Application Security

Exercise Set 1

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

1. Consider 3 symmetric encryption algorithms and make performance tests. Both encryption and decryption should be included in test results.
   [1p]

2. Consider at least 5 different hash functions and prepare a summary of performance tests results. Additionally include any "slow" function (e.g. PBKDF2) and check a difference.
   [2p]

3. In the example *AsymmetricEncryptionDecryption* make the following changes:

   - Replace *AnotherStore* with *YetAnotherStore*.
   - Add *Flags = CspProviderFlags.UseUserProtectedKey* parameter.

   Find an explanation for the observed behavior[1]
   [2p]

4. DPAPI. Prepare a scenario in which a difference between using a user-level and machine-level key container can be observed[2].
   [1p]

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

6. Create and implement a scenario of key exchange using cryptography API.
   [2p]

Paweł Rajba

[1] In other than .NET technologies, rewrite an example and explain asymmetric encryption including key pair generation. Find a solution for securing private key.

[2] In other than .NET technologies, find a way of secure storing symmetric key.