# STUDY MODULE DESCRIPTION FORM

| | | |
|---|---|---|
| Name of the module/subject<br>**Information security in Internet** | | Code<br>**1010332421010334336** |
| Field of study<br>**Information Engineering** | Profile of study (general academic, practical)<br>**(brak)** | Year /Semester<br>**1 / 2** |
| Elective path/specialty<br>**-** | Subject offered in:<br>**polish** | Course (compulsory, elective)<br>**obligatory** |
| Cycle of study:<br>**Second-cycle studies** | Form of study (full-time,part-time)<br>**full-time** | |
| No. of hours<br>Lecture: **2** Classes: **-** Laboratory: **1** Project/seminars: **-** | | No. of credits<br>**5** |
| Status of the course in the study program (Basic, major, other)<br>**(brak)** | (university-wide, from another field)<br>**(brak)** | |
| Education areas and fields of science and art<br>**technical sciences** | | ECTS distribution (number and %)<br>**5 100%** |

## Responsible for subject / lecturer:

dr hab. inż. Janusz Stokłosa, prof. nadzw.
email: janusz.stoklosa@put.poznan.pl
tel. +48 61 665 37 57
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

## Prerequisites in terms of knowledge, skills and social competencies:

| | | |
|---|---|---|
| 1 | **Knowledge** | Student has in-depth knowledge in the field of data security. He/she has in-depth knowledge of cryptography and basic in cryptanalysis. |
| 2 | **Skills** | Student can use advanced tools and information technologies. |
| 3 | **Social competencies** | Student understands the need to provide public information concerning the achievements in computer science and other aspects of business-computing engineer; he/she shall endeavour to provide information in a way understandable by presenting different points of view. |

## Assumptions and objectives of the course:

Presentation of cryptographic protocols on the Internet.

## Study outcomes and reference to the educational results for a field of study

### Knowledge:

1. Student has knowledge concerning IT, their applications and related problems. - [K_W06]
2. Student has knowledge of the trends and the most important new developments in the field of computer science. - [K_W14]

### Skills:

1. Student can obtain information from literature, databases, and other sources; can integrate the information obtained, their interpretation and critical evaluation, and also draw conclusions and formulate and fully justify the feedback. - [K_U01]
2. Student is able to propose and justify improvements to existing solutions. - [K_U12]

### Social competencies:

1. Student is able to think and act in a way that is creative and enterprising - [K_K01]

## Assessment methods of study outcomes

Written or/and oral examination based on lecture. Laboratory: written test.

## Course description

Standardization, TLS, IPsec (ESP, AH, ISAKMP, IKE), PKIX (Profiles, LDAP i OSCP, certification policy), PKCS (Cryptographic libraries, PKCS #11 - Cryptoki), Time stamping, cryptographic algorithms in access networks (GSM, UMTS, IEEE 802.11i).

Laboratory: SSL, TLS, S-HTTP protocols; Digital certificate; Public cryptographic system ? based on RSA, Communication security ? Secure Shell; Cryptographic algorithms in radio access networks

## Basic bibliography:

1. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001

2. Network and Internetwork Security, W. Stallings, Prentice Hall, 1994

3. RFC., http://www.ietf.org/rfc.html

## Additional bibliography:

1. Digital Signature Schemes., B. Pfitzmann, Springer, Berlin, 1996

2. Protection and Security on the Information Superhighway, F. B. Cohen, J. Wiley, New York, 1995.

3. Selected papers from Lecture Notes in Computer Science, Springer.

## Result of average student's workload

| Activity | Time (working hours) |
|---|---|
| 1. Lecture | 30 |
| 2. Laboratory | 15 |
| 3. Preparation to the laboratory | 15 |
| 4. Realization of laboratory reports | 10 |
| 5. Preparation to tests | 10 |
| 6. Preparation to the examination | 35 |
| 7. Participation in the consultations and examination | 10 |

## Student's workload

| Source of workload | hours | ECTS |
|---|---|---|
| Total workload | 125 | 5 |
| Contact hours | 50 | 2 |
| Practical activities | 25 | 1 |