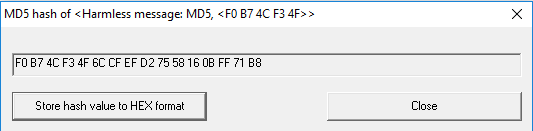
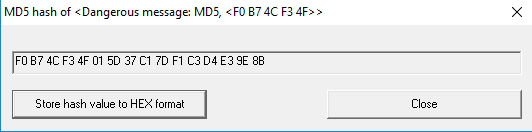
Matthew Austin

Cryptology

Anwar

November 2018

Digital Signatures

* 1. Given an RSA signature scheme with the public key (n = 9797,e = 131), which of the following signatures are valid?
  + A. Let w = 123 be the message and sig(w) = 6292 its signature. Because 6292131 mod 9797 = 123 the signature is valid.
  + B. Let w = 4333 be the message and sig(w) = 4768 its signature. Because 4768131 mod 9797 = 9644 the signature is not valid.
  + C. Let w = 4333 be the message and sig(w) = 1424 its signature. Because 1424131 mod 9797 = 4333 the signature is valid.
* 2.
  + G. The first 5 and last spot of the hashes are similar to each other, the rest in between is different.
    - 
    - 
  + H. I could not, because by the time it would be completed I would be dead.
  + I. If I had more hardware resources, I would be able to successfully attempt a mathematical attack.