Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 14
October 16, 1997

Solutions to Problem Set 4

Problem 4-1. Elliptic Curve Groups

(a) Okay, we plug and chug to get the following values:

$(1,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$
$(2,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$
$(3,0)$	$(2,1)$	$(3,2)$	$(3,3)$	$(2,4)$
$(4,0)$	$(4,1)$	$(4,2)$	$(4,3)$	$(4,4)$

For the particular curve:

$$y^2 = x^3 + x + 1 \pmod 5$$

(b) We get the points on the curve by plugging in values for x and seeing if they work for a pair of y's (note that both the positive and negative values of y are possible). The points on the curve are: I (the point at infinity), $(0,1)$, $(0,4)$, $(2,1)$, $(2,4)$, $(3,1)$, $(3,4)$, $(4,2)$, $(4,3)$.

(c) The addition table for this group is computed by plugging the values into the addition formula. Since we are working in mod 5, we can just take mod 5 of whatever values we get to simplify our computations. The resulting table is:

	01	04	21	24	31	34	42	43	I
01	42	I	34	43	24	31	21	04	01
04	I	43	42	31	34	21	01	24	04
21	34	42	24	I	04	43	31	01	21
24	43	31	I	21	42	01	04	34	24
31	24	34	04	42	01	I	43	21	31
34	31	21	43	01	I	04	24	42	34
42	21	01	31	04	43	24	34	I	42
43	04	24	01	34	21	42	I	31	43
I	01	04	21	24	31	34	42	43	I

(d) To find the order of any element, we just go to the addition table and see how many elements we go through before we get ourselves. Then, we count how many elements we have 'generated'. One thing to note for the order of the set is that whatever order we generate, it can devide the order of the entire set (or 9). Since the only possible values that devide 9 are 1, 3, and 9, we know that those are the only possible orders.

For $(2,1)$, we get:

$$\begin{aligned} (2,1)+(2,1) &= (2,4) \\ (2,4)+(2,1) &= I \\ (2,1)+I &= (2,1) \end{aligned}$$

So we generated 3 items, and so the order of $(2,1)$ is 3. For all the elements(except for I, whose order is always 1), the orders are:

(0,1)	9	(3,1)	9
(0,4)	9	(3,4)	9
(2,1)	3	(4,2)	9
(2,4)	3	(4,3)	9

Problem 4-2. Hash Functions

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 $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$.

We claim that h_2 is strongly-collision free

Proof. We prove by contradiction: Assume it is not, so we can find x, x' s.t. $x \neq x'$ and $h_2(x) = h_2(x')$. Take these x's, and break them into two halves, so: $x = (x_1 \| x_2)$ and $x' = (x'_1 \| x'_2)$. By the construction of h_2, we know that $(h_1(x_1) \| h_1(x_2)) = (h_1(x'_1) \| h_1(x'_2))$. This of course means that both $h_1(x_1) = h_1(x'_1)$ AND $h_1(x_2) = h_1(x'_2)$.

Since $x \neq x'$, $(x_1 \| x_2) \neq (x'_1 \| x'_2)$. So either $x_1 \neq x'_1$ OR $x_2 \neq x'_2$ (or both). Assume w.l.o.g that $x_1 \neq x'_1$. Then, since $h_1(x_1) = h_1(x'_1)$ (from above) we have found a collision. BUT h_1 is assumed to be collision-free, so we have a contradiction.

Therefore, 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 $h_i(x) = h_1(h_{i-1}(x_1) \| h_{i-1}(x_2))$.

Proof. We will prove that h_i is strongly collision-free using induction.

Base case: $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$ was proven above. h_2 is strongly collision-free.

Induction case: We assume that $h_n(x) = h_1(h_{n-1}(x_1) \| h_{n-1}(x_2))$ is strongly collision-free. We need to show that h_{n+1} is also strongly collsion-free. But this proof is exactly the same as the proof of part (a), so we have the inductive step.

Therefore, h_i is strongly collision-free for all values of i, assuming h_1 is strongly collision-free.