

# Ochrona i poufność danych

Maciej Nikodem

4.10.2010

# Ochrona i poufność danych

- dr inż. Maciej Nikodem, 223/C3 (220/C3),
- www: [www.zak.ict.pwr.wroc.pl/nikodem](http://www.zak.ict.pwr.wroc.pl/nikodem)
- e-mail: [maciej.nikodem@pwr.wroc.pl](mailto:maciej.nikodem@pwr.wroc.pl)
- konsultacje: pn.11-13, śr.15-17
- wykład (pn.7:30-9:00, 20/C3) + projekt (pn.9:15-11:00, 223/C3)

# Kontakt

- maciej.nikodem@pwr.wroc.pl,
- **tylko** z poczty w domenie PWR.WROC.PL,
- w tytule **koniecznie** wpisywać **[OiPD]**,

# Literatura

- 1 A.Menezes, P.van Oorschot, S.Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996 - wersja elektroniczna:  
<http://www.cacr.math.uwaterloo.ca/hac/>
- 2 M.Kutyłowski, Willy-B. Strothmann, *Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych*, Oficyna Wydawnicza ReadMe 1999  
<http://wwwcs.uni-paderborn.de/fachbereich/AG/agmadh/WWW/german/LehreKuty/kryptografia/>
- 3 B.Schneier, *Kryptografia dla praktyków*, WNT 1995
- 4 D.Elizabeth, R.Denning, *Kryptografia i ochrona danych*, WNT 1993

# Zasady zaliczenia

## Wykład i projekt

- obecność na zajęciach — max. 1 nieusprawiedliwiona nieobecność,
- projekt – grupy 2-3 osobowe
- wykład – ocena z kolokwium na koniec semestru,
- ocena końcowa — 50% ocena z wykładu, 50% ocena z projektu,
- ocena 5.5 — artykuł na konferencję dotyczącą kryptografii.

# Plan wykładów

- 4.X Zajęcia organizacyjne
- 11.X Wprowadzenie i historia kryptografii
- 18.X
- 25.X
- 8.XI
- 15.XI
- 22.XI
- 29.XI
- 6.XII
- 13.XII
- 20.XII
- 3.I
- 10.I
- 17.I kolokwium
- 24.I wpisy/poprawka

# Dwie grupy projektów

- "lokalne",
- NSN Innovative,

# Projekty w ramach NSN Innovative

- Hardware wiruses - investigates feasibility of malicious digital designs (viruses) which could be incorporated into genuine designs. The project outcome should include: possible implementations, digital design obfuscation techniques, security risk analysis
- Design analyser for hardware viruses detection - this project implements the tool for detecting malicious digital circuits within medium/large VLSI designs, based on design netlist analysis. The project outcome should include: implementation of the design netlist (EDIF) parser and number of design pattern detection algorithms supporting detection of digital circuits.

# Projekty w ramach NSN Innovative

- Radio-on-Chip - this proof-of-concept project implements pair of radio transceivers which communicate inside the VLSI chip (e.g. FPGA) using only simple radio interface.
- Transceiver for temperature-channel communication - this proof-of-concept project implements pair of transceivers which communicate inside the VLSI chip (e.g. FPGA) using only chip temperature as the communication channel.
- Transceiver for clock-line-based communication - this project investigates the feasibility of inter-module communication using the global clock-tree inside a VLSI chip (e.g. FPGA)

# Tematy projektów

- Secure-JTAG - bezpieczne testowanie układów kryptograficznych.
- Zagrożenia bezpieczeństwa bezstykowych kart płatniczych.
- Personalizowana reklama wykorzystująca karty bezstykowe.
- Analiza bezpieczeństwa rozkazów specjalnych AES w procesorze i5.
- Komunikator internetowy wykorzystujący kanał podprogowy.
- Implementacja ataku różnicowego/liniowego z wizualizacją kolejnych kroków (tutorial).

# Przebieg projektu

- do **11.X** ostateczny wybór tematu projektu
- do **18.X** plan prac w ramach projektu:
  - etapy max. 2-tygodniowe => 5-6 etapów,
  - zadania i zakres prac na każdy etap,
  - efekty na koniec każdego etapu,
  - pierwsze 1-2 etapy dotyczą analizy teoretycznej problemu i proponowanych rozwiązań,
- dokumentowanie i spotkania:
  - raporty częściowe na koniec każdego etapu (w wersji elektronicznej),
  - po przesłaniu raportu - spotkania omawiające każdy etap,
  - raport końcowy do **17.I.2011**,