Solutions to Problem Set 4

Problem 4-1. Smaller and Smaller

This problem was apparently much more difficult than we anticipated. Therefore, the grading was somewhat more lenient than normal. The following was a popular solution which was not what we were looking for, but which was acceptable. The "correct" solution will appear after that.

(a) Diagnolizeable matrices can be represented as

$$\begin{aligned} M &= S\Lambda S^{-1} \\ M^e &= S\Lambda^e S^{-1} \end{aligned}$$

Where Λ is a diagonal matrix whose elements are the eignevalues of the matrix. Since it is easy to raise diagonal matrices to powers (just raise all the elements to the power), we can easily compute M^e for any diagonalizeable matrix.

When doing these operations mod$n$, we do the same thing. Then, we can select $ed \equiv 1 \pmod{(p-1)(q-1)}$, and do RSA just like we always did.

However, the method of computing the eignevalues requires us to compute square roots (in mod n). However, only 3/4 of the numbers in $modn$ have square roots, so this only works for about 3/4 of the possible matrices. Our requirement is therefore that the matrix be diagonlizeable (which, btw, assumes we know how to compute square roots, which means this scheme is only useful for signing – you need to be able to factor n in order to compute square roots in mod$n$).

(b) The correct solution involves modelling this system as another 'group', and then doing operations over it. We use Lagrange's Theorem and the Chinese Remainder Theorem (from the CLR readings) to solve this for as general a case as we can.

First of all, we note the basis of RSA. e, d are selected such that $ed \equiv 1 \pmod{\phi(n)}$. More importantly, this comes from Lagrange's Theorem which states that if we repeat the group operation a number of times equal to the size of the group, we wrap around. A corrolary of it yields:

$$a^{(x)} \equiv a^{(y)} \text{ if } x \equiv y \pmod{|S|}$$

$$a^{(ed)} \equiv a \text{ if } ed \equiv 1 \pmod{|S|}$$

Where S is the size of the group (normally, it is $\phi(n)$.

Now, we note that Matrix multiplication forms a group if we restrict the matrices to invertible ones (that is, ones who have a determinant that is in Z_n^*). We have an identity, we have an inverse, we have associativity, and we have closure.

Now that we have a group, if we could compute its size (call it $\psi(n)$) we could use Lagrange's Theorem to compute a pair of values $ed \equiv 1 \pmod{\psi(n)}$ which will make the RSA equations work. In order to do this, we model the matrix in mod$p$, and then extend it to mod$n$.

First, we note that invertible matrices in mod$p$ are those where the top row is not zero AND the bottom row is not a multiple of the top row. There are exactly $(p^2-1)(p^2-p)$ such matrices if all the elements are taken mod$p$. This is also true $bmodq$.

If we start with two matrices:

$$A = \begin{vmatrix} a_1 & a_2 \\ a_3 & a_4 \end{vmatrix} \pmod{p} B = \begin{vmatrix} b_1 & b_2 \\ b_3 & b_4 \end{vmatrix} \pmod{q}$$

From the above, we can construct a matrix C that is unique to A, B using the Chinese Remainder Theorem. Since $det(C) \equiv det(A) \pmod p$ and $det(C) \equiv det(B) \pmod q$, we know that the determinant of C is relatively prime to n, and so the matrix formed this way is invertible and in our group. Through the Chinese Remainder Theorem, we therefore have $\psi(n) = (p^2-1)(p^2-p)(q^2-1)(q^2-q)$ possible matrices in our group.

We can now easily pick an e, d pair, and do RSA over the matrices, and we can publish e, n just like with RSA.

Problem 4-2. Strongly Collision-Free Hash Functions

Roger Dingledine
Nick Mathewson
Brian Sniffen

(a)

By definition, if $h_1 = (\mathbb{Z}_2)^{2m} \to (\mathbb{Z}_2)^m$ is strongly collision-free, then it is computationally infeasible to find any messages x and x' such that $x \neq x'$ and $h_1(x') = h(x)$.

We will now prove by contradiction that $h_2 : (\mathbb{Z}_2)^4 m \to (\mathbb{Z}_2)^m$ is strongly collision-free, where $h_2(x) = h_1(h_1(x_1) \parallel h_1(x_2))$, and $x = x_1 \parallel x_2$, for $x_1, x_2 \in (\mathbb{Z}_2)^2 m$.

Suppose that h_2 is not strongly collision-free, and that we have a pair of distinct messages $a, b \in (\mathbb{Z}_2)^4 m$ such that $h_2(a) = h_2(b)$. This implies, by the definition of h_2, $h_1(h_1(a_1) \parallel h_1(a_2)) = h_1(h_1(b_1) \parallel h_1(b_2))$.

Either $h_1(a_1) \parallel h_1(a_2)$ is equal to $h_1(b_1) \parallel h_1(b_2)$, or it is not. Let us consider each case individually.

If, on the one hand, $h_1(a_1) \parallel h_1(a_2) = h_1(b_1) \parallel h_1(b_2)$, then $h_1(a_1) = h_1(b_1)$ and $h_1(a_2) = h_1(b_2)$. In this case, we have computed collisions under h_1, and so h_1 is not strongly collision-free.

If, on the other hand, $h_1(a_1) \parallel h_1(a_2) \neq h_1(b_1) \parallel h_1(b_2)$, then we have found two messages, $m_1 = h_1(a_1) \parallel h_1(a_2)$ and $m_2 = h_1(b_1) \parallel h_1(b_2)$ such that $h_1(m_1) = h_1(m_2)$. So therefore, in this case as well, we can compute a collision under h_1 and so h_1 is not strongly collision-free.

In each case, if h_2 is not strongly collison-free, then h_1 is not strongly collision-free. But by assumption, we know that h_1 is strongly collison-free. So therefore h_2 must be strongly collision-free as well.

(b)

Suppose that $h_i : (\mathbb{Z}_2)^{2^i m} \to (\mathbb{Z}_2)^m$ is defined recursively as given in the problem. We will show by induction that, if h_1 is strongly collision-free, then so is h_i.

Base case: By assumption, h_1 is strongly collision-free.

Inductive step: We will now show that, if h_{i-1} is strongly collision-free, then so is h_i. Our argument runs homologously to the one in part (a) above: if we have can collision for h_i, then we can find a distinct a and b such that $h_{i-1}(h_{i-1}(a_1) \parallel h_{i-1}(a_2)) = h_{i-1}(h_{i-1}(b_1) \parallel h_{i-1}(b_2))$. This implies that either $h_{i-1}(a_1) = hi-1(b_1)$; or that $h_{i-1}(m_1) = hi-1(m_2)$, where, $m_1 \neq m_2$, $m_1 = h_{i-1}(a_1) \parallel h_{i-1}(a_2)$, and $m_2 = h_{i-1}(b_1) \parallel h_{i-1}(b_2)$. In either case, we have a collision for h_{i-1}, and so we deduce that if h_i is not strongly collision-free, then neither is h_{i-1}. The contrapositive of this result gives what we wanted: if h_{i-1} is strongly collision-free, then so is h_i.

Result: Since h_1 is strongly collision-free, and h_{i-1}-is-strongly-collision-free $\Longrightarrow$ h_i-is-strongly-collision-free, we conclude by weak mathematical induction that h_i is strongly collision-free for all $i \geq 1$.