Lab Cryptool No. 2

1. Use Cryptool to generate hash codes (MD2, MD5 etc.) from different documents.
2. Cryptool includes a hash demonstration. Run and understand this demonstration.
3. Cryptool includes an "attack on the hash value of the digital signature" Run and understand this attack.
4. Use Cryptool to:
5. Generate a set of RSA keys. Encrypt a document with RSA. Decrypt the document with RSA.
6. Export your certificate to another student in the class, and import his certificate. Then send and receive RSA encrypted messages to each other and decrypt them. – notice Cryptool can only export certificates including the private key -
7. Cryptool includes a demonstration of RSA encryption/decryption. Run and understand this demonstration.
8. Cryptool includes a demonstration of Diffie Hellmann . Run and understand the demonstration.
9. In most security protocols a asymmetric algorithm is used to distribute a session key, which is then used to a symmetric algorithm to encrypt all the data transmitted.

   Cryptool include a demonstration of this procedure "Hybrid Demonstration" Run and understand this demonstration.

10. Use Cryptool to sign a message and to verify the signature.
11. Send a signed message to another student in the Class and receive a signed message from him. Verify the signatures.