Problem Set 6

This problem set is due on *Thursday, October 28, 1999* at the end of class. Late homeworks will *not* be accepted. You are to work on this problem set in groups of three to four people. (Be sure that you all understand the solutions turned in to each problem.)

Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**[1], and be clear. Points may be deducted if your TA has problems understanding your solution.

Problem 6-1. The Real World

Pick a vulnerability or exploit described in Lecture 12. Describe it in detail. What tools are available to automate it? Under what circumstances does it succeed? Under what circumstances does it fail? Describe some ways of protecting against this vulnerability.

Please limit your discussion to two pages. Assume general familiarity with the topics and issues – focus on the more interesting material.

If you get a check plus on this problem and you include a pointer to the Latex, you will get included in the solutions. Yes, this means there will be a number of 4's given for this problem.

Problem 6-2. Discrete Logs

Let p and q be distinct primes, and let $n = pq$. Suppose that g is a generator of both Z_p^* and of Z_q^*. (That is, the powers of g yield all the nonzero elements mod$p$, and similarly mod$q$.)

Let x be an integer that is relatively prime to both p and q, and suppose that we know the discrete logarithm a of x mod p and the discrete logarithm b of x mod q. Thus

$$g^a = x (\mathrm{mod} p)$$

$$g^b = x (\mathrm{mod} q)$$

(a) Do these assumptions imply that there exists an integer c such that

$$g^c = x (\mathrm{mod} n)$$

(b) Explain what additional conditions, if any, are required to ensure the existence of c, and show how to compute c efficiently from p, q, g, a, b when it exists.

Problem 6-3. Common Modulus Systems

Alice and Bob are very good friends. In order to save time, they agree to simply find one good pair of primes p, and q, and therefore use the same public modulus $n = pq$. Of course, to not have any

[1]If you latex your solutions, include a URL or AFS path where I can find the latex file(s); I will distribute my favorite solution for each problem to the class as the 'official' solution – this is your chance to become famous! Note that if I choose your solution, then you get an extra point on that problem.

confusions over who signed which message and to prevent, they select different exponents e_a and e_b.

Show that in this system, it is possible to decrypt a message M sent to both of them if $\gcd(e_a, e_b) = 1$. That is, given:

$$\begin{aligned} C_a &\equiv M^{e_a} \pmod{n} \\ C_b &\equiv M^{e_b} \pmod{n} \end{aligned}$$

an adversary can compute M.

Problem 6-4. Bonus Point

Add a new user `toor` to the password file of `belegost.mit.edu`. You are free to probe, scan, attempt remote buffer overflow exploits, etc, but don't specifically attack to deny service, and don't break laws with respect to any other computers or people (in particular, do not attempt to gain physical access to the machine).

This problem is difficult – I do not expect any groups to succeed. If you do seriously deny service for the machine, you will lose a point rather than gain a bonus point on this problem set. If you succeed, you get an extra (bonus) point on the problem set. No need to do any sort of write-up for this problem.