Cryptography for Computer Scientists 2018/19 Oct 24, 2018

Exercises 4

Stefan Dziembowski MIM UW

Exercise 1: Definitions of hash functions

Let $\{H^s\}_{s\in\{0,1\}^*}$ be a family of hash functions. Prove the following implications

$$\begin{gathered}\{H^s\}_{s\in\{0,1\}^*} \text{ is collision-resistant}\\ \Downarrow\\ \{H^s\}_{s\in\{0,1\}^*} \text{ is second preimage resistant}\\ \Downarrow\\ \{H^s\}_{s\in\{0,1\}^*} \text{ is preimage resistant,}\end{gathered}$$

and give examples that show that the implications in the opposite directions do not hold.

Exercise 2: Birthday paradox

Suppose we choose uniformly at random n elements $(X_1,\ldots,X_n)$ from an m-element set. Let A be the event that all the X_i's are distinct.

1. Prove that
$$\Pr[A] \leq e^{-\frac{n(n-1)}{2m}}.$$
2. Using this fact show a generic attack on any hash function $H:\{0,1\}^*\to\{0,1\}^a$ that finds a collision with in time $O(2^{n/2})$ with probability $1/2$.

(In the class we skipped Point 1, since it was already covered on some other course.)

Exercise 3: Time-memory trade-offs for inverting functions

Let $H:\{0,1\}^n\to\{0,1\}^n$ be a hash function that is a bijection on $\{0,1\}^n$. Show an algorithm for inverting H that runs in time $O(2^{n/2})$ if the following *preprocessing* is allowed: before obtaining x the algorithm gets access to H and fills-in a table of size $O(2^{n/2})$ (assume that his time in this phase is unbounded).

Bonus question: what kind of a similar speed-up one can achieve without the assumption that H is a bijection?

Exercise 4: Combining hash functions

Let $\{H^s\}_{s\in\{0,1\}^*}$ and $\{G^s\}_{s\in\{0,1\}^*}$ be families of hash functions where at least one is collision resistant. For every $s,x\in\{0,1\}^*$ define

$$F^s(x) := H^s(x)||G^s(x).$$

Prove that $\{F^s\}_{s\in\{0,1\}^*}$ is also collision resistant.

Exercise 5: Composing hash functions

Let $\{H^s\}_{s\in\{0,1\}^*}$ be a family of collision resistant hash functions. For every $s, x \in \{0,1\}^*$ define

$$F^s(x) := H^s(H^s(x)).$$

Is $\{F^s\}_{s\in\{0,1\}^*}$ is also collision resistant? If yes, then prove it, if not then show an example.