YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #23*
Felipe Saint-Jean *December 9, 2005*

Solution to Problem Set 7

Due in class on Thursday, November 17, 2005.

In the problems below, "textbook" refers to *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington..

Problem 32: Discrete log authentication

Textbook, problem 14.3.2.

Solution:

part a

If Peggy does not know a she can't know both r_1 and r_2 at the same time. Otherwise she would know a, since $a = r_1 + r_2$. If Victor requests the number that Peggy does not know, then his checks will fail, and he will not be convinced.

part b

By part (a), Peggy knows at most one of r_1 and r_2 at each trial. If Victor chooses i uniformly at random he has a probability of at most $1/2$ of getting a number from Peggy that passes his checks. Victor is convinced only if his checks succeed on each of t trials. The probability of that occurrence is at most $1/2^t$.

part c

The random number r is uniformly distributed over $\mathbf{Z}_{p-1}$. Less obvious is that $(a - r)$ is also uniformly distributed over $\mathbf{Z}_{p-1}$. This is because the mapping $r \mapsto (a - r)$ is a permutation on $\mathbf{Z}_{p-1}$. Hence, whichever r_i Victor requests, Nelson can just send back a random number in $\mathbf{Z}_{p-1}$, and Victor has nothing to verify it against. In Peggy's scheme, h_1 and h_2 serve to commit her to r and $a - r$, and Victor has the opportunity to verify one of those two commitments..

Problem 33: Challenge-response protocol

Textbook, problem 14.3.3.

Solution:

part a

What Nelson does is compute the square root $\pmod p$ and $\pmod q$ using the method of Section 3.9. He then combines the results using the Chinese Remainder Theorem to generate a square root $\pmod n$.

part b

Victor can generate a random number r and send $r^2 \pmod{n}$. If he gets back a root r_2 that is not r or $-r$ he can factor n by computing the $\gcd(r - r_2, n)$.

part c

She gets no information. All she sees are pairs of the form (y, y^2) that are indistinguishable from pairs generated by a simulator that generates y at random and gives her the pair (y, y^2).

Problem 34: Schnorr identification scheme

Textbook, problem 14.3.4.

Solution:

part a

$$\alpha^y \beta^r \equiv \alpha^{k-ar}(\alpha^a)^r \equiv \alpha^{k-ar+ar} \equiv \alpha^k \equiv \gamma \pmod{p}$$

part b

No, all he knows after the protocol is γ, and y. He can't compute k from γ because that is a discrete log problem. Since he doesn't know k, y looks just a random number (all possible values for a are equally likely given y). Therefore he can't get a from it.

part c

Those are the same values Victor knows. Since he can't compute a then neither can Eve.

part d

In that case Eve knows

$$y_1 \equiv k - ar_1 \pmod{p-1}$$

and

$$y_2 \equiv k - ar_2 \pmod{p-1}.$$

Knowing y_1, y_2, r_1 and r_2 she can solve for a and k.

Problem 35: RSA-based authentication scheme

Textbook, problem 14.3.5.

Solution:

Step 4: Victor asks for r_i with i chosen uniformly from $\{1, 2\}$ and verifies that $r_i^e \equiv x_i \pmod{n}$. If Peggy is cheating she has a probability of successfully cheating of $\frac{1}{2}$ on each iteration. To have a 0.99 probability of catching a cheating Peggy they need to repeat the protocol s.t.

$$\frac{1}{2^t} \leq 0.01$$

so they need to repeat the protocol at least 7 times.