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., Mgr. Zuzana Ševčíková, Ing. Milan Vojvoda, PhD. (Deputy Head of Dept.)
Research Workers	Ing. Fedor Lehocki
Technical Staff	Zuzana Šabíková (secretary)
PhD. Students	Ing. Ondrej Gallo,Ing. MSc. Martin Horňanský, Ing. Matúš Jókay Mgr. Dušan Lacika, Ing. Stanislav Marček, Mgr. Michal Mikuš, Ing.Vladislav Novák, Mgr. Marek Sýs, 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
- Laboratory of Medical Informatics

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 lectures and for seminars or practical exercises, name of the 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	(5th sem., 3-1 h)	M. Vojvoda
Basic of Real-time Systems	(3rd sem., 3-2 h)	J. Fogel
Basic of Real-time Systems	(4th sem., 3-2 h)	J. Fogel
Classical Ciphers	(4th sem., 2-2 h)	O. Grošek
Database Systems	(3rd sem., 3-2 h)	T. Delikat
Operating Systems	(3rd sem., 3-2 h)	J. Fogel
Programming Techniques	(2nd sem., 3-2 h)	F. Schindler
Design of Database Systems	(4th sem., 3-1 h)	T. Delikat
Information Security	(5th sem., 3-1 h)	J. Šiška
Public Key Infrastructure	(6th sem., 3-1 h)	J. Šiška
Cryptography	(5th sem., 2-2 h)	O. Grošek
Fast Algorithms	(6th sem., 2-2 h)	K. Nemoga

III.2 Graduate Study (Ing.)

Security of Mobile Communications	(1st sem., 3-2 h)	M. Vojvoda
System Programming	(2nd sem., 3-2 h)	J. Fogel
Design of Block Ciphers	(3rd sem., 2-3 h)	O. Grošek
Object-Oriented Programming	(1st sem., 3-2 h)	F. Schindler
Ciphering in Computer Networks	(1st sem., 3-2 h)	K. Nemoga
Modelling and Simulations of Event Systems	(1st sem., 3-1 h)	G. Juhás
Security of Information Systems in Practice	(1st sem., 3-1 h)	O. Grošek

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

Algorithms and Programming	(1st sem., 3-2 h consul.)	M.Vojvoda
Introduction to Engineering and Technical Documentation	(1st sem., 2-2 h consul.)	P.Zajac Z. Ševčíková

III.4 Distance Study

Algorithms and Programming	(2st sem., 3x2 h consul.)	T. Delikat
Algorithms and Programming	(1st sem., 4x2 h consul.)	A. Hambalík

IV. RESEARCH PROJECTS

- Design and Security of Cryptographics Applications. VEGA 1/3115/06, 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
- Modelling and Control of Distributed Processes Based on the Multi-agent Systems. G2/4148/04, J.Fogel
- MEDITECH – Modern Biomedical Technologies, ESF SORO/JPD-26/2005, F. Lehocki
- ERASMUS Educational Project, Bilateral Agreement, University of La Laguna, Spain, O. Grošek
- ACUMED – innovative development program of modern study materials for medical high schools. ESF SORO/JPD3 2005/3-043, F. Lehocki
- Application of biosensors, biomaterials and biosignals in medicine. F. Lehocki
- Application of modern ICT in rehabilitation process of long-term ill children.. F. Lehocki
- Scenario based approaches for misbehaviour detection in ad hoc wireless networks (SAMANET), DAAD 7/2006, G. Juhás
- Digital Štúr Generation, Open School, Ministry of Transport and Posts No. 114, A. Hambalík
- Development and Integration of Nonlinear Systém Methods, VEGA 1/3089/06, M. Huba, F. Schindler
- Dominant Determinants of Engineering Padagogy and Its task After Slovak Entering into EU, VEGA 1/2531/05, D. Driensky, A. Hambalík
- Improvement of Students Preparation in Bachelor and Engineering Studies for Their Future Profession . ESF-JPD 3-1-004/2004, A. Hambalík.
- Number Theory and its Applications. G 2/4138/24, K. Nemoga
- Working Group for Gas Dynamics. ESF – JPD 3 2005/1312020003701, K. Nemoga
- Use of IKT in Teaching – Functional Literacy of Pedagogical Employees in Information Technologies, ESF-JPD 3, Priority 2, Step 2.1, Code 13120120283, A. Hambalík
- Stimulation and Improvement of Education for Employer Needs – Increase of Competetiveness of High Schools in Self-governing Bratislava region via Development of Human Resources , ESF-JPD 3, Priority 2, Step 2.1, Code 13120120149, A. Hambalík

V. COOPERATION

V.1 Cooperation in Slovakia

- Mathematical Institute, Slovak Academy of Sciences, Bratislava
- National Security Authority, Bratislava
- Micronic, Ltd. Košice
- 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
- Technical University, Zvolen
- J. Selye University, Komárno
- Bratislava Metodical and Pedagogical Centre
- Trenčín Metodical and Pedagogical Centre
- Virtual Academy of Bratislava Self-governing region
- University of Constantin the Philosopher, Nitra
- Department of Engineering Pedagogy and Psychology, MtF STU Trnava
- Ministry of Finance of the SR

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
- Department of Computer Sciences de Montfort University, Milton Keynes, UK
- Department of Mathematics, Faculty of Electrical Engineering, ČVUT Prague
- 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, Tacoma, Washington, USA
- Institute for Experimental Mathematics, University of Essen, Germany
- Department of Mathematics and Science, Indiana State University, USA
- DELTA Elektronik Limited, Budapest, Hungary
- Fundatia Sapientia–Universitatea Sapientia, Facultătile din Miercurea Ciuc, Roumania
- AINTEK A.E, Greece
- Virginia Tech, Blacksburg, Virginia, USA (prof, Sandeep K. Shukla)
- McMaster University, Hamilton, Canada (prof. Ryzsard Janicki)
- University of Waterloo, Canada (prof. Jo Atlee)
- University of Toronto, Canada (prof. Eric Hehner)
- Universität Ausgsburg, Germany (prof. Robert Lorenz)
- Eszterházy Föiskola, Eger, Hungary

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
- Transactions on Petri Nets and Other Models of Concurrency, G. Juhás

VI. THESES

none

VII. OTHER ACTIVITIES

- Seminar Crypto (O. Grošek)
- Reviewer of Mathematical Reviews and for ZentralblattMath (O.Grošek)
- Reviewer of ZentralblattMath (O. Grošek, K. Nemoga)

VIII. PUBLICATIONS

VIII.1 Journals

[1] DELIKÁT, T.: Basic Directions in Design of Present Database Systems. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 13, Special Issue (2007), p. 281-288. (in Slovak)

[2] GROŠEK, O., ZAJAC, P.: Efficient Selection of the AES-Class MixColumns Parameters. In: WSEAS Transactions on Information Science and Applications. - ISSN 1790-0832. - Vol. 4, Iss. 4 (2007), p. 663-668. (in English)

[3] LACIKA, D.: Recursive Construction for Longest Induced Cycles in Unitary Circulant Graphs. In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 58, No. 7/s (2007), p. 83-85. (in English)

[4] LEHOCKÁ, A., JUHÁS, G., LEHOCKI, F., ŠEVČÍKOVÁ, Z.: Petri Nets in Designing of Workflow Processes. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 13, Special Issue (2007), p. 303-305. (in Slovak)

[5] LEHOCKI, F.: Knowledge Propagation in Logical and Fuzzy Petri Nets. In: Petri Net Newsletter. - ISSN 0931-1084. - Vol. 73, October (2007), p. 26-37. (in English)

[6] LEHOCKI, F., JUHÁS, G., ŠEVČÍKOVÁ, Z., LEHOCKÁ, A.: Applications of Petri Nets in Medical Diagnostic Systems. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 13, Special Issue (2007), p. 299-302. (in Slovak)

[7] JUHÁS, G., LORENZ, R.D., MAUSER, S.: Complete Process Semantics for Inhibitor Nets. In: Lecture Notes in Computer Science. - ISSN 0302-9743. - Vol. 4546: Petri Nets and Other Models of Concurrency - ICATPN 2007 (2007), p. 184-203. (in English)

[8] NOVÁK, V., SCHINDLER, F.: Interpolation by Means of Arc-Length Parametrized B-Splines. In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 58, No. 7/s (2007), p. 72-75. (in English)

[9] SÝS, M.: Isotopy Classes of Latin Squares. In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 58, No. 7/s (2007), p. 97-99. (in English)

[10] ŠEVČÍKOVÁ, Z., JUHÁS, G., LEHOCKÁ, A., LEHOCKI, F.: Semantics and Applications of Petri Nets. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 13, Special Issue (2007), p. 306-308. (in Slovak)

[11] ZAJAC, P.: Smoothness Probability in Degree Six Number Fields. In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 58, No. 7/s (2007), p. 14-16. (in English)

VIII.2 Conference Proceedings

[1] GROŠEK, O.: On the Relation among Computer Science, Cryptology and Mathematics. In: 39th Slovak National Conference in Mathematics. Jasná pod Chopkom, Slovak Republic, 22.-25.11.2007. - Žilina: JSMF pri SAV, 2007. - ISBN 978-80-8070-772-9. - p. 16. (in Slovak)

[2] HAMBALÍK, A.: New Information and Communication Technologies in Preparing of Engineers. In: XX. DIDMATTECH 2007: International Conference. Olomouc, Czech Republic, 20.-21.6.2007. - Olomouc: Votobia, 2007. - ISBN 80-7220-296-0. - p. 444-447. (in Slovak)

[3] HAMBALÍK, A.: New Requirements of Practice and Preparation of Teachers of Special Technical Courses. In: XX. DIDMATTECH 2007: International Conference. Olomouc, Czech Republic, 20.-21.6.2007. - Olomouc: Votobia, 2007. - ISBN 80-7220-296-0. - p. 305-307. (in Slovak)

[4] JUHÁS, G., LEHOCKI, F., LORENZ, R.D.: Semantics of Petri Nets: A Comparison. In: Proceedings of the 2007 Winter Simulation Conference: Washington, USA, 9.-12.12.2007. - Piscataway: IEEE, 2007. - ISBN 1-4244-1306-0. - CD-Rom. (in English)

[5] LORENZ, R.D., MAUSER, S., JUHÁS, G.: How to Synthesize Nets from Languages - A Survey. In: Proceedings of the 2007 Winter Simulation Conference: Washington, USA, 9.-12.12.2007. - Piscataway: IEEE, 2007. - ISBN 1-4244-1306-0. - CD-Rom. (in English)

[6] NÉMETHOVÁ, Z., GROŠEK, O., BABINEC, M.: Slovak Large Statistical Program for Dactyloscopy. In: 8th International Symposium on Forensic Sciences: Šamorín-Čilistov, Slovak Republic, 26.-29.9.2007. - Bratislava: KEUPZ, 2007. - p. 12-13. (in English)

[7] NOVÁK, V., SCHINDLER, F.: Interopolation by Means of Arc-Length Parametrized B-Splines. In: ISCAM 2007: International Conference in Applied Mathematics for Undergraduate and Graduate Students. Bratislava, Slovak Republic, 20.-21.4.2007. - Bratislava: STU, 2007. - p. 29. (in English)

[8] SCHINDLER, F.: Importance of Communication in Online Distance Education over the Internet. In: ICETA 2007: 5th International Conference on Emerging e-Learning Technologies and Applications. Stará Lesná, Slovak Republic, 6.-8.9.2007. - Košice: Elfa, 2007. - ISBN 978-80-8086-061-5. - p. 73-76. (in English)

[9] SÝS, M.: Isotopy Classes of Latin Squares. In: ISCAM 2007: International Conference in Applied Mathematics for Undergraduate and Graduate Students. Bratislava, Slovak Republic, 20.-21.4.2007. - Bratislava: STU, 2007. - p. 38. (in English)

[10] VOJVODA, M., SÝS, M., JÓKAY, M.: A Note on Algebraic Properties of Quasigroups in Edon80. In: SASC 2007. The State of the Art of Stream Ciphers: Workshop. Bochum, Germany, 31.1.-1.2.2007. - Bochum: ECRYPT Network of Excelence in Cryptology, 2007. - p. 307-315. (in English)

[11] VOJVODA, M., JÓKAY, M.: Distributed System for File Decryption. In: 8th International Symposium on Forensic Sciences: Šamorín-Čilistov, Slovak Republic, 26.-29.9.2007. - Bratislava: KEUPZ, 2007. - p. 13. (in English)

[12] ZAJAC, P.: Generalized Line Sieve Algorithm. In: ELITECH ´07. 9th Conference for PhD Students of Electrical Engineering and Information Technology: Bratislava, Slovak Republic, 16.5.2007. - Bratislava: STU, 2007. - ISBN 978-80-227-2655-9. - CD-Rom. (in English)

[13] ZAJAC, P.: How to Solve XTR-DL Using NFS. In: Santa's Crypto Get-Together 2007. Prague, Czech Republic, 6.-7.12.2007. - Prague: Trusted Network Solutions, 2007. - ISBN 80-903083-8-4. - p. 91-97. (in English)

[14] ZAJAC, P.: Remarks on Polynomial Selection for the NFS. In: ISCAM 2007: International Conference in Applied Mathematics for Undergraduate and Graduate Students. Abstracts. Bratislava, Slovak Republic, 20.-21.4.2007. - Bratislava: STU, 2007. - p. 45. (in English)

[15] ZAJAC, P.: Remarks on Using NFS to Solve DLP in XTR Supergroup. In: Tatracrypt 2007: Smolenice, Slovak Republic, 22.-24.6.2007. – Bratislava: SAV, 2007. - p. 44. (in English)

VIII.3 Textbook

[1] GROŠEK, O., VOJVODA, M., ZAJAC, P.: Classical Ciphers. - Bratislava: STU, 2007. - 214 p. - ISBN 978-80-227-2653-5. (in Slovak)