Examples of exam questions connected to the cryptography lectures

Comments to help you understand the context of some problem texts (e.g. whether you should still be able to answer them or not on the IntroSec course) are marked with square brackets - [ ])

2010-11-27

Problem 2

Imagine that a person intends to implement their own symmetric encryption algorithm in order to keep large amounts of data safe on a hard drive. To ensure that the decryption and encryption processes are quick and effective she has decided to keep to a fairly simple substitutional method. The security and practicality of this method will to a significant degree be dependent on certain qualities of the keys that are used. Suggest and motivate what such qualities can be.

2011-08-25

Problem 4

Describe each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *description*, *relationship to [your chosen related concept]*, and *example.*

Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

- Rootkit
- Sandbox
- Bell LaPadula
- **Caesar Cipher**

2011-06-10

Problem 4

Describe each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *description*, *relationship to [your chosen related concept]*, and *example.*

Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

- **Substitutional cipher**
- Capability based access control

- Certificate Revocation List [N.B. This concept was made clear in earlier course books. Pfleeger does not, so it is unlikely that this concept will make it into the IntroSec course material]
- Mix network (also referred to as *Mixed networks*, *Mix nets* and *Digital mixes*, and as is utilized in the *mixmaster remailer*).

2009-10-20

Problem 2

Having knowledge of which language is used in a clear text can assist a cryptanalyst in deciphering the corresponding ciphertext. This is true whether the cipher is based on substitutional or on transpositional methods (or a mixture of both). Explain in outline (i.e. you need not go deeply into cryptanalytical techniques) how.

2010-08-18

Problem 2

For a time during the 1990s many security experts claimed that cryptography would be the answer to building secure system. Suggest and explain reasons why cryptography has so far proven not to be a complete security solution.

2008-10-22

Problem 2

The concept of keyspace for a cryptographic algorithm is similar to that of the space of all possible passwords that an authentication method allows.

a) Identify and motivate a factor (or factors) that effects the strength of keys and of passwords which are similar for both of these concepts.

b) Identify and explain a factor (or factors) of the space of all possible passwords that can make the authentication method weak, and that you would not normally expect to see occurring in the keyspace for a cryptographic algorithm.

Problem 3

Describe each of the following IT security related terms. Also, clearly relate each of your descriptions to a closely connected IT security concept of your own choosing, and give an example of an application of these tools/threats/concepts:

- **Steganography**
- Risk Analysis
- Formal Verification
- Common Criteria