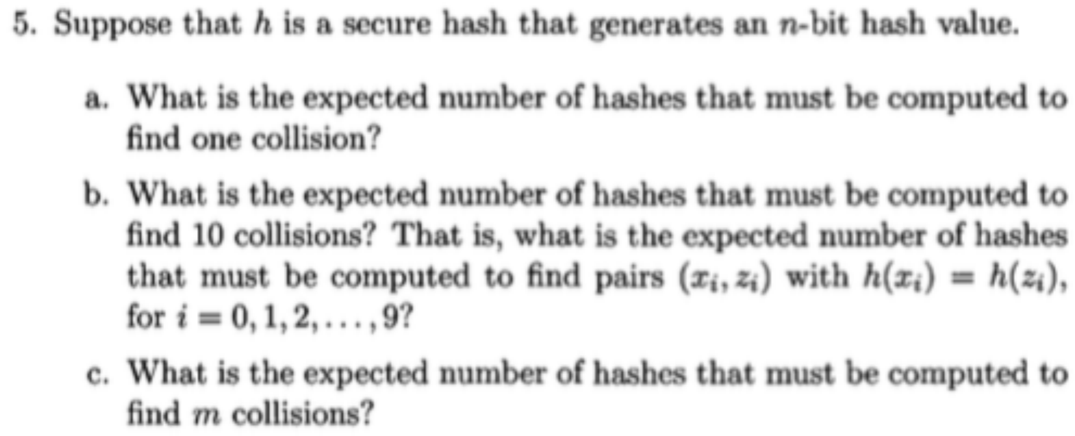
Chapter 5

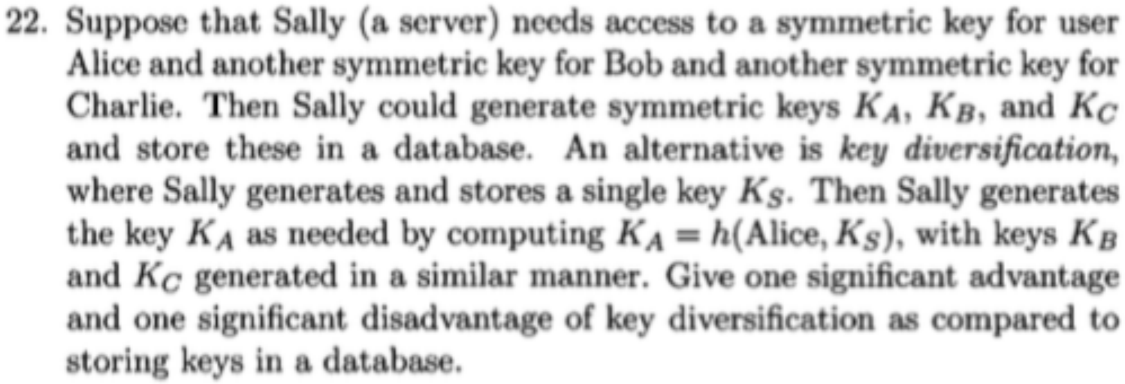


5. Suppose that h is a secure hash that generates an n-bit hash value.

   a. What is the expected number of hashes that must be computed to find one collision?

   b. What is the expected number of hashes that must be computed to find 10 collisions? That is, what is the expected number of hashes that must be computed to find pairs (x_i, z_i) with $h(x_i) = h(z_i)$, for $i = 0, 1, 2, \ldots, 9$?

   c. What is the expected number of hashes that must be computed to find m collisions?



22. Suppose that Sally (a server) needs access to a symmetric key for user Alice and another symmetric key for Bob and another symmetric key for Charlie. Then Sally could generate symmetric keys K_A, K_B, and K_C and store these in a database. An alternative is *key diversification*, where Sally generates and stores a single key K_S. Then Sally generates the key K_A as needed by computing $K_A = h(\text{Alice}, K_S)$, with keys K_B and K_C generated in a similar manner. Give one significant advantage and one significant disadvantage of key diversification as compared to storing keys in a database.

27. Suppose that you receive an email from someone claiming to be Alice, and the email includes a digital certificate that contains

$$M = (\text{"Alice"}, \text{Alice's public key}) \text{ and } [h(M)]_{\text{CA}},$$

where CA is a certificate authority.

   a. How do you verify the signature? Be precise.

   b. Why do you need to bother to verify the signature?

   c. Suppose that you trust the CA who signed the certificate. Then, after verifying the signature, you will assume that only Alice possesses the private key that corresponds to the public key contained in the certificate. Assuming that Alice's private key has not been compromised, why is this a valid assumption?

   d. Assuming that you trust the CA who signed the certificate, after verifying the signature, what do you know about the identity of the sender of the certificate?

35. Obtain the file `visual.zip` from the textbook website and extract the files.

   a. Open the file `visual.html` in your favorite browser and carefully overlay the two shares. What image do you see?

   b. Use the program with a different image file to create shares. Note that the image must be a gif file. Give a screen snapshot showing the original image, the shares, and the overlaid shares.