ one can often just invert A as if it were an integer matrix without worrying about $\pmod N$ to obtain an inverse with elements being fractions, and in the end invert the denominator $\pmod N$. Consider the matrix

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 1 & -2 & 1 \\ 0 & 2 & 1 \end{bmatrix}$$

Find the inverse matrix $A^{-1} \pmod{29}$.

Problem 3 Assume that in our RSA public key cryptosystem the encryption key is $(N, e) = (1073, 41)$.

(A) Find the deciphering key (N, d) without using a computer or calculator.
(B) Assume that you have received the enciphered message $\mathcal{C} = 830$. Decipher it. In the standard 26 letter alphabet digraph, which two letters does the deciphered message correspond to, assuming that the messages are coded using base 26 expansion as discussed in class before?

Potential Term Project Topics Cryptography is an area where it is rather easy to find interesting term projects. Here are some suggestions, but of course you are encouraged to explore further.

(1) Do an in-depth review of one of these other public key cryptosystems.
(2) In-depth review on how Bitcoin works.
(3) In-depth review of how the German Enigma code worked, and the Allied effort to solve it.
(4) Study on your own how digital authentication can be done in a public key cryptosystem such as the RSA. Write an essay describing how is it done (try to be concise and to the point) or have it as part of your end of semester presentation.