Institut for Matematik og Datalogi — March 8, 2004
Syddansk Universitet — JFB

Computer Security – F04 – Lecture 6

Repeat announcement

The deadline for discussing your project topic with me is March 19. Please make an appointment to discuss it.

Lecture, March 4

We finished chapter 3.

Lecture, March 11

We will cover the sections on authentication in chapter 4.

Lecture, March 18

We will finish chapter 4, combining it with section 5.4.

Discussion section: March 16

The last three problems are taken from Gollmann's textbook, *Computer Security*.

1. Read and be prepared to discuss the article at
   http://www.advisor.com/Articles.nsf/AID.KNIGE01
2. Do problem 22 on page 227.
3. Assume that you are only allowed to use the 26 letters from the English alphabet to construct passwords. How many distinct passwords are there if there is no difference between upper and lower case letters

passwords have length 4? Length 6? Length 8? What if the passwords are case sensitive?

4. For the above problem, how long will a brute force attack take on average if it takes one tenth of a second to check a password? What if it takes a microsecond?

5. If you are using the same password on two systems, one where passwords are case sensitive and one where they are not, how would a password cracker find your password on the system where they are case sensitive?