University of Pisa

Department computer science

First hands-on: Universal hash family

Domenico Erriquez

1. PROBLEM

Prove that the family H of functions is UNIVERSAL for given $m > 1$ and $p \in [m+1, 2m]$ prime:

$$H = \{h_{ab}(x) = (ax + b) \% p \% m, where\ a \in [1, p-1]\ and\ b \in [0, p-1]\}$$

That is for any $k_1 \neq k_2$ it holds that $|\{h \in H : h(k_1) = h(k_2)\}| = \frac{|H|}{m}$

Hint: consider first

- $r = (a\, k_1 + b)\% p$
- $s = (a\, k_2 + b)\% p$

Where $k_1, k_2 \in [0, p-1]$

2. SOLUTION

H is a universal family hash function if $\forall k_1, k_2 \in U, k_1 \neq k_2: Pr_{h \in H}[h(k_1) = h(k_2)] \leq \frac{1}{m}$ So for any two distinct inputs $k_1, k_2 \in [0, p-1]$, the probability of a random function in H mapping them to the same output is $\frac{1}{m}$.

So, we have a collision when $k_1 \neq k_2$ we have that $h(k_1) = h(k_2)$ which can be written as follows:

$$ak_1 + b \equiv ak_2 + b\ mod\ m\ \ mod\ p$$

$$ak_1 + b\ - ak_2 - b \equiv i * m\ \ mod\ p$$

$$a(k_1 - k_2) \equiv i * m\ \ (mod\ p)$$

Where $i \in [0, \frac{p-1}{m}]$

To solve a we have:

$$\mathrm{a}\ \equiv i * m(k_1 - k_2)^{-1}\ \ (mod\ p)$$

Where $a \in [1, p-1]$, varying i in its range, $i * m(k_1 - k_2)^{-1}$ has $\frac{p-1}{m}$ values not equal to 0. Finally the collision probability is $\frac{\#a\ and\ b\ that\ cause\ a\ collision}{\#all\ possible\ a\ and\ b} = \frac{p\left(\frac{p-1}{m}\right)}{p(p-1)} = \frac{1}{m}$