

DEPARTMENT OF APPLIED INFORMATICS AND INFORMATION TECHNOLOGY

<http://www.elf.stuba.sk/departments/kaivt/kaivt.html>

Head of Department

prof. RNDr. Otokar Grošek, PhD.
e-mail: otokar.grosek@stuba.sk

Tel: ++421-2-602 91 226
Fax: ++421-2-654 20 415

I. STAFF

Professors	prof. RNDr. Otokar Grošek, PhD.
Associate Professors	doc. RNDr. Jaroslav Fogel, PhD doc. RNDr. Frank Schindler, PhD.
Assistant Professors	Ing. Tomáš Delikát, PhD., Ing. Milan Vojvoda, PhD.
Research Workers	Ing. Martin Babinec
Technical Staff	Zuzana Šabíková (secretary)
PhD. Students	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

II. 2 Special Measuring Instruments and Computers

- HP Proliant ML 150
- 2x CPU INTEL XEON 2,8 GHz
- RAM 12 GB
- HDD 35 GB

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)	P. Zajac
Analysis and Complexity of Algorithms	(5th sem. 3-2 h)	M. Vojvoda
Bases of Real-time Systems	(3rd sem. 3-2 h)	J. Fogel
Cryptology	(5th sem. 3-1h)	O. Grošek
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. 2-2 h)	F. Schindler
Information Security	(5th sem. 3-1 h)	J. Šiška

III.2 Graduate Study (Ing.)

Formal Methods	(3rd sem. 3-1 h)	J. Fogel
Object Oriented Programming	(1st sem. 3-2 h)	F. Schindler
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

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

Informatics I	(1st sem 3 h consul.)	J. Fogel
Informatics II	(1st sem 1 h consul.)	J. Fogel

III.4 Distance Study

Bases of Real-time Systems	(3rd sem. 4x2 h consul.)	J. Fogel
Informatics	(3rd sem. 3x2 h consul.)	F. Schindler
Informatics II	(3rd sem. 3x2 h consul.)	T. Delikát
Algorithms and Programming	(2nd sem. 3x2 h consul.)	T. Delikát

IV. RESEARCH PROJECTS

- Information Processing in distributed Environment of Intelligent Agents. VG 1/0161/03, O. Grošek
- Modelling and Control of Distributed Processes Based on the Multi-agent Systems. G 2/4148/04, J.Fogel
- MARABU – Multi-agent Control System. APVT 51 011602, J. Fogel

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

V.2 International Cooperation

- Florida Atlantic University, Boca Raton, Florida, USA
- Academy of Sciences of the Czech Republic, Prague, CzR
- Department of Mathematics, University of Washington, Washington, USA
- Institute for Experimental mathematics, University of Essen, Germany
- University of LA LAGUNA, Department of Statistics, Operations Research and Computing, Tenerife, Spain
- Faculty of informatics MU Brno, CZ
- Department of Computer Sciences de Montfort University, Milton Keynes, UK,

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)

V.4 Contracts

- O. Grošek – Advanced course in Cryptology. Contract with NBU.

VI. THESES

VI.1 Masters Theses

- [1] M. Bálík: Attacks on the A5/1 Stream Cipher. (M. Vojvoda)

VII. OTHER ACTIVITIES

none

VIII. PUBLICATIONS

VIII.1 Journals

- [1] DELIKÁT, T.: Preparation of Implementation of ERP System in SMB Segment. In: eFocus. - Vol.5, No.4 (2005) - pp. 47-51. (in Slovak)
- [2] FOGEL, J., SCHINDLER, F.: Threads and Their Synchronization in Java Programs. In: EE - časopis pre elektrotechniku a energetiku. - Vol.11, Special Issue (2005) - pp. 34-36. (in Slovak)
- [3] ORAVEC, V., FOGEL, J.: Modeling of Agent Negotiation Process. In: Journal of Cybernetics and Informatics. - Vol.5 (2005) - pp. 24-31. (in English)
- [4] SCHINDLER, F.: New Trends in Evaluation Grading and Testing Students over the Internet. In: Technológia vzdelávania. - Vol.13, No.8 (2005) - pp. 8-10. (in Slovak)
- [5] SCHINDLER, F.: WEBYCHO: A Web-Based Tool for Problem Based Learning over the Internet. In: Technológia vzdelávania. - Vol.13, No.5 (2005) - pp. 15-17. (in English)

- [6] SÝS, M., GROŠEK, O.: New DL Problem. In: Journal of Electrical Engineering. - Vol.56, No.12/s (2005) - pp. 119-122. (in English)
- [7] ZAJAC, P.: Remark to the Mixing Layer of SPN Ciphers. In: Journal of Electrical Engineering. - Vol.56, No.12/s (2005) - pp. 32-35. (in English)

VIII.2 Conferences

- [1] FOGEL, J.: Deriving Knowledge in Multi Agents Control Systems with Imperfect Information. In: The International Conference on "Computer as a Tool" : Belgrade, Serbia and Montenegro, 21.-24.11.2005. pp. 1109-1112. (in English)
- [2] FOGEL, J.: Modeling Knowledge in Multi-Agents Control Systems. In: 8th International Conference Informatics 2005 : Bratislava, Slovak Republic, 20.-21.6.2005. pp. 73-76. (in English)
- [3] FOGEL, J., SCHINDLER, F.: Coping with Threads in Java Programming. In: 3rd Scientific Conference with International Participation "Communication and Information Technologies" : Liptovský Mikuláš, Slovak Republic, 23.-25.11.2005. pp. 119-122. (in English)
- [4] ORAVEC, V., FOGEL, J.: Modeling Multi Agent System with Alternating Transition Systems. In: International Conference "Cybernetics and Informatics" : Dolný Kubín, Slovak Republic, 9.-11.2.2005. pp. 171-178. (in English)
- [5] ORAVEC, V., FRANKOVIČ, B., FOGEL, J.: CookBook of Alternating Time System. In: 7th Conference for PhD Students ELITECH 2005 : Bratislava, Slovak Republic, 9.2.2005. pp. 42-44. (in English)
- [6] SCHINDLER, F.: Creation and Management of Virtual Learning Communities over the Internet. In: 1st Conference with International Participation "Informatics in School and Applications" : Ružomberok, Slovak Republic, pp. 6-10. (in Slovak)
- [7] SCHINDLER, F.: Evaluation, Testing and Grading of Students over the Internet. In: Conference "Technologies for e-Education 2005" : Prague, Czech Republic, 17.6.2005. pp. 37-42. (in Slovak)
- [8] SCHINDLER, F.: Learning with Support of the Virtual Learning Environment. In: 4th International Conference on Emerging e-Learning Technologies and Applications : Košice, Slovak Republic, 13.-14.9.2005. pp. 307-310. (in English)
- [9] SCHINDLER, F.: Management of Virtual Learning Communities over the Internet. In: 5th Czech-Slovak Conference BELCOM : Prague, Czech Republic, 21.-22.2.2005. (in English)
- [10] SCHINDLER, F.: New Trends in Monitoring, Testing and Grading of students over the Internet. In: 6th International Conference "Virtual University" : Bratislava, Slovak Republic, 15.-16.12.2005. pp. 182-185. (in English)
- [11] SCHINDLER, F.: Problem Based Learning over the Internet. In: 7th International Conference "Computer Based Learning in Science" : Žilina, Slovak Republic, 2.-6.7.2005. pp. 361-366. (in English)
- [12] SCHINDLER, F.: Remarks on Security in Programming. In: International Conference "Cybernetics and Informatics" : Dolný Kubín, Slovak Republic, 9.-11.2.2005. pp. 199-203. (in English)

- [13] SCHINDLER, F.: The Circle as a Non-Uniform Rational B-Spline Curve. In: 4th International Conference APLIMAT 2005 : Bratislava, Slovak Republic, 1.-4.2.2005. pp. 357-360. (in English)
- [14] SCHINDLER, F.: Virtual Collaboration under WebTycho. In: International Conference UNINFOS 2005 : Banská Bystrica, Slovak Republic, 7.-9.9.2005. pp. 228-233. (in English)
- [15] SCHINDLER, F.: WebTycho: A Web-Based Tool for Problem Based Learning over the Internet. In: Scientific Colloquium " Distance Education in Applied Informatics" : Nitra, Slovak Republic, 19.5.2005. pp. 36-41. (in English)
- [16] SCHINDLER, F.: WebTycho: a Web Based Tool to Test and Grade Students over the Internet. In: 8th International Conference Informatics 2005 : Bratislava, Slovak Republic, 20.-21.6.2005. pp. 211-215. (in English)

VIII.3 Parts of Books

- [1] SÝS, M., ZAJAC, P.: Discrete Logarithm Problem and Its Applications in Cryptography. In: Begabtenförderung im MINT-Bereichn 12. - Ulm: Aegis-Verlag, 2005. - pp. 129-146. (in English)
- [2] VOJVODA, M.: On the Correlation Attacks on Stream Ciphers. In: Begabtenförderung im MINT-Bereichn 12. - Ulm: Aegis-Verlag, 2005. - pp. 147-183. (in English)