Institut for Matematik og Datalogi
Syddansk Universitet

February 17, 2004
JFB

Computer Security – F04 – Lecture 3

Lecture, February 12

We covered up through section 2.7 in the textbook.

Lecture, February 19

We will finish with chapters 2.

Lecture, February 26

We will begin on chapter 3.

Discussion section: February 24

Be prepared to discuss the following exercises from, mostly taken from Gollmann's textbook *Computer Security*.

1. Is the following statement correct? "Cryptographic protocols are intended to let agents communicate securely over an insecure network.
2. Why is the following statement correct? "Cryptography needs physical security".
3. Given a modular exponentiation algorithm for n-bit integers that needs $O(n^3)$ bit operations, how much does the performance of RSA deteriorate by moving from 512-bit numbers to 1024 bits?
4. When a document is too long to be processed directly by a digital signature algorithm, a hash of the document is computed and then signed. Which properties do you require from this hash function to prevent an attacker from forging signatures? Consider an attacker who

only knows some pairs of messages and signatures on them by user A versus an attacker who can choose messages that user A will sign. Consider whether you want to allow *existential forgeries*, where the attacker would be happy to sign any message, even one it had no control over. What is the difference between this and allowing *selective forgeries*, where the attacker wants to able to sign at least one of a certain set of messages?

5. When using RSA to sign messages, what is necessary to prevent an attacker from creating an existential forgery?

6. Given that for n bit numbers, the current best factoring algorithms take time $e^{O(\log^{1/3}(n)\cdot\log\log^{2/3}(n))}$, what effect on security do you get by doubling the number of bits in an RSA modulus?