RTU studiju kurss "Kriptogrāfija un datu aizsardzība (speckurss)"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	TRL512
Nosaukums	Kriptogrāfija un datu aizsardzība (speckurss)
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācībspēks	Ernests Pētersons - Habilitētais doktors, Profesors
Apjoms daļās un kredītpunktos	1 daļa, 2.0 kredītpunkti, 3.0 EKPS kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Datu aizsardzības uzdevumi un to risināšanas ceļi. Šifrēšanas algoritmi uz substitūcijas un permutācijas bāzes. Standarts DES un tā stabilitāte. Virtuālie privātie tīkli. Autentificēšana un autorizēšana. Autentificēšana ar vienreizēju paroli. Autentificēšana ar sertifikātiem. Sertificēšanas centri. Publiskās atslēgas. Informācijas autentificēšana. Elektroniskais paraksts. Algoritms RSA. Ugunsmūri un maršrutētāji.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Apgūt teorētiskās zināšanas, lai kompetenti orientētos kriptogrāfiskās sistēmās. Praktiski apgūt RSA, PGP un DES metodes.
Patstāvīgais darbs, tā organizācija un uzdevumi	Patstāvīgas literatūras studijas. Studiju procesā tiek apgūts papildmateriāls par dažādu veidu telemātisko sistēmu datu aizsardzības risinājumiem.
Literatūra	RFD 2401-Security Architecture for the Internet Protocol. 1998. Stalling, W. Data and Computer Communications. Prentice Hall, 2002. A.Prasad, N. Prasad. 802.11 WLANs and IP Networking. Security, QoS and Mobility. Artech House, 2008.
Nepieciešamās priekšzināšanas	Datortīklu pamatus.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Datu aizsardzības uzdevumi un to risināšanas ceļi.	4	0	0	0
Šifrēšanas algoritmi uz substitūcijas un permutācijas bāzes.	4	0	0	0
Standarts DES un tā stabilitāte.	4	0	0	0
Virtuālie privātie tīkli.	4	0	0	0
Autentificēšana un autorizēšana. Autentificēšana ar vienreizēju atslēgu.	4	0	0	0
Publiskās atslēgas. Informācijas autentificēšana. Elektroniskais paraksts. Algoritms RSA.	8	0	0	0
Ugunsmūri un maršrutētāji.	4	0	0	0
Kopā:	32	0	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Spēj raksturot šifrēšanas algoritmus uz substitūcijas un permutācijas bāzes.	Kontroldarbs. Orientējas šifrēšanas algoritmos uz substitūcijas un permutācijas bāzes.
Spēj raksturot DES standartu.	Kontroldarbs.Orientējas DES standarta.
Spēj raksturot 'Publiskās atslēgas" (RSA) algoritmu.	Kontroldarbs.Orientējas RSA algoritmā.
Spēj raksturot Informācijas autentificēšanu un Elektroniskā paraksta principus.	Kontroldarbs.Orientējas autentificēšanas un elektroniskā paraksta principos.
Spēj raksturot PGP algoritmu.	Kontroldarbs.Orientējas PGP algoritmā.
Spēj raksturot ugunsmūra izveidošanas metodes.	Ieskaite. Kompetenti raksturo datu un tīklu aizsardzības sistēmas. Noslēgumā eksāmens.

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	2.0	1.0	0.0	1.0		*	