Institut for Matematik og Datalogi — November 12, 2010
Syddansk Universitet — JFB

# Introduction to Computer Science
# E10 – Lecture 14

## Lecture, November 11, 14:15–16, U71

We covered RSA and its implementation, plus digital signatures using RSA.

## Lecture, November 15, 8:15–10, U37

We will finish chapter 12.

## Lecture, November 22, 8:15–10, U37

We will cover sections 6.6 and 6.7 of chapter 6.

## Discussion sections: November 22 and 29, 14:15–16, Terminal Room

Discuss the following problems in groups of two or three. Note that two labs (four hourse) are allocated to this.

1. Design three hash functions and program them in Java (or Maple).
2. Test your hash functions. Create an array of length $m+1$ which will count how many random large integers are hashed to each of the distinct values between zero and $m$. Look at the results for some relatively small values of $m$ (for example, $m = 4, 8, 12, 20, 50, 100$).
3. With at least four different values of $m$ and some different length large strings (integers) which are hashed, check how many values you need to hash before you get a collision. Does it behave as one would predict with the Birthday Paradox?

4. With at least four different values of $m$ and some different length large strings, check how even your distribution is? What is the difference between the largest number of strings hashing to any particular value and the smallest number? How does this seem to depend on the number of strings you hash?

5. With your hash functions, how would you find collisions (two strings that hash to the same value) when $m$ is very large (say $2^{80}$)? Are your hash functions cryptographically secure?