Assignment 2

Secure Programming, 2016

Elias Athanasopoulos - Sanjay Rawat

i.a.athanasopoulos@vu.nl - s.rawat@vu.nl

Question 1

— Alice, born in 1992, did not take any security class while studying at the University. Bob managed to compromise the database of two web services Alice uses and got the credentials from two of her accounts. However, Bob could not use the credentials, without further processing the information. Can you help Bob to figure out the password Alice uses in the web? Here is what Bob has obtained, so far:

```
f19140c8cafc55a60464d939554ef027a46ea9cbe32a0e58bef43296e5f57574
8100333bbf2d99565cf387158491667ab4ae8712874ee3d636ace23757d6392f
```

Question 2

— Assumming $p = 5$ and $q = 13$ calculate a private and a public key based on the RSA algorithm. Discuss each step.

Question 3

— Implement a document signing utility based on assymetric encryption and cryptographic hash functions. The tool should take as input a file and an RSA key pair. The tool should generate the hash key of the contents of the file and then encrypt it using RSA. The outcome (i.e., the signature) should be appended to the original document. In addition, you should implement a client that verifies the signature of a document. Discuss your design decissions, which cryptographic hash funtion you used, and how the RSA keys (public and private) are used in the tool and the client.

Question 4

— Write a program that compares the contents of two files using cryptographic hash functions. The files should be divided in several blocks and each block should be hashed

using a cryptographic hash function. Your tool should process the number of desired blocks per file. For example, if the number of blocks is 1 then the function should just hash the entire contents of the file, if the number of blocks is 2, then the file should be divided into two blocks, and two hash values will be produced. The final comparison of the files will be evaluated by checking how many hash values of the first file match the hash values of the second one.