Paul Diaz
CS 166 Homework 4
Chapter 5

5. Suppose that h is a secure hash that generates an *n*-bit hash value.

   a. **The expected number must be $2^{\frac{n}{2}}$ hashes.**
   b. **The expected number that must be computed to find 10 collisions is $\sqrt{10} * 2^{\frac{n}{2}}$. Collisions are expected for each $2^{\frac{n}{2}}$ comparison; since the expected number of hashes result about 10* 2^{n} comparisons.**
   c. **The expected number of hashes to find m collisions must be about $\sqrt{m} * 2^{\frac{n}{2}}$. Since all hashes can be compared to all of the previous hashes, it will continuously easier to find collisions as more hashes are calculated.**

22. Key diversification = K_s - Sally generate and stores a single key.
    Then she generates a key $K_A = h(Alice, K_s)$ and so on…

    Here, Alice is using key diversification as an alternative approach, where it uses some sort of master key (K_s) to generate the other symmetric keys as needed. Some of the advantages are, a) almost no storage is needed for the generation of symmetric keys, b) if one of the symmetric keys is compromised (any K_{A-B}), the damage is limited to that one key, not the whole system. This is because attacker still doesn't know the master key. On the contrary, the disadvantages are: a) if the master key is compromised, then all keys are compromised b) attacker may access and compromise the database as well, since he/she accessed master key.

27. M = ("Alice", Alice's public key) and $[h(M)]_{CA}$
    CA = certification authority

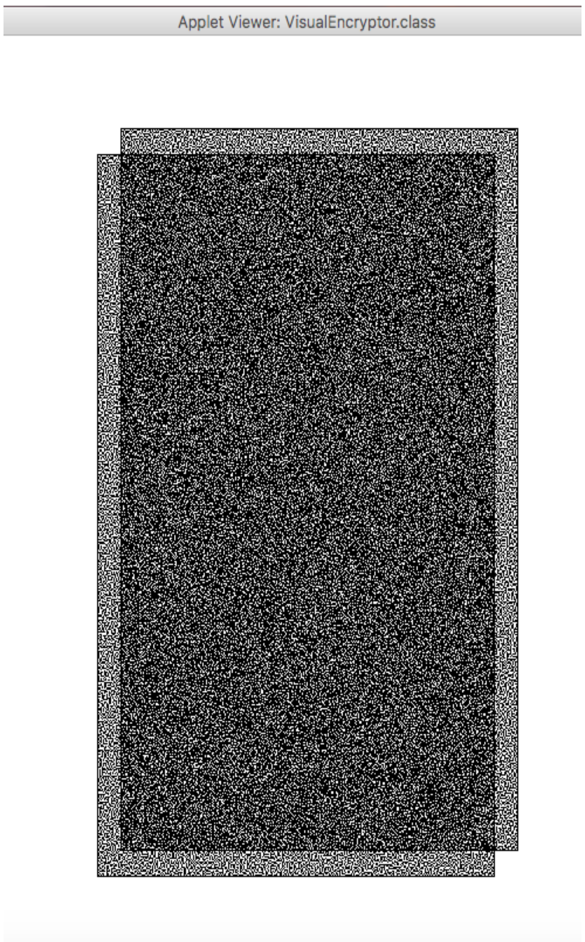
   a. **To verify the signature, receiver has to compute $\{S\}_{CA}$ and verify that it matches M, which is ("Alice", Alice's public key) and $[h(M)]_{CA}$.**
   b. **Well, the private key could be anybody's key. For instance, an attacker could simply create public and private keys, publish public key and use private key to sign a certificate that "guarantees" that this attacker is Alice; in this scenario, the attacker keeps the private key. Now, the bad thing about this scenario is that when when try to send a message and encrypt it, we can end up using the attacker's public key (that pretends to be Alice). Consequently, the attacker could decrypt the message we sent, not the real Alice.**
   c. **Overall, the main responsibility of certificate authority is to make sure that Alice's private key is to keep it private and not compromised, such that only she possesses and accesses it. Subsequently, if we trust the certificate authority that signed it, and confirmed that the private key used to sign the certificate authority**

is from “Alice,” then we can assume that certificate authority did what it’s suppose to do; to not compromise Alice’s private key and only she possesses and accesses it.

d. We don’t know nothing about it.

35.

a. Image of Alice.



B. Using a black and white leaf photo

Original