Massachusetts Institute of Technology | Handout 13
6.857: Network and Computer Security | October 8, 1998
Professor Ronald L. Rivest

Problem Set 4

This problem set is due on *Thursday, October 16, 1998* 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. Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**, and be clear. Points may be deducted if your TA has problems understanding your solution. We strongly recommend you get started on this problem set early.

Problem 4-1. Generalizing RSA

Let M_n denote the set of 2×2 matrices with entries chosen modulo $n = pq$.

Can you generalize the RSA encryption scheme to work over M_n? If not, explain why not. If so, explain how in detail. Discuss.

(The factorization of n would be the secret key, and encryption would involve raising a message matrix to some power e given in the public key. If necessary, you can restrict attention to a subset of M_n.)

(Option: You can, if you like, instead do the similar question about adapting the El Gamal encryption scheme to work over M_p for some large public prime p, as long as you attempt to deal seriously with the fact that M_p may not be cyclic.)

Problem 4-2. Smaller and Smaller

Definition 1 *A hash function is* **weakly collision-free** *if, given a message x, it is computationally infeasible to find a message $x' \neq x$ such that $h(x') = h(x)$.*

Definition 2 *A hash function is* **strongly collision-free** *if it is computationally infeasible to find messages x and x' such that $x' \neq x$ and $h(x') = h(x)$.*

Suppose $h_1 : (\mathbb{Z}_2)^{2m} \to (\mathbb{Z}_2)^m$ is a strongly collision-free hash function.

(a) Define $h_2 : (\mathbb{Z}_2)^{4m} \to (\mathbb{Z}_2)^m$ thus:

- write $x \in (\mathbb{Z}_2)^{4m}$ as $x = x_1 \| x_2$, where $x_1, x_2 \in (\mathbb{Z}_2)^{2m}$
- define $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$.

Prove that h_2 is strongly collision-free.

(b) For an integer $i \geq 2$, define a hash function $h_i : (\mathbb{Z}_2)^{2^i m} \to (\mathbb{Z}_2)^m$ recursively from h_{i-1} thus:

- write $x \in (\mathbb{Z}_2)^{2^i m}$ as $x = x_1 \| x_2$, where $x_1, x_2 \in (\mathbb{Z}_2)^{2^{i-1} m}$
- define $h_i(x) = h_1(h_{i-1}(x_1) \| h_{i-1}(x_2))$.

Prove that h_i is strongly collision-free.