**Cryptool lab – Unit 3**

First, download and install Cryptool from the website at <http://cryptool.com>

* If using a windows PC, installed crytool1
* If using a MAC PC, install jcryptool

Part1.1

a. Identify the digital signature schemes and MAC schemes that are supported by Cryptool. For each scheme, determine the key sizes supported by Cryptool and which key sizes are recommended by NIST.

b. Encrypt text using two digital signature schemes, measure the execution time for key generation (if applicable), signature generation, and signature verification. Measurements should be performed multiple times and then the analysis should use the average time for comparisons. In order to obtain measurable results, you will likely need to use long messages (i.e. 5 MB or larger). A sample document is available under Doc Sharing if student is unable to find a suitable document to use.

c. Record results and draw conclusions. Identify the encryption algorithm used. Discuss the results of the measurements and any variations or trends observed when comparing the results from the group members. Report the results and the analysis. Be sure to include details on the measured results and details on each member’s computer (i.e., processor type, speed, cache size, RAM size, OS, etc.).

Part 1.2

1. Using CRYPTOOL generate a MD5 hash for a small plaintext document
2. Record the hash result (cut and paste)
3. Change one character in the plaintext and regenerate a hash on the changed text.
4. Record the hash (cut and paste into your report)
5. Do you think you could find a hash collision? (that is, can you find two different texts that produce the same hash? Experiment a few times and draw a conclusion about whether this can be done easily.)

Part 1.3

1. Generate a large prime (at least 20 digits long) and a short prime (less than 10 digits in length) (HINT Individual Procedures \ RSA Cryptosystem \ Generate prime numbers)
2. Determine which factorization algorithms are implemented within Cryptool (Indiv. Procedures -> RSA Demonstration -> Factorization of a Number).
3. Identify the characteristic features of these algorithms by reading the “Factorization algorithms” help within the tutorials section of Cryptool’s built in help.
4. Try to factor the primes using some of these methods
5. Report your results, identifying the methods you used. Be sure to include how long the factorization took (or how long it was estimated to take if it did not complete in a reasonable time)
6. Now, just enter numeric values to be factored (again one long number and one short one)
7. What are the results? Were factors found? Are you good at guessing prime numbers?