Last Revised: February 15, 2000

Chapter 5

Hash Function

This chapter is yet to be drafted.

5.1 The Secure Hash Algorithm (SHA-1)

5.2 Hash-Function Families and Collision-Intractability

Definition 5.2.1 Let $H\colon \mathsf{Key} \times \mathsf{Message} \to \mathsf{Hash}$ be a hash-function family, and let A be an adversary. Then

$$\mathbf{Adv}^{\mathrm{cr}}_{H}(A) \quad = \quad \Pr[K \stackrel{R}{\leftarrow} \mathsf{Key};\ (M, M') \stackrel{R}{\leftarrow} A(K) :\ \ M \neq M' \text{ and } H_K(M) = H_K(M')]$$

Let

$$\mathbf{Adv}^{\mathrm{cr}}_{H}(t) \quad = \quad \max_{A}\{\mathbf{Adv}^{\mathrm{cr}}_{H}(A)\}$$

where the maximum is over all adversaries A that run in time at most t.

5.3 The Merkle-Damgård construction

Generalize what went on in SHA-1, and prove.

5.4 Hash Functions from Block Ciphers

Do we want this? Choose a construction and prove it correct in the Shannon model. Make the point that security does not follow from PRF security.

5.5 Weaker Notions of Collision Resistance

Alternatively, these various notions can be made into problems. I think that is my preference.

5.6 Universal Hash-Function Families

Definitions, constructions, and basic results about ϵ-AU2 families. Plenty of possible problems based on this material.

Definition 5.6.1 Let H: $\mathsf{Key} \times \mathsf{Message} \to \mathsf{Hash}$ be a hash-function family and let $\epsilon \geq 0$ be a real number. Then we say that H is **ϵ-Almost universal**, written ϵ-AU, if for all distinct $M, M' \in \mathsf{Message}$,

$$\Pr[K \stackrel{R}{\leftarrow} \mathsf{Key} : \; H_K(M) = H_K(M')] \quad \leq \quad \epsilon \; .$$

5.7 Problems

5.8 History and References