A small Test / repetition

Talk and discuss with your neighbour following questions

DNS:

- What is the primary purpose of DNS?
- Any secondary purposes?
- How is the information in the logical names structured?
- Describe the three top layers in the logical name structure.
- Why do we not just all switch to IPv6?

Security -- concepts:

- What are the four different goals for security?
- What does each (sub) goal mean?

- For symmetric encryption / decryption, how many key(s) do you have?
- Which goal does symmetric key(s) fulfil?
- For symmetric keys what are the typical length of a key?
- For symmetric keys, name at least two algorithms.
- What are the major problem using symmetric keys

- For asymmetric encryption / decryption, how many key(s) do you have?
- Which goal do asymmetric keys fulfil?
- For asymmetric keys what are the typical length of a key?
- For asymmetric keys, name at least one algorithm.
- What are the major problem using asymmetric keys?

- What is message digest? In addition, a digital signature?
- What is PGP? In addition, how does it make use of encryption/decryption?
- What is SSL? In addition, how does it make use of encryption/decryption?
- When do you use PGP? In addition, when SSL?

- Describe the most important C#-classes in a **client** for SSL programming.
- Describe the most important C#-classes in a **server** for SSL programming