General Information

Course name ÚINF/KRP1/15	**Cryptographic Protocols**	**ECTS Credits**	**4**
		Semester	**1**

Aims

To teach students about the design and verification of cryptographic protocols

Content

Authentication and key establishment using shared and public key cryptography, key agreement protocols, conference key agreement, zero-knowledge protocols.

Assessment Methods and Criteria

1. Attendance - students are expected to attend each class according to the schedule. Should the student miss three or more classes, he/she will not receive credits for the course no matter what his/her overall results are on the tests(s). The student must be on time for class.
2. Active participation - students are required to do their best with respect to active participation in seminar sessions.

Assessment: Home works 35%, active work on seminar + project 25%, test 40%.

Grading Scale (in %):
A 91-100%
B 81-90%
C 71-80%
D 61-70%
E 51-60%
FX 50 and less

Grading System:
The University recognizes the following six degrees for the evaluation of the study results:
a) A – excellent (excellent results) (numerical value 1)
b) B – very good (above average results) (1.5)
c) C – good (average results) (2)
d) D – satisfactory (acceptable results) (2.5)
e) E – sufficient (results meet the minimum criteria) (3)
f) FX –failed (requires further work) (4)

Bibliography

BOYD, C., MATHURIA, A.: Protocols for Authentication and Key Establishment, Springer, 2003
STINSON, D. R.: Cryptography: Theory and Practice, Third Edition, Chapman & Hall/CRC, 2006
SCHNEIER, B.: Applied Cryptography, Second Edition,
John Wiley & Sons Inc., 1996

RYAN, P., SCHNEIDER, S.: Modelling and Analysis of Security Protocols, Addison-Wesley, 2001