Cryptology – E16 – Lecture 7

Lecture, September 26

We covered DES, 3DES and AES from chapter 13.

Lecture, October 3

We will cover the rest of chapter 13, except for subsection 13.5, which we will cover later. We may begin on chapter 14.

Lecture, October 5

We will cover chapter 14.

Problem session October 10

1. Why is there more than one type of security for hash functions if collision resistance is stronger than the others?

2. Suppose $h : \mathcal{X} \to \mathcal{Y}$ is a hash function, and $|\mathcal{X}| = N$ and $|\mathcal{Y}| = M$. For any $y \in \mathcal{Y}$, let
$$h^{-1}(y) = \{x \mid h(x) = y\}$$
and let $s_y = |h^{-1}(y)|$. Define

$$S = |\{\{x_1, x_2\} \mid h(x_1) = h(x_2)\}|.$$

Note that S counts the number of unordered pairs in $\mathcal{X}$ that collide under h.

(a) Prove that
$$\sum_{y\in\mathcal{Y}} s_y = N,$$

so the mean of the s_y's is

$$\overline{s} = \frac{N}{M}.$$

(b) Prove that
$$S = \sum_{y\in\mathcal{Y}} \binom{s_y}{2} = \frac{1}{2}\sum_{y\in\mathcal{Y}} s_y^2 - \frac{N}{2}.$$

(c) Prove that
$$\sum_{y\in\mathcal{Y}} (s_y - \overline{s})^2 = 2S + N - \frac{N^2}{M}.$$

(d) Using the result proved in part (c), and the fact that the left-hand side in part (c) is not negative, prove that

$$S \geq \frac{1}{2}\left(\frac{N^2}{M} - N\right).$$

Further, show that equality is attained if and only if

$$s_y = \frac{N}{M}$$

for every $y \in \mathcal{Y}$. (Problem 4.1 in CTP.)

3. Suppose that $f : \{0,1\}^m \to \{0,1\}^m$ is a preimage resistant (one-way) bijection. Define $h : \{0,1\}^{2m} \to \{0,1\}^m$ as follows: Given $x \in \{0,1\}^{2m}$, write $x = x'||x''$ where $x', x'' \in \{0,1\}^m$. Then define $h(x) = f(x' \oplus x'')$. Prove that h is not second preimage resistant. (Note that the $\oplus$ is a bitwise XOR.) (Problem 4.6 in CTP.)

4. Suppose that $f_k : \{0,1\}^m \to \{0,1\}^m$ is a family of preimage resistant (one-way) bijections, with keys $k \in \mathcal{K}$. Let $n \geq 2$ be an integer, and define $h_k(x_1, x_2, ..., x_n) = f_k(x_1) \oplus f_k(x_2) \oplus \cdots \oplus f_k(x_n)$. Show that h_k is not collision resistant, and it is not second preimage resistant. Show the lack of collision resistance for the both the security game for weak collision resistance and the security game for collision resistance of families of functions. (From problem 4.12 in CTP.)

2

5. I may lecture at the end.