



Denumirea disciplinei	Sisteme criptografice
Codul disciplinei	S.06.A.044
Tipul disciplinei	De specialitate, opțională
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

Conținutul cursului:

Noțiuni 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 secretă
Sisteme de criptare cu cheie publică. Sistemul de criptare RSA. Sistemul de criptare Elgamal.
Funcții hash. Algorimi ale funcțiilor hash: DSA, MD5, SHA-1, SHA-2, SHA-3.
Certificate digitale

Finalități de studiu:

La finalizarea acestui curs, studentul trebuie să demonstreze următoarele cunoștințe, abilități și competențe:

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

Bibliografie:

1. Răuciu Ciprian. Criptografie și securitatea informației. București: Editura Universității „Titu Maiorescu”, 2010.
2. Нестеров С. А. Информационная безопасность и защита информации. 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.