Institut for Matematik og Datalogi
Syddansk Universitet

May 24, 2004
JFB

Computer Security – F04 – Lectures 14 and 15

Lecture, May 13

We finished chapter 7, covered section 8.1 and began on section 8.2.

Lectures, May 25 and 27

We will cover chapters 8 and 10. Some of the misleading statements in chapter 10 are as follows:

- Page 632, characteristic 2 – although this holds for the Satisfiability and Knapsack, it is not the case for all NP-Complete problems that the number of cases to be considered is 2^n, though it does always seem to be at least exponential in the worst case.
- Page 633 – P is usually defined as the class of decision problems (problems with "yes"/"no" answers) which can be solved in polynomial time. In order to make it a subset of NP, you have to define it this way so "sorting" is not a problem in P.
- Page 636 – Another reason why NP-Complete problems are not necessarily perfect for cryptography is that NP-Complete problems are often easy to solve on most instances. We just know there exist instances which are hard to solve if P≠NP. It is also not obvious how to build the trapdoor into most NP-Complete problems.
- Page 641 – For any $0 < a < p$, $a^{p-1} \pmod{p} = 1$. Note that it does not hold for $a = 0$.
- Pages 679–680 – The argument that encryption followed by decryption gives the original plaintext is not quite right. If done their way, they should mention the Chinese Remainder Theorem to be the result modulo n by combining the results modulo p and modulo q. But one can do

without that: $(P^e)^d \pmod{n} \equiv P^{e*d} \pmod{n} \equiv P^{k*\phi(n)+1} \pmod{n} \equiv (P^{\phi(n)})^k * P \pmod{n} \equiv 1^k * P \pmod{n} \equiv P$.

- Page 681 – It says “If a number is suspected to be a prime and passes both of these tests, the likelihood that it is a prime is at least 1/2.” A correct statement is, “If a number p is composite, the probability that this test will fail is at least 1/2. The probability that this test will fail k times (on k randomly chosen values) on a composite is at most $1/2^k$.”