

# Ochrona i poufność danych

Maciej Nikodem

2.10.2009

# Ochrona baz 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 (pt.11:15-13, 20/C3) + projekt (pt.13:15-15, 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 - digital version:  
<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 osobowe
- wykład – ocena z kolokwium na koniec semestru,
- ocena końcowa — 60% ocena z wykładu, 40% ocena z projektu,
- ocena 5.5 — dla każdego z oceną końcową  $\geq 4.0$ , kto przygotuje artykuł na konferencję podejmującą tematykę kryptografii.

# Plan wykładów

9.X Podstawy kryptografii

16.X

23.X

30.X

6.XI

13.XI

20.XI

27.XI

4.XII

11.XII

18.XII

8.I

15.I kolokwium

# Tematy projektów

- **Implementacja arytmetyki dużych liczb i wybranych algorytmów kryptografii symetrycznej i asymetrycznej.**
- Ataki z uszkodzeniami na algorytmy kryptograficzne w krzywych eliptycznych (ECC) i propozycje rozwiązań ochronnych.
- **Podpis cyfrowy zgodny z ustawą i realizowany z wykorzystaniem kryptograficznych kart mikroprocesorowych.**
- **Algorytmy dystrybucji, uzgadniania i wymiany kluczy kryptograficznych dla bezprzewodowych sieci czujników.**
- Pay-TV vs. Broadcast Encryption.
- Rootkity w bazach danych i metody ich wykrywania.
- Projekt i proof-of-concept systemu programowania układów FPGA zapewniającego bezpieczeństwo.
- Projekt i implementacja wieloosobowej i uczciwej gry w sieci P2P bez centralnego, zaufanego serwera.

# Projekty **sprzętowe**

- karty  $\mu$ P, układy Mica2/IRIS,
- laboratorium 24/D6,
- dostęp od listopada,

# Przebieg projektu

- do **9.X** ostateczny wybór tematu projektu
- do **23.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,
- dokumentowanie i spotkania:
  - raporty częściowe na koniec każdego etapu,
  - po przesłaniu raportu - spotkania omawiające każdy etap,
  - raport końcowy do **15.I.2010**,

# Tematy projektów w WCSS

- Budowa OCSP (Online Status Certificate Protocol) agregującego dane z wielu ośrodków certyfikacyjnych (CA).
- Zastosowanie OpenXPKI do utworzenia elementów Infrastruktury Klucza Publicznego.
- Zastosowanie OpenSSL do utworzenia elementów Infrastruktury Klucza Publicznego.
- Budowa ośrodka znakowania czasem dokumentów elektronicznych.

# Uwagi organizacyjne

- grupy dwuosobowe
- projekty realizowane w większej grupie projektowej (osoby spoza grup zajęciowych)
- każdy projekt będzie polegał na zainstalowaniu, skonfigurowaniu, dostosowaniu oprogramowania (momentami, napisaniu własnych elementów oprogramowania). Następnie odbędą się testy funkcjonalne rozwiązania.
- bieżące tworzenie dokumentacji projektowej, dokumentacja użytkowa na koniec
- szczegółowy zakres zadań zostanie określony indywidualnie