

Stefan Dziembowski, semestr zimowy 2003/2004.

# Teoria Protokołów Kryptograficznych

## 1 Cel zajęć

Celem zajęć jest zapoznanie studentów z najnowszymi tematami badawczymi w kryptografii. Spora część omawianych technik nie jest jeszcze stosowana komercyjnie (co nie znaczy, że nie będzie zastosowana w przyszłości). Poznanie tych technik da słuchaczom podstawy do zrozumienia prac publikowanych w specjalistycznych periodykach, będzie dobrym punktem wyjścia do prowadzenia własnych prac badawczych i pozwoli na zrozumienie podstaw działania niektórych rozwiązań przemysłowych.

Program zajęć obejmuje takie zagadnienia jak: dowody interakcyjne, dowody z wiedzą zerową, schematy identyfikacji, obliczenia wielopodmiotowe, protokoły głosowania elektronicznego, protokoły prywatnego pozyskiwania danych oraz protokoły elektronicznej gotówki.

Na zajęciach *nie* będziemy zajmować się konkretnymi standardami przemysłowymi metodami zabezpieczeń komputerów w sieci. Nie będziemy zagłębiać się w zagadnienia związane z szyfrowaniem (były one szeroko omawiane na wykładzie *Wstęp do Kryptografii Stosowanej* z zeszłym roku).

## 2 Zasady zaliczania

Student ma do zdobycia na wykładzie 100 punktów. Zalicza 60. Dokładniejsza skala zostanie ustalona później. Punkty można zdobywać następująco

- przez bycie *skrybą* (patrz Rozdział 2.1) — 40 p. za jeden raz
- przez robienie zadań domowych
- przez zdanie egzaminu — maks. 100 p.

Ćwiczenia będą polegały na rozwiązywaniu zadań lub będą dalszym ciągiem wykładu.

### 2.1 Skryba

Zadanie skryby polega na sporządzeniu w systemie L<sup>A</sup>T<sub>E</sub>X notatek z wykładu oraz z wyznaczonej części ćwiczeń (na podstawie literatury udostępnionej przez wykładowcę, własnych notatek oraz L<sup>A</sup>T<sub>E</sub>Xowego brudnopisu wykładowcy). Notatki należy wysłać email'em do wykładowcy do końca niedzieli następującej po wykładzie. Wykładowca postara się jak najszybciej opublikować te notatki na stronie internetowej wykładu (po ewentualnych poprawkach).