Introduction to Cryptography, 2021 Fall

Homework 5, due 4pm, 12/20/2021 (Monday)

Part 1: Written Problems

1. Let the hash function be H(M) = the last 6 bits of sha256(M) for a message M. Then, the last 6 bits are treated as a binary number for computing signature, such as, 100011 (binary) is 35 (decimal). To hash a decimal number x, we treat it as the ASCII string. For example, x=47 is treated as the ASCII string "47" or 3437 (Hex). For each of the following methods of specified parameters, sign "Hello!" with random k=13 (if needed), compute the verification key, and verify correctness of the signature.
   Note: You must provide reasonably detailed computation steps, not just the answers.
   a) RSA: n=493=17x29, private key = (493, 369)
   b) ElGamal: q=113, α=17, private key = (113, 17, 37)
   c) Schnorr: p=293, q=73, a=53, private key = (293, 73, 53, 29)
   d) DSA: p=293, q=73, g=53, private key = (293, 73, 53, 61)

Part 2: Mini report

1. Write a mini report about certificates. The report consists of the following three parts:
   a. **Definition and creation of a certificate for digital signature**
   b. **Find a real certificate of digital signature and explain the fields of the certificate**
   c. Find an application for certificates and explain how certificates are used for security functions in the application
2. The report should be at least 3 pages long with 1.5 line spacing, 12-point font and moderate page margin, like the format of this homework sheet.
3. Submit your report in file cert.pdf to the course website (E3) by the due date.