Denumirea disciplinei	**Sisteme criptografice**
Codul disciplinei	S.06.A.044
Tipul disciplinei	De specialitate, opţională
Anul de studiu / semestrul	Anul III, semestrul VI
Limba de predare	română
Credite ECTS	3
Numărul de ore de contact/ Numărul total de ore	44/90
Evaluare	Examen
Titularul cursului	Lector universitar Vitalii Mititelu

Conţinutul cursului:

Noţiuni de bază ale Criptografiei. Clasificarea cifrurilor.
Sisteme de criptare cu cheie secretă. Cifrul DES. Cifrul Blowfish. Cifrul AES.
Administrarea cheilor criptografice ale cifrurilor cu cheie secreta
Sisteme de criptare cu cheie publică. Sistemul de criptare RSA. Sistemul de criptare Elgamal.
Funcţii hash. Algorimi ale funcţiilor hash: DSA, MD5, SHA-1, SHA-2, SHA-3.
Certificate digitale

Finalităţi de studiu:

La finalizarea acestui curs, studentul trebuie să demonstreze următoarele cunoştinţe, abilităţi şi competenţe:

- Să cunoască aparatul matematic aplicat la studierea metodelor de criptare a informaţiei;
- Să fie capabil să aplice limbajele de programare în realizarea algoritmilor de criptare studiaţi;
- Să realizeze un produs software care reprezintă un sistem de criptare;

Bibliografie:

1. Răcuciu Ciprian. Criptogrfie şi securitatea informaţiei. Bucureşti: Editura Universităţii „Titu Maiorescu”, 2010.
2. Нестеров С. А. Информационная безопасность и защита информациии. Санкт-Петербург: Издательство Политехнического университета, 2011; http://elib.spbstu.ru/dl/2451.pdf/view.
3. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition, Bruce Schneier, John Wiley & Sons, 1996.