Advanced Topics in Cryptography – Exercise Set 2

Handed out on May 15, 2013

To be handed in on May 22, 2013

Exercise 1

Prove that the family of all functions from a finite set $\mathcal{X}$ to a finite set $\mathcal{Y}$ (i.e. $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}$) is universal.

Exercise 2

Suppose that $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ is a strongly universal (N, M)-hash family, such that $|\mathcal{K}| = M^2$.

Consider the following modification to a substitution attack: an adversary is now allowed to receive one more authentication tag.

Formally: The adversary chooses $x, x' \in \mathcal{X}$, $x \neq x'$ and receives two valid pairs (x, y), (x', y') — i.e. $y = h_K(x)$, $y' = h_K(x')$, where K is the key chosen by the legitimate parties. The forger must output a valid pair (x_0, y_0), s.t. $x_0 \neq x$, $x_0 \neq x'$.

Show that the success probability of the above attack is equal to 1.
In other words, the adversary can *always* fake the authentication tag, if he learns two valid pairs.

Exercise 3

Let p be an odd prime. For $a, b \in \mathbb{Z}_p$, define a hash family $\mathcal{H}$ as $h_{(a,b)}(x) = (x + a)^2 + b$.

Prove that $\mathcal{H}$ is a strongly universal (p, p)-hash family.

Exercise 4

Let p be a prime, and let $k \in \mathbb{Z}^+$. For $a, b \in \mathbb{Z}_p$, define a hash family $\mathcal{H}$ as $h_{(a,b)}(\vec{x}) = b + \sum_{i=1}^{k} x_i a^i$, where $\vec{x} = (x_1, \ldots, x_k) \in (\mathbb{Z}_p)^k$.

Prove that $\mathcal{H}$ is an ε-almost strongly universal (p^k, p)-hash family with $\varepsilon = \frac{k}{p}$.

It shows that one can construct hash functions with short keys, if strong universality requirement is relaxed to ε-almost strong universality.