DEPARTMENT OF APPLIED INFORMATICS AND INFORMATION TECHNOLOGY

http://www.elf.stuba.sk/Katedry/KAIVT

Head of Department
prof. RNDr. Otokar Grošek, PhD. Tel: ++421-2-602 91 226
e-mail: otokar.grosek@stuba.sk Fax: ++421-2-654 20 415

I. STAFF

Professor	prof. RNDr. Otokar Grošek, PhD.
Associate Professors	doc. RNDr. Jaroslav Fogel, PhD., doc. RNDr. Gabriel Juhás, PhD. doc. RNDr. Karol Nemoga, PhD., doc. RNDr. Frank Schindler, PhD.
Assistant Professors	Ing. Tomáš Delikát, PhD., Ing. Alexander Hambalík, PhD., Ing. Milan Vojvoda, PhD.
Research Workers	Ing. Martin Babinec, Ing. Fedor Lehocki
Technical Staff	Zuzana Šabíková (secretary)
PhD. Students	Ing. MSc. Martin Horňanský, Mgr. Dušan Lacika, Ing.Vladislav Novák, Mgr. Marek Sýs, Mgr. Zuzana Ševčíková, Ing. Pavol Zajac

II. EQUIPMENT

II. 1 Teaching and Research Laboratories

- Laboratory of Security Technologies
- DIEDC - Database Information Education and Demonstration Center
- Laboratory of System Programming

II. 2 Special Measuring Instruments and Computers

- HP Proliant ML 150
- 2x CPU INTEL XEON 2,8 GHz
- RAM 12 GB
- HDD 35 GB
- MSDN Academic Alliance (MSDN AA) = Microsoft Developers Network Academic Alliance

III. TEACHING

III.1 Undergraduate Study (Bc.)

Subject, semester, hours per week for seminars or practical exercises, name of lecturer:

Algorithms and Programming	(1st sem., 3-2 h)	F. Schindler
Algorithms and Programming	(1st sem., 3-2 h)	M. Vojvoda
Algorithms and Programming	(1st sem., 3-2 h)	G. Juhás
Analysis and Complexity of Algorithms	(3rd sem., 3-2 h)	M. Vojvoda
Analysis and Complexity of Algorithms	(5th sem., 3-1 h)	M. Vojvoda

Bases of Real-time Systems	(3rd sem., 3-2 h)	J. Fogel
Classical Ciphers	(4th sem., 2-2 h)	O. Grošek
Cryptography	(5th sem., 2-2 h)	O. Grošek
Database Systems	(3rd sem., 3-2 h)	T. Delikat
Fast algorithms	(1st sem., 2-2 h)	K. Nemoga
Information Security	(5th sem., 3-1 h)	J. Šiška
Operating Systems	(3rd sem., 3-2 h)	J. Fogel
Programming Techniques	(2nd sem., 3-2 h)	F. Schindler
Public Key Infrastructure	(6th sem., 3-1 h)	J. Šiška

III.2 Graduate Study (Ing.)

Design of Block Ciphers	(3rd sem., 2-3 h)	O. Grošek
Formal Methods	(3rd sem., 3-1 h)	J. Fogel
Object-Oriented Programming	(1st sem., 3-2 h)	F. Schindler
Network Security	(1st sem., 3-2 h)	K. Nemoga
Security of Mobile Communications	(1st sem., 3-2 h)	M. Vojvoda
System Programming	(2nd sem., 3-2 h)	J. Fogel

III.3 Undergraduate and Graduate Study for Foreign Students (in English Language)

Basics of RT Systems	(3rd sem., 1 h consul.)	J. Fogel

III.4 Distance Study

Algorithms and Programming	(1st sem., 4x2 h consul.)	A. Hambalík
Basics of RT Systems	(3rd sem., 4x2 h consul.)	J. Fogel

IV. RESEARCH PROJECTS

- Modelling and Control of Distributed Processes Based on the Multi-agent Systems. G2/4148/04, J.Fogel
- Design and Security of Cryptographics Applications. 2006-2008, O. Grošek
- Development and innovation of subjects for Study program of Applied Informatics fulfilling modern demands of e-learning. ESF-JPD 3-038/2005 O. Grošek
- Project about the Improvement of Students Preparation in Bachelor and Engineering Studies for Their Future Profession . ESF-JPD 3-1-004/2004, A. Hambalík.
- Application of modern ICT in rehabilitation process of long-term ill children.. F. Lehocki
- Application of biosensors, biomaterials and biosignals in medicine. F. Lehocki
- Number Theory and its Applications. G 2/4138/24, K. Nemoga
- Working Group for Gas Dynamics. ESF – JPD 3 2005/1312020003701, K. Nemoga
- ACUMED – innovative development program of modern study materials for medical high schools. ESF SORO/JPD3 2005/3-043, F. Lehocki

V. COOPERATION

V.1 Cooperation in Slovakia

- Mathematical Institute, Slovak Academy of Sciences, Bratislava
- National Security Authority, Bratislava
- Micronic, LTD, Košice
- Data Security Consulting, LTD, Liptovský Mikuláš
- SWH – Siemens, Bratislava
- Institute of Forensic Science of Police Corps, Bratislava
- Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava
- Association of the Infovek Project, Ministry of Education of the Slovak Republic – Project of Informatization of Regional School – PIRŠ
- Slovak Research and Development Agency, Bratislava
- Faculty of Chemical and Food Technology, STU, Bratislava
- Technical University, Zvolen
- J. Selye University, Komárno

V.2 International Cooperation

- Institute of Informatics, Academy of Sciences of the Czech Republic, Prague, CzR
- University of LA LAGUNA, Department of Statistics, Operations Research and Computing, Tenerife, Spain
- Department of Information Systems Security, Concordia University College of Alberta, Canada
- Faculty of Informatics MU Brno, CzR
- Lehrstuhl fuer Angewandte Informatik, Katholische Universitaet Eichstaett-Ingolstadt, Germany
- Fachgruppe Simulation und Modellierung, Institut fuer Systems Engineering, Universitaett Hannover, Germany
- Florida Atlantic University, Boca Raton, Florida, USA
- Department of Mathematics, University of Washington, Washington, USA
- Institute for Experimental Mathematics, University of Essen, Germany
- Department of Mathematics, FEL ČVUT Praha , CzR
- Department of Mathematics and Science, Indiana State University, USA

V.3 Membership in International Organizations and Societies

- AMS – American Mathematical Society (O.Grošek)
- SIAM – Society for Industrial and Applied Mathematics (O.Grošek)
- IEEE Computer Society (F.Schindler)
- IEEE Computer Society (J.Fogel)
- Union of Czech Mathematicians and Physicists (F.Schindler)
- Slovak Society for Cybernetics and Informatics (F. Schindler)
- Slovak Society for Informatics (F. Schindler)
- Union of Slovak Mathematicians and Physicists (F. Schindler)
- The European Association for the Transfer of Technologies, Innovation and Industrial Information (F. Lehocki)
- Membership in Editorial Boards of International Journals
  - -Tatra Mountains Mathematical Publications, O. Grošek
  - Tatra Mountains Mathematical Publications, K. Nemoga – managing editor
  - Zentralblath Math, K. Nemoga, managing editor of Slovak Unit
  - Atlantic Journal of Mathematical Cryptology, O. Grošek

V.4 Contracts

- O. Grošek: Advanced course in Cryptology. Contract with National Security Authority of SR.

VI. THESES

VI.1 Masters Theses

[1] L. Klenovič: Fast correlation attack using convolutional codes on stream ciphers. (M. Vojvoda)

VI.2 Doctoral Theses

[1] M. Šrámka: **:** Cryptanalysis of selected Public-key and Private-key Cryptosystems. (O.Grošek)

VII. OTHER ACTIVITIES

- Seminar Crypto (O. Grošek)
- Reviewer of Mathematical Reviews and for Zentralblatt für Mathematik (O.Grošek)

VIII. PUBLICATIONS

VIII.1 Journals

VIII.2 Conferences

VIII.3 Parts of Books