Assignment 1

Secure Programming, 2016

Elias Athanasopoulos - Sanjay Rawat

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

Question 1

— Which requirement is violated when a third-party passively monitors unencrypted network packets exchanged between two hosts?

(a) Confidentiality (b) Integrity (c) Availability (d) Non-repudiation

— Which requirement is violated when a third-party modifies network packets exchanged between two hosts?

(a) Confidentiality (b) Integrity (c) Availability (d) Non-repudiation

— Alice downloaded a Twitter client and once she installed it in her smartphone, the application asked her Twitter credentials to access her Twitter feed. Which requirements are affected?

(a) Confidentiality/Authentication (b) Availability/Authentication
(c) Integrity/Authorization (d) Authentication/Authorization

— Describe a methodology which allows two parties to exchange messages through a protocol that ensures the integrity of the communication.

Question 2

— Alice sent the following encrypted message to Bob. Can you decipher it?

```
dtucluclmlcuy xqlyqccmsqlqzobi dqplgudtlmlcuy xqlobi d!sbm tuolmxs!budty
```

— Bob replied with the following encrypted message, but using a different algorithm. Can you decipher it?

```
xqm drwieiwrqypndvi wjkndnrlvftaimddmaliewdrqyvxznhig!ayxxk!eylrgieukxvrxqq
```

Question 3

— Implement the Playfair cipher in a language you are most familiar with. The program should take as an input a key and a file and operate in two modes: (a) encryption, and (b) decryption.

Question 4

— Implement a file vault based on AES encryption in a language you are most familiar with. The file vault should support arbitrary files. The user should be able to add files to the vault and retrieve files from the vault. Each file should be placed in the vault encrypted using AES, and should be retrieved and decrypted upon user request.