CS458-HW4

Due Date: Monday, 2 December 2024 - 11:59 pm

1. In this problem, you are to experiment with SHA-256 by writing programs that gather statistics. In addition to answering some relevant questions about the distribution of SHA-256 digests, you will gain experience using a real cryptographic library in your code. You can code this in any language you want. Submit your programs for 2 parts a and b, and include the output or results in your written solution.

(a) Write a program that computes and prints the SHA-256 hash value of your name. The output should be printed in hexadecimal.

(b) Write a program that computes hashes of many different inputs, and counts how many 1-bits are in the output for each hash value. The output for this problem should be a histogram of the number of times each bit count occurred. I don't care how you generate the different inputs — they can be random, or you can make a big binary counter — just make sure your inputs are all different (at least with high probability). You can either write code to output a histogram from your program, or you can output the counts and use Excel or some other program that can create the histogram. Your program should be able to run in a reasonable amount of time.

(c) Time your program, report both the overall time and number of hashes and then report the time as the number of hashes computed per second. How long would it take to compute 2^{128} hash values (the number needed for a birthday attack against weak collision resistance)? How long would it take to compute 2^{256} hash values (the number needed for a brute-force attack on strong collision resistance)?

(d) If the output hash values were completely random, then each of the 256 output bits would be one with probability ½. Therefore, the distribution of bit counts would be a binomial distribution, and so the probability of an output having 128 bits set to one would be Binomial[256,128] / 2^{256} . What is this probability? (Hint: Use Mathematica — the format of the formula in the preceding sentence is a valid Mathematica formula.) What is the probability of having just 100 bits set to one?

2. We have an RSA public-key cryptosystem with Bob's public key: (N=143, e=7) and Alice's public key: (N=39, e=5). Show your work in detail completely

Bob wants to sign a message (M = 3), then encrypt it and send it to Alice.
Explain the whole process and calculations, and find all the numbers, such as:

Bob's task:

a. Sign a message and calculate the signature value
b. Encrypt signature value and send it to Alice

Alice's task:

c. Decrypt the received encrypted signature
d. Verify the signature and signer identity