Information Systems Security

Exercise Set 1

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

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

2. 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]

3. 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]

4. Implement a common scenario of the digital signature and message authentication code using a cryptography API.
   [2p]

5. Let assume there are 4 components with an uptime guaranteed on 99.9%. Calculate what is the uptime of the solution based on those 4 components in the worst case? What uptime is required for every component to achieve 99.9% uptime for the whole solution? What can we do if one of the components can’t support the required uptime?
   [2p]

Paweł Rajba