COMPUTER SUBJECT:	ENCRYPTION/DECRYPTION
TYPE:	GROUP WORK EXERCISE/DISCUSSION
IDENTIFICATION:	CRYPTOOL No 2/MC
COPYRIGHT:	*Michael Claudius and Homayoon Fayes*
LEVEL:	EASY
DURATION:	30 min
SIZE:	10 lines!! Answering a few questions
OBJECTIVE:	Introduction to public encryption and hashing
REQUIREMENTS:	Exercise CrypTool No. 1

IDENTIFICATION: CRYPTOOL No 2/MC

Mission
You are to get a general understanding of the basic asymmetric encryption/ decryption and hashing.

Purpose
The purpose of this assignment is to utilize Cryptool to get insight of the algorithms: RSA, SHA512, MD5. Cryptool is very comprehensive SW-Tool with both visualizations and simulation of many algorithms); and we just look into a few of them.

The following assignments can be solved in groups (1-2 persons).

Useful links http://www.cryptool.org

1. If not done already: Download and install Cryptool from http://www.cryptool.org/ Choose the new stable version 2.1.
   Start the tool

2. You are to encrypt and decrypt a message with a asymmetric encryption algorithm for example RSA

3. Key generation
   Use the template RSA Key Generator to generate a public key(n,e) and a private key (n,d).
   Discuss n= pxq

4. Use RSA Encryption to encrypt a document/text with RSA.
   Decrypt the encrypted document with RSA.
   Maybe take a look at RSA Chiper.

5. Encrypt a short text message with the RSA encryption algorithm, and e-mail the encrypted text to one of the other students in this course. Supply her/him with the necessary information to decrypt it.

6. Cryptool includes a visualization of RSA Signed QR code encryption/decryption.
   Run and understand this visualization.

7. Use Cryptool Blind Signature with RSA to sign a text and to verify the signature.

8. Use Cryptool to generate hash codes (SHA512, MD2, MD5 etc.) from different documents/texts.

9. Run the HMAC template.

10. Cryptool includes an "attack on the hash value of the digital signature".
    Run and understand this attack.

------------------------------------ NOT TO BE DONE ----------------------------

11. Cryptool includes a hash visualization. Run and understand this demonstration.

12. In most security protocols an 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.

13. Send a signed message to another student in the Class and receive a signed message from him. Verify the signatures.

14. Cryptool includes a demonstration of Diffie Hellmann.
    Run and understand the demonstration.
    Well I would say I got more confused when I look at this diagram. Skip it!!