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. Hossam El-Ddin, PhD., Ing. Alexander Hambalík, PhD., Mgr. Marek Sýs, 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. Ondrej Gallo, Ing. Matúš Jókay, Ing. Stanislav Marček, Ing. Ján Mazanec, Mgr. Michal Mikuš, Ing.Vladislav Novák, Ing. Filip Pilka

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 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)	P. Zajac

Algorithms and Programming	(1st sem., 3-2 h)	G. Juhás
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	(4rd sem., 3-1 h)	T. Delikat , G. Juhás
Information Security	(5th 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

III.2 Graduate Study (Ing.)

Object-Oriented Programming	(1st sem., 3-2 h)	F. Schindler
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

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

Algorithms and Programming	(1st sem., 12 h consul.)	P. Zajac
Algorithms and Programming	(1st sem., 12 h consul.)	M. Mikuš
Introduction to Engineering and Technical Documentation	(1st sem., 12 h consul.)	Z. Ševčíková
Programming Techniques	(2nd sem., 12 h consul.)	M. Mikuš
Programming Techniques	(2nd sem., 12 h consul.)	V. Novák
Database Systems	(3rd sem., 12 h consul.)	Š. Balogh
Computer Architecture	(2nd sem., 12 h consul.)	H. El-Ddin
Introduction to Cryptography - ERASMUS	(Ws. 2-2 h)	O. Grošek

III.4 Distance Study

Algorithms and Programming (1st sem., 6x2 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
- 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
- Development and Integration of Nonlinear System Methods, VEGA 1/3089/06, M. Huba,
  F. Schindler
- 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 Impovement 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
- 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
- Recognition of Human Face Images as the Part of Biometric Methods for Increasing the Security of Open Society, VEGA 1/3117/06, M. Oravec

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

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

none

VII. OTHER ACTIVITIES

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

VIII. PUBLICATIONS

VIII.1 Journals

[1] ADAMKO, L., VOJVODA, M., JÓKAY, M.: Statistical Analysis of ECRYPT eSTREAM Phase3 Ciphers. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 14, Special Issue (2008), p. 193-196. (in English)

[2] FOGEL, J.: Verification of Concurrent Programs by Model Checking. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 14, Special Issue (2008), p. 188-192. (in English)

[3] JUHÁS, G., LORENZ, R.D., MAUSER, S.: Causal Semantics of Algebraic Petri Nets Distinguishing Concurrency and Synchronicity. In: Fundamenta Informaticae. - ISSN 0169-2968. - Vol. 86, No. 3 (2008), p. 255-298. (in English)

[4] JUHÁS, G., LORENZ, R.D., MAUSER, S.: Complete Processes Semantics of Petri Nets. In: Fundamenta Informaticae. - ISSN 0169-2968. - Vol. 87, No. 3-4 (2008), p. 331-365. (in English)

[5] LEHOCKI, F., JUHÁS, G., LORENZ, R.D., SZCZERBICKA, H., DROZDA, M.: Decision Support with Logical and Fuzzy Petri Nets. In: Cybernetics and Systems. - ISSN 0196-9722. - Vol. 39, No. 6 (2008), p. 617-639. (in English)

[6] ORAVEC, M., PETRÁŠ, M., PILKA, F.: Video Traffic Prediction Using Neural Networks. In: Acta Polytechnica Hungarica. - ISSN 1785-8860. - Vol. 5, No. 4 (2008), p. 59-78. (in English)

[7] RIESZ, M., BALÁŽ, M., JUHÁS, G.: PetriFlow: A Petri Net Based Framework for Modelling and Control of Workflow Processes. In: Petri Net Newsletter. - ISSN 0931-1084. - Vol. 74, April (2008), p. 3-7. (in English)

[8] VAGÁNEK, P., ZAJAC, P.: Implementation of ECC in C#.Net. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 14, Special Issue (2008), p. 197-201. (in Slovak)

[9] VOJVODA, M., GROŠEK, O.: Side-Channels in Cryptoanalysis. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 14, Special Issue (2008), p. 26-29. (in Slovak)

VIII.2 Conference Proceedings

[1] ADAMKO, L., JÓKAY, M., VOJVODA, M.: Statistical Analysis of ECRYPT eSTREAM

Profile 1 Stream Ciphers. In: ELITECH ´08: PhD Students Conference. Bratislava, Slovak Republic, 20.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2878-2. - CD-Rom. (in English)

[2] GALLO, O., MARČEK, S.: Application of Optical Sensors in Biomedical Engineering. In: Meditech - Proceedings of the ESF Project Conference: Innovative Program of Modern Biomedical Technologies. Bratislava, Slovak Republic, 26.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2881-2. - p. 159-164. (in English)

[3] GROŠEK, O., VOJVODA, M., KRCHŇAVÝ, R.: A New Matrix Test for Randomness. In: 8th Central European Conference on Cryptography: Graz, Germany, 2.-4.7.2008. - p. 22-23. (in English)

[4] HAMBALÍK, A.: E-Learning and ICT. In: Trends in Education 2008: Olomouc, Czech Republic, 4.-5.6.2008. - Olomouc: Votobia, 2008. - ISBN 978-80-7220-311-6. – p. 307-310. (in English)

[5] JÓKAY, M., VOJVODA, M.: Distributed System for Files Decryption. In: 8th International Symposium on Forensic Sciences: Šamorín-Čilistov, Slovak Republic, 26.-29.9.2007. - Bratislava: KEUPZ, 2008. - ISBN 978-80-969471-2-6. - p. 31-40. (in English)

[6] KUBAČKA, S., BALOGH, Š.: Electronic Health Records. In: Meditech - Proceedings of the ESF Project Conference: Innovative Program of Modern Biomedical Technologies. Bratislava, Slovak Republic, 26.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2881-2. - CD-Rom.

[7] LABUDA, J., LEHOCKI, F.: About Meditech. In: Meditech - Proceedings of the ESF Project Conference: Innovative Program of Modern Biomedical Technologies. Bratislava, Slovak Republic, 26.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2881-2. - p. 4-7. (in English)

[8] LEHOCKI, F., STUCHLÍKOVÁ, Ľ., GALLO, O., KÉKEŠIOVÁ, G.: E-Learning in Professional Education for Medical High-School Students. In: Virtual University 2008: 9th International Conference. Bratislava, Slovak Republic, 11.-12.12.2008. - Bratislava: STU, 2008. - ISBN 978-80-89316-10-6. - CD-Rom. (in English)

[9] LEHOCKI, F., JUHÁS, G., LORENZ, R.D., DROZDA, M.: Extended Fuzzy Petri Nets for Decision Support. In: ISABEL 2008: 1st International Symposium on Applied Sciences in Biomedical and Communication Technologies. Aalborg, Denmark, 25.-28.10.2008. – Aalborg: Aalborg University, 2008. - CD-Rom. (in English)

[10] MARČEK, S., GALLO, O.: Non-Invasive Patient Monitoring. In: Meditech - Proceedings of the ESF Project Conference: Innovative Program of Modern Biomedical Technologies. Bratislava, Slovak Republic, 26.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2881-2. - p. 153-158. (in English)

[11] MIKUŠ, M.: New Way of Factoring Numbers. In: ELITECH ´08: PhD Students Conference. Bratislava, Slovak Republic, 20.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2878-2. - CD-Rom. (in English)

[12] 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, 2008. - ISBN 978-80-969471-2-6. - p. 12-13. (in English)

[13] PAVLOVIČ, A., LEHOCKI, F., BALOGH, Š.: Security of Electronic Health Records. In: Meditech - Proceedings of the ESF Project Conference: Innovative Program of Modern Biomedical Technologies. Bratislava, Slovak Republic, 26.5.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2881-2. - CD-Rom. (in English)

[14] PLANČÍK, M., ZAJAC, P.: Cryptoanalytic Language Distinguishing. In: ŠVOČ 2008:

Proceedings of Winning Works. Bratislava, Slovak Republic, 23.4.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2865-2. - CD-Rom. (in Slovak)

[15] STRAKA, T., SCHINDLER, F.: Basic Rules of Secure Internet. In: ŠVOČ 2008: Proceedings of Winning Works. Bratislava, Slovak Republic, 23.4.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2865-2. - CD-Rom. (in Slovak)

[16] SÝS, M.: Algorithm for Finding Isotopisms between Latin Squares. In: ITAT 2008: Information Technologies – Application and Theory. Hrebienok, Slovak Republic, September 2008. - Seňa: PONT Ltd., 2008. - ISBN 978-80-969184-8-5. - p. 99-104. (in Slovak)

[17] VAGÁNEK, P., ZAJAC, P.: ECC Implementation in the NET Framework. In: ŠVOČ 2008: Proceedings of Winning Works. Bratislava, Slovak Republic, 23.4.2008. - Bratislava: STU, 2008. - ISBN 978-80-227-2865-2. - CD-Rom. (in Slovak)

VIII.3 Parts of Books

[1] GROŠEK, O., ZAJAC, P.: Automated Cryptanalysis. In: Encyclopedia of Artificial Intelligence. - Hershey: Information Science Reference, 2008. - ISBN 978-1-59904-849-9. - p. 179-185. (in English)

[2] GROŠEK, O., ZAJAC, P.: Automated Cryptanalysis of Classical Ciphers. In: Encyclopedia of Artificial Intelligence. - Hershey: Information Science Reference, 2008. - ISBN 978-1-59904-849-9. - p. 186-191. (in English)