# Course Title: Information Systems Security (11464)

**Assignment # 2**

Cut-off date: **November 20, 2021**

## Table of Contents



## Table of Figures

## Question:

The aim of this question is to provide you with a hands-on practice on some of the cryptographic primitives that you have seen in the cryptography course. In particular, the symmetric, asymmetric and hybrid encryption algorithms. In order to do so, you will be using a teaching cryptographic tool named Cryptool.

CrypTool – as introduced by its developers - is a "comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations". In order to complete this question, you need to install CrypTool-1[1] on your personal computer/notebook. You can download it from the Cryptool-1 download page [2].

(a) A hybrid cryptosystem is a combination of symmetric and asymmetric system designed to solve the limitations of each type of cryptosystem while combining their advantages. In this exercise, you will be using a hybrid cryptosystem consisting of the combination of AES (symmetric) and RSA (asymmetric) cryptosystems.

1- Run Cryptool
2- Prepare plaintext file
    a. Create a text file (.txt) that will serve as a file to encrypt using the hybrid cryptosystem from the menu bar, click on the menu file and select new to create file and may can use any text editor for this purpose. This file should include your first/last name and your student ID in the first line and any other text of your choice. Save this file as "plaintext-xxxx.txt" (xxxx should be replaced with your student ID, for instance if the student ID is 430112211, the file name will be plaintext-430112211.txt).
3- Generate RSA key pair:
    a. From the menu bar, click on the menu item: Digital Signatures/PKI -> PKI -> Generate/Import Keys, and follow the steps to generate RSA Key pairs (1048 bits). Use your last and first name as identifiers and use **1234** as a PIN code. (You should explain the role of this PIN code in your answer)
4- Export key pairs
    a. After generating the keys, click on "Show Key Pairs" Button and from the next window, Select the key you have generated in step 3 and click on export "PSE (PKCS#12)". Again use **1234** as the PIN code. (You should explain why there are two PIN codes in your answer).
    b. Save the file as "privatekeys-xxxx.p12" (xxxx should be replaced with your student ID, for instance if the student ID is 430112211, the file name will be privatekeys - 430112211.p12).
5- Hybrid cryptosystem: encryption process
    a. Open the plaintext file you have created in step 1. Then, click on the following menu Item: Encrypt/Decrypt -> Hybrid -> RSA-AES encryption. This will show you the

[1] As you will notice on the Cryptool website, there is another version called Cryptool-2. Cryptool-2 is a more advanced cryptographic tool but some of the functions that will be used in this question are not straightforward in Cryptool-2. Students working on "non-windows" OS can use the JCrypt which can be run on different platforms. All these software (among others) are available at [1].

process of the hybrid encryption (Figure 2).

b. **Using your own words**, explain how a hybrid key cryptosystem works.

c. Encrypt the plaintext file using the hybrid RSA-AES cryptosystem. During this process, you will use the public key that you have generated in 3. Explain each step of the process. Screenshots should highlight the progress of the encryption process and the output of each step (session key, Asymmetric keys, encrypted document, encrypted session key, and final output). You should explain each of the outputs.

d. Save the encrypted file as "ciphertext-xxxx.txt" (xxxx should be replaced with your student ID, for instance if the student ID is 430112211, the file name will be ciphertext - 430112211.txt).

6- Hybrid cryptosystem: Decryption process

a. Open the ciphertext file you have created in step 5.d. Then, click on the following menu Item: Encrypt/Decrypt -> Hybrid -> RSA-AES decryption, and follow process of the hybrid encryption (Figure 2). Explain each step of the process (screenshot for each step with explanation).

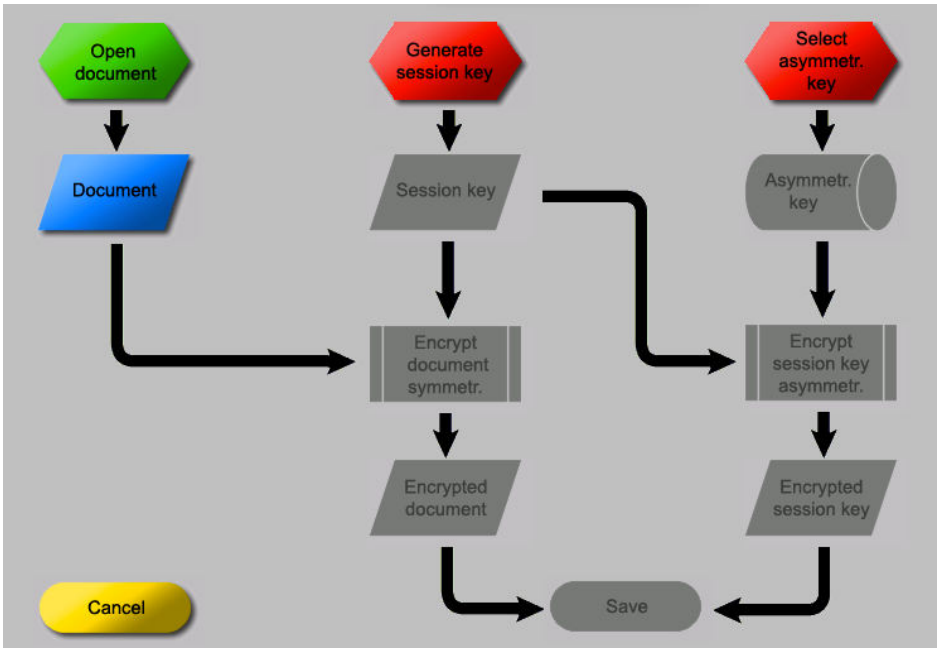


**Figure 1. Hybrid Cryptosystem - Encryption process**

(b) Generate keys and a digital signature for data using the private key and to export the public key and the signature to files. Verify a digital signature by importing a public key and a signature that is alleged to be the signature of a specified data file and to verify the authenticity of the signature. Using the following algorithms:

1. RSA digital signature: Sign the file and verify signature, Select the key you have generated in step 3. Modify the message and then verify the authenticity of the signature.
2. DSA: Sign the file and verify signature. Modify the message and then verify the authenticity of the signature.

**Note:** Screenshots should highlight the progress of the encryption and decryption processes and the output of each step.

**References**


[1] Cryptool project website, URL: http://www.cryptool.org, Last accessed on Nov 10, 2021

[2] Cryptool-1 download page, URL: http://www.cryptool.org/en/ct1-download-en, Last accessed on Nov 10, 2021.