Introduction to Hash Functions

Ira A. Fulton Schools of Engineering
Arizona State University

Objective

Objective

Recognize possible malware by comparing the hashes of software packages

Cryptographic Hash Function

Pre-image resistance

- Given a hash value h it should be difficult Second pre-image resistance

Second pre-image resistance

- Given an input m_1, it should be difficult to find a difficult to find a different input m_2 such that hash(m_1)=hash(m_2)

Collision resistance

- It should be difficult to find two different inputs m_1 and m_2 such that hash(m_1)=hash(m_2)