ANEXA 2

Universitatea Politehnica Timişoara
Centrul de Educaţie Permanentă

Fişa disciplinei:

"Tehnici Criptografice Moderne"

Domeniul / Specializarea: CALCULATOARE / SECURITATEA INFORMAŢIILOR ŞI A SISTEMELOR CIBERNETICE

Anul I / Semestrul I

Titularul cursului: *Prof. dr. Bogdan GROZA*					
Colaboratori*: s.l.dr.ing. Pal-Stefan MURVAY, as.dr.ing. Horatiu-Eugen Gurban*					
Număr de ore total/Verificarea/Credite					
Curs	**Seminar**	**Laborator**	**Proiect**	**Examinare**	**Credite**
21	**-**	**9**	**12**	**E**	**3**

A. Obiectivele cursului

- Însuşirea de către cursanţi a fundamentelor teoretice în domeniul criptografiei, familiarizarea cu standardele în domeniul criptografiei simetrice şi asimetrice, introducere unor concepte moderne în criptografie, aplicarea conceptelor criptografice într-un mediu de dezvoltare software;
- Pregătirea de specialitate a cursanţilor le va permite alinierea la stadiul actual al criptografiei şi posibilitatea de a asimila materiile conexe care aplica cunostinte din domeniul criptografiei in alte domenii precum retele de calculatoare, vehicule, etc. oferind cunostintele de baza pentru proiectarea şi implementarea securitatii in aceste domenii.

B. Subiectele cursului

1. Introducere. Context istoric. Obiective de securitate. Tipuri de adversari şi de atacuri. (1 ora)
2. Fundamente matematice şi probleme computaţionale. Elemente de teoria informaţiei, teoria probabilităţiilor şi teoria numerelor (2 ore)
3. Funcţii criptografice simetrice. Funcţii fără cheie: generatoare de numere pseudo-aleatoare şi functii hash. Standarde existente, comun folosite in practica: MD5, SHA1, SHA2, SHA3. Funcţii cu cheie simetrică: coduri MAC şi criptări simetrice. Standarde existente comun folosite in practica: NMAC, HMAC,, 3DES, AES. Moduri de functionarea ale codurilor bloc, criptarea autentificata. (4 ore)
4. Funcţii Asimetrice. Funcţii de criptare cu cheie publică şi semnătură digitală. Standarde existente folosite in practica: RSA, Diffie-Hellman-Merkle, ElGamal, DSA. Moduri sigure de functionarea ale criptosistemelor asimetrice folosind paddinguri OAEP, PKCS, etc. (4 ore)
5. Curbe eliptice si variante pe curbe eliptice ale criptosistemelor bazate pe logaritmi discreti ECDSA si ECDH. (2 ore)
6. Protocoale de autentificare challenge-response si protocoale zero-knowledge. Protocoale de tunelare frecvent folosite in practica SSL/TLS, IPSec, SSH. (2 ore)
7. Modele formale pentru securitatea functiilor criptografice. Reductii de securitate pentru scheme de semnaturi digitale si criptari asimetrice. (2 ore)
8. Sisteme criptografice bazate pe identitate. Semnaturi digitale bazate pe identitate, algoritmii de semnare Shamir si Girault (2 ore).
9. Sisteme criptografice bazate pe transformate biliniare. Semnaturi bazate pe identitate si semnaturi de grup folosind transformate biliniare. Criptarea bazata pe identitate folosind transformari biliniare (algoritmii lui Boneh et al.). (2 ore)
10. Protocoale proof-of-work, scurt istoric si aplicatii. Tehnologia Blockchain. (2 ore)

C. Subiectele aplicaţiilor (laborator, seminar, proiect)

Laborator:

1. Utilizarea bibliotecilor pentru functii criptografice simetrice in .NET si Java. (3 ore)
2. Utilizarea bibliotecilor pentru functii criptografice asimetrice in .NET si Java. (3 ore)
3. Utilitarea unei bibliotecilor pentru conexiuni SSL/TLS in mediul Java. Biblioteci pentru functii criptografice folosind curbe eliptice si transformari biliniare. (3 ore)

Proiect:

Realizarea unei aplicatii care sa integreze concepte discutate la curs si laborator intr-o aplicatie practica de protectia datelor stocate local pe un calculator sau aflate in tranzit pe o conexiune TCP/IP. Alternativ, elaborarea unui studiu de caz. (12 ore)

D. Bibliografie

1. Oorschot, PC van, Scott A. Vanstone, and Alfred MENEZES. Handbook of Applied Cryptography, (1997).
2. Mao, W. Modern cryptography: theory and practice. Pearson Education India, (2003).
3. Lindell, Y., & Katz, J.. Introduction to modern cryptography. Chapman and Hall/CRC, (2014).

E. Evaluarea

Examen scris de tip grila + evaluare proiect practic. Nota finală este compusă din media celor două note obţinute: nota la examenul scris şi nota obţinută la evaluarea proiectului.

Data: 05.09.2018

Director de program de studii postuniversitare,	**Titular de disciplină,**
Prof. dr. ing. Bogdan GROZA	**Prof. dr. Ing. Bogdan GROZA**