Application Security

Exercise Set 1

In order to solve the following problems all technologies are allowed.

1. Read about the Parkerian Hexad and shortly explain every constituent.
   [1p]

2. Implement encryption using the symmetric and the asymmetric cryptography. Conduct performance tests with checking different options (e.g. key lengths, block sizes, etc.) in the encryption configuration and prepare a short report.
   [2p]

3. Consider at least 3 different hash functions and prepare a summary of performance tests results. Additionally include any "slow" function (e.g. PBKDF2) and check the difference.
   [2p]

4. Check what capabilities are offered by your favourite technology (e.g. Django, RoR, Spring) to protect the secret key (in the symmetric encryption) and the private key (in the public key encryption). Is this the same way or are there any differences?
   [2p]

5. Create and implement a scenario of the digital signature using a cryptography API.
   [2p]

6. Let assume there are 4 components with the uptime guaranteed on 99.9%. Calculate what is the uptime of the solution in the worst case? What uptime is required for every component to achieve 99.9% uptime for the whole solution? Propose changes in the solution if we can't guarantee the required uptime for all components.
   [1p]

Paweł Rajba