Homework 8

due Wednesday November 25, 2015

Problem 1.
Suppose you intercept the public key

$$(e, n) = (972828952658213, 1021916794516973)$$

and the ciphertext 667391567223399. What was the original message? (*Hint*: you can use `Sage` and the factor command to first "crack" the code and then decipher it. If you use the ASCII decoding of the resulting number you actually get a text.)

Problem 2.
Consider the following variant of the Diffie–Hellman key exchange protocol:

(1) Alice and Bob publicly choose a big prime p and a number $1 < r < p$ together.
(2) Alice secretly chooses an integer $1 \leq k_A < p - 1$ and Bob secretly chooses an integer $1 \leq k_B < p - 1$.
(3) Alice tells Bob $k_A r \pmod{p}$.
(4) Bob tells Alice $k_B r \pmod{p}$.
(5) The "secret" key is $s \equiv k_A k_B r \pmod{p}$ which both Alice and Bob can easily compute.

Now do the following:

(a) Suppose you are Alice and you agreed with Bob to pick $p = 83$ and $r = 6$. You secretly picked $k_A = 42$ and receive from Bob $k_B r \equiv 79 \pmod{83}$. What would be the secret key s? Which number would you tell Bob?
(b) Everybody including evil Eve knows $p = 83$, $r = 6$, the number Alice told Bob $k_A r$ and the number Bob told Alice $k_B r$. Eve can now solve for x and y in $xr + yp = 1$ since $\gcd(r, p) = 1$. What are x and y?
(c) Show that Eve can now retrieve k_A. How?

This exercise shows that in the Diffie-Hellman key exchange it is important to take exponents and not just products!

Problem 3.
This is a real life scenario that happened recently: Professor Dan Bump from Stanford University opened a repository with some files and asked all collaborators to send their public keys. Is it secure to send the public key by e-mail? Explain your answer!

Problem 4.
Show that if n is a positive integer, then

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0,$$

where $\mu(n)$ is the Möbius function.

Problem 5.
Let n be a positive integer. Show that

$$\prod_{d|n} \mu(d) = \begin{cases} -1 & \text{if } n \text{ is a prime} \\ 0 & \text{if } n \text{ has a square factor} \\ 1 & \text{if } n \text{ is square-free and composite.} \end{cases}$$