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. Dr. Ing. Miloš Oravec, Doc. RNDr. Frank Schindler, PhD.
Assistant Professors	Ing. Štefan Balogh, Ing. Alexander Hambalík, PhD., Mgr. Marek Sýs, PhD., Mgr. Zuzana Ševčíková, Ing. Milan Vojvoda, PhD. (Deputy Head of Dept.) Ing. Pavol Zajac, PhD.
Research Workers	Ing. Fedor Lehocki
Technical Staff	Zuzana Šabíková (secretary) Brigita Timková
PhD. Students	Ing. Lukáš Adamko, Ing. Michal Braško, Ing. Ondrej Gallo, Ing. Matúš Jókay, Ing. Stanislav Marček, Ing. Ján Mazanec, Mgr. Michal Mikuš, Ing.Vladislav Novák, Ing. Ľuboš Omelina, Ing. Filip Pilka, Ing. Štefan Počarovský, Ing. Martin Riesz, Ing. Milan Zelina

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
- Laboratory of Operating Systems and Communication Protocols

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)	P. Zajac
Algorithms and Programming	(1st sem., 3-2 h)	M. Sýs
Algorithms and Programming	(1st sem., 3-2 h)	I. Kossaczký
Analysis and Complexity of Algorithms	(5th sem., 3-1 h)	M. Vojvoda
Classical Ciphers	(4th sem., 2-2 h)	O. Grošek
Database Systems	(3rd sem., 3-2 h)	M. Vojvoda
Operating Systems	(3rd sem., 3-2 h)	J. Fogel
Programming Techniques	(2nd sem., 3-2 h)	F. Schindler
Designing of Database Systems	(4th sem., 3-1 h)	G. Juhás
Information Security	(5th sem., 2-2 h)	E. Kostrecová
Computer Crimes	(6th sem., 2-2 h)	E. Kostrecová
Public Key Infrastructure	(6th sem., 2-2 h)	J. Šiška
Introduction to Cryptography	(5th sem., 2-2 h)	O. Grošek
Fast Algorithms	(6th sem., 2-2 h)	K. Nemoga
Communication Protocols	(6th sem., 4-1 h)	A. Hambalík
Introduction to Computer Science	(3rd sem., 3-2 h)	O. Grošek
Communication and Information Networks	(2nd sem., 3-1 h)	M. Oravec
Software Application Development	(3rd sem., 2-2 h)	G. Juhás
Software Architecture	(5th sem., 2-2 h)	G. Juhás

III.2 Graduate Study (Ing.)

Object-Oriented Programming	(1st sem., 3-2 h)	V. Novák
Ciphers in Communication Networks	(1st sem., 3-2 h)	K. Nemoga
Modelling and Simulations of Event Systems	(1st sem., 3-2 h)	G. Juhás
Practice of Security of Information Systems	(1st +3rd sem., 3-2 h)	M. Zanechal
Formal methods	(1st sem., 3-2 h)	J. Fogel
Cryptanalysis	(1st sem., 3-2 h)	M. Vojvoda, M. Sýs, P. Zajac
Analysis of Event Systems	(1st sem., 3-2 h)	G. Juhás
Neural Networks for Signal Processing	(3rd sem., 3-2 h)	M. Oravec
System Programming	(2nd, 4th sem., 3-2h)	J. Fogel
Design of Ciphers	(3rd sem., 3-2 h)	P. Zajac

Machine Learirng and Neural Networks	(1st sem., 3-2h)	M. Oravec

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

Algorithms and Programming	(1st sem., 12 h consul.)	M. Sýs
Introduction to Engineering and Technical Documentation	(1st sem., 6 h consul.)	Z. Ševčíková
Databases Systems	(3rd sem., 12 h consul.)	Š. Balogh

III.4 Distance Study

Algorithms and Programming	(1st sem., 6x2 h consul.)	A. Hambalík

IV. RESEARCH PROJECTS

- 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
- ERASMUS Educational Project, Bilateral Agreement, University of La Laguna, Spain, O. Grošek
- Technology transfer in the area of workflow process analysis, grant APVV-0618-07 G. Juhás
- Synthesis of Petri nets from nonsequential scenarios, VEGA 1/0872/08, G. Juhás
- Development of Norwegian –Slovak cooperation in Cryptology, NIL Fund Supporting Cooperation in the Field of Education NIL-I-004, 07.07.2008 – 30.09.2010, O. Grošek
- Solution of Current Problems in Cryptology, VEGA 1/0244/09, O. Grošek
- Recognition of Human Face Images as the Part of Biometric Methods for Increasing the Security of Open Society, VEGA 1/3117/06, M. Oravec
- Modernization of Education Process in Basic and Grammar Schools., ITMS: 26110130083, 26140130013 and ITMS: 26110130084, 26140130084, certified lector in the project: A. Hambalík

V. COOPERATION

V.1 Cooperation in Slovakia

- Mathematical Institute, Slovak Academy of Sciences, Bratislava
- National Security Authority, 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
- 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 Bratislava
- Ministry of Finance of the SR

- Institute of Measuremet, Slovak Academy of Sciences, Bratislava
- Slovak Standards Institute
- Ministry of Health of the SR, Strategic targets of Health
- Security Authority of the Ministry of Defence of the SR
- Institute of Forensic Science of Police Corps, Bratislava
- ÚIPŠ Bratislava
- Elfa, Ltd. Košice
- Datalan, Ltd. Bratislava

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 Mathematics, Faculty of Electrical Engineering, ČVUT Prague, 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, Tacoma, Washington, USA
- Institute for Experimental Mathematics, University of Essen, Germany
- Department of Mathematics and Science, Indiana State University, USA
- Eszterházy Károly College, Eger, Hungary
- DELTA Elektronik Limited, Budapešť, Hungary
- Fundatia Sapientia–Universitatea Sapientia, Facultătile din Miercurea Ciuc, Roumania
- AINTEK A.E, Greece
- Virginia Tech, Blacksburg, Virginia, USA
- McMaster University, Hamilton, Canada
- University of Waterloo, Canada
- University of Toronto, Canada
- Universität Ausgsburg, Germany
- Institut for Informatikk, Universitetet i Bergen, Norway

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 (J. Fogel)
- IACR (K. Nemoga)
- IET (M. Oravec)
- The European Association for the Transfer of Technologies, Innovation and Industrial
- Information (F. Lehocki)
- 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)

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 the Slovak Unit
- Atlantic Journal of Mathematical Cryptology, O. Grošek

VI. THESES

VI.1 Masters Theses

Masters theses supervised at the Department of Power Engineering. The names of supervisors are in brackets.

none

VI.2 Doctoral Theses

[1] Sýs, M.: Latin Squares in Cryptography (O. Grošek)

VII. OTHER ACTIVITIES

- Seminar Crypto (O. Grošek)
- Reviewer of ZentralblattMath (K. Nemoga, O. Grošek)

VIII. PUBLICATIONS

VIII.1 Journals

[1] BERGENTHUM, R., MAUSER, S., LORENZ, R.D., JUHÁS, G.: Unfolding Semantics of Petri Nets Based on Token Flows. In: Fundamenta Informaticae. - ISSN 0169-2968. - Vol. 94, No. 3-4 (2009), p. 331-360. (in English)

[2] BESZÉDEŠ, M., CULVERHOUSE, P., ORAVEC, M.: Facial Emotion Classification Using Active Appearance Model and Support Vector Machine Classifier. In: Machine Graphics and Vision. - ISSN 1230-0535. - Vol. 18, No. 1 (2009), p. 31-46. (in English)

[3] GROŠEK, O., VOJVODA, M., KRCHNAVÝ, R.: A New Matrix Test for Randomness. In: Computing. - ISSN 0010-485X. - Vol. 85 (2009), p. 21-36. (in English)

[4] GROŠEK, O., HORÁK, P., ZAJAC, P.: On Complexity of Round Transformations. In: Discrete Mathematics. - ISSN 0012-356X. - Vol. 309, No. 18 (2009), p. 5527-5534. (in English)

[5] JUHÁSOVÁ, A., JANOV, V., JUHÁS, G.: Dynamic Deadlock Of WorkFlow Processes. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 15, Special Issue (2009), p. 205-208. (in Slovak)

[6] LORENZ, R.D., JUHÁS, G., BERGENTHUM, R., DESEL, J., MAUSER, S.: Executability of Scenarios in Petri Nets. In: Theoretical Computer Science. - ISSN 0304-3975. - Vol. 410 (2009), p. 1190-1216. (in English)

[7] RÁSTOCKÝ, M., KUBÍK, M., LEHOCKI, F.: WorkFlow Systems in Medicine. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 15, Special Issue (2009), p. 193-196. (in Slovak)

VIII.2 Conference Proceedings

[1] ANTAL, E., GROŠEK, O.: Fialka M-125. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[2] BAN, J., FÉDER, M., ORAVEC, M.: Biometric Methods for Recognition of Human Face Images. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[3] FÉDER, M., BAN, J., ORAVEC, M.: Experiments with Selected Machine Learning Methods for Biometric Face Recognition. In: Proceedings Redžúr 2009: 3rd International Workshop on Speech and Signal Processing. Bratislava, Slovak Republic, 24.9.2009. - Bratislava: STU, 2009. - ISBN 978-80-227-3137-9. - p. 28-33. (in English)

[4] HAMBALÍK, A.: Biometry and Education. In: Trends in Education 2009. Information Technologies and Technical Education: International Conference. Olomouc, 25.6.2009. - Olomouc: Votobia, 2009. - ISBN 978-80-7220-316-1. - 286-288. (in Slovak)

[5] HURTOŇ, R., SCHINDLER, F.: Information System for Creation of Conferences by Using Technology J2EE. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[6] JANÍK, Z., ŠEVČÍKOVÁ, Z.: Web-Based Analysis of Petri Nets. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[7] JÓKAY, M., ZAJAC, P.: Parallelization Techniques for the Matrix Test Precomputation. In: 5th International Workshop on Grid Computing for Complex Problems. GCCP 2009: Bratislava, Slovak Republic, 26.-28.10.2009. - p. 103-109. (in English)

[8] KAZLOV, I., JUHÁS, G.: Bottleneck in Petri Nets. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[9] MAZANEC, J.: Human Face Recognition Capabilities - Psychological Experiment. In: ELITECH `09: 11th Conference of Doctoral Students. Bratislava, Slovak Republic, 25.5.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3091-4. - CD-Rom. (in English)

[10] MIKUŠ, M.: Remarks on Gödel's Code as a Hash Function. In: 9th Central European Conference on Cryptography. Třebíč, Czech Republic, 23.-26.6.2009. - Brno: University of Technology, 2009. - p. 16-17. (in English)

[11] PÁLFY, J., SCHINDLER, F.: XML in Environment of SQL Server 2008. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[12] PILKA, F., ORAVEC, M.: Time Delayed Neural Networks for Video Prediction. In: ELITECH `09: 11th Conference of Doctoral Students. Bratislava, Slovak Republic, 25.5.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3091-4. - CD-Rom. (in English)

[13] RASCHMANN, Š., ZAJAC, P.: Works Matching Using a Finite State Machine. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[14] ŠIMKO, J., SCHINDLER, F.: Development of Applications on the Platform J2ME. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[15] ŠUTKA, M., SCHINDLER, F.: Modern Techniques of Programming with Databases MS SQL in Environment .NET Framework. In: ŠVOČ 2009. Proceedings of Winning Works. Bratislava, Slovak Republic, 29.4.2009. - Bratislava: FEI STU, 2009. - ISBN 978-80-227-3094-5. - CD-Rom. (in Slovak)

[16] SZABÓ, T., SCHINDLER, F.: The Programming Language F# for the .NET Platform. In: Trends in Education 2009: Information technologies and Technical Education. Olomouc, 25.6.2009. - Olomouc: Votobia, 2009. - ISBN 978-80-7220-316-1. - p. 366-369. (in Slovak)

[17] ZAJAC, P.: Remarks on the 3D Lattice Sieve. In: 9th Central European Conference on Cryptography. Třebíč, Czech Republic, 23.-26.6.2009. - Brno: University of Technology, 2009. - p. 43-44. (in English)

VIII.3 Book

[1] ZAJAC, P.: Discrete Logarithms and Degree Six Number Field Sieve: A practical Approach. - Saarbrücken: VDM Verlag Dr. Müller, 2009. - 91 p. - ISBN 978-3-639-12331-9. (in English)

VIII.4 Parts of Books

[1] JUHÁS, G., LORENZ, R.D., DESEL, J.: Unifying Petri Net Semantics with Token Flows. In: Lecture Notes in Computer Science. - ISSN 0302-9743. - Vol. 5606: Applications and Theory of Petri Nets. - Berlin: Springer Verlag, 2009, p. 2-21. (in English)

[2] LORENZ, R.D., JUHÁS, G., MAUSER, S.: Partial Order Semantics of Types of Nets. In: Lecture Notes in Computer Science. - ISSN 0302-9743. - Vol. 5404: SOFSEM 2009. Theory and Practice of Computer Science. – Berlin: Springer Verlag, 2009. - ISBN 3-540-95890-8, p. 388-400. (in English)