Kursuseprogramm

Ainekood: **IFI6020**	NIMETUS: **KRÜPTOLOOGIA MEETODID ANDMETURBES**		
Maht 4.0 EAP	Kontakttundide maht: 42	Õppesemester: K	Eksam
Eesmärk:	Luua eeldused süstemaatilise ülevaate saamiseks kaasaja krüptograafiast nii teoreetilise kui ka praktilise ehk kasutusliku poole pealt, mida läheb valdkonnas orienteerumiseks vaja ühel kaasaja IT spetsialistil või matemaatikul.		
Aine lühikirjeldus: (sh iseseisva töö sisu kirjeldus vastavuses iseseisva töö mahule)	Kursus algab krüptograafia ajaloost. Seejärel tutvustatakse valdkonna põhimõisteid ja alusprintsiipe. Põhjalikult vaadeldakse sümmeetrilisi krüptoalgoritme, sealhulgas plokk ja jadašifreid ning järgnevalt asümmeetrilisi krüptoalgoritme. Vaadeldakse nende kasutusrežiime ja koostoimeid enamlevinud krüptoprotokollides. Ülejäänud kursuse osa keskendub mitmesugustele krüptotehnika praktilistele rakendustele: autentimine, digisignatuur/digiallkiri.		
Õpiväljundid:	Teadmised krüptograafia teoreetilistest alustest. Suutlikkus orienteeruda krüptograafia põhimõistetes ja algoritmides. Praktilised oskused krüpteerimises ja dekrüpteerimises erinevate algoritmide abil. Teadmised andmeturbest ja krüptotehnika rakendamisest antud valdkonnas. Teadmised krüptotehnika praktilistest rakendustest.		
Hindamismeetodid:	Igal üliõpilasel tuleb teha aine sooritamiseks eksam. Eksam koosneb teoreetilisest kirjalikust tööst ning praktilisest ülesandest. Kursuse hinne 50% ulatuses koosneb eksami tulemusest ning 35% kontrolltöö tulemusest ning 15% kodutööst		
Õppejõud:	Dotsent Erika Matsak, PhD		
Ingliskeelne nimetus:	CRYPTOLOGY IN DATA SECURITY		
Eeldusaine:	MLM6202, MLM6222		
Kohustuslik kirjandus:	Infosüsteemide turve. 1. osa: turvarisk. Hanson, V. (1997) Infosüsteemide turve. 2. osa: Turbe tehnoloogia. Hanson, V., Buldas, A., Lipmaa, H. (1998) Digitaalallkiri – tee paberivabasse maailma. Praust, V. (2001)		

Asenduskirjandus: (üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab ainekursuse loengulist osa)	T. Beltier, J. Beltier, J. Blackley. Information Security Fundamentals. Auerbach, 2004 A. Manezes, P. Oorschot, S. Vanstone. Handbook Of Applied Cryptography. CRC Press, 2001 J. Katz, Y. Lindell. Introduction to modern cryptography. CRC Press, 2007 J. Tablot, D. Welsh. Complexity and Cryptography. An Introduction. Cambridge Universitu Press, 2006
Õppetöös osalemise ja eksamile/arvestusele pääsemise nõuded	Eksami pääsemise eelduseks on kaitstud kodutöö, positiivne tulemus kontrolltöös ning esitatud praktikumides tehtud töö. Järeleksamit saab sooritada ainult järelvastamiseks ettenähtud nädalatel eelnevalt välja kuulutatutel kuupäevadel.
Iseseisva töö nõuded	Iseseisvaks tööks on praktiline kodutöö. Kodutöö variandi saab valida tunnis. Kodutöö numbrit tuleb registreerida õppejõu juures. Osalemine praktikumis ja loengutes toetab eduka kodutöö valmistamist. Kodutöö tuleb dokumenteerida vastavalt nõudmistele ning kaitsta seminaril. Igal nädal on võimalik tulla konsultatsioonile õppejõu poolt väljakuulutatud nädalapäeval ja kellaajal.
Eksami hindamiskriteeriumid või arvestuse sooritamiseks vajalik miinimumtase	Hindamiskriteeriumid, millest hindamisel lähtutakse: 1.kriteerium: Teoreetiline baas A – Oskab seletada 91-100% ulatuses teoreetilisel tasemel krüpteerimisel käsitlevaid aspekte (vt aine lähikirjeldust) etteantud küsimustes kirjalikus töös. Tunneb mitmeid erinevaid algoritme detailides, oskab võrrelda algoritmide tugevusi ja nõrkusi. B - Oskab seletada 81-90% ulatuses teoreetilisel tasemel krüpteerimisel käsitlevaid aspekte (vt aine lähikirjeldust) etteantud küsimustes kirjalikus töös. Tunneb mitmeid erinevaid algoritme detailides, oskab võrrelda algoritmide tugevusi ja nõrkusi. C - Oskab seletada 71-80% ulatuses teoreetilisel tasemel krüpteerimisel käsitlevaid aspekte (vt aine lähikirjeldust) etteantud

	küsimustes kirjalikus töös. Tunneb **mõningaid (üle nelja)** algoritme detailides, oskab võrrelda **nende** algoritmide tugevusi ja nõrkusi. D - Oskab seletada 61-70% ulatuses teoreetilisel tasemel krüpteerimisel käsitlevaid aspekte (vt aine lähikirjeldust) etteantud küsimustes kirjalikus töös. Tunneb **mõningaid (üle kahte)** algoritme detailides, oskab võrrelda **nende** algoritmide tugevusi ja nõrkusi. E - Oskab seletada 51-60% ulatuses teoreetilisel tasemel krüpteerimisel käsitlevaid aspekte (vt aine lähikirjeldust) etteantud küsimustes kirjalikus töös. Tunneb **vähemalt ühte** algoritmi detailides, oskab esile tuua **selle** algoritmi tugevusi ja nõrkusi. 2.kriteerium: Praktilised oskused (Abimaterjali kasutamine on lubatud) A – Krüpteerib avateksti ja dekrüpteerib krüptogramme tuntud kaasaegsete algoritmide abil (91-100% õpitud kogusest). Oskab programmeerida mitme lihtsamate algoritmide realisatsioone. B - Krüpteerib avateksti ja dekrüpteerib krüptogramme tuntud kaasaegsete algoritmide abil (81-90% õpitud kogusest). Oskab programmeerida mitme lihtsamate algoritmide realisatsioone. C - Krüpteerib avateksti ja dekrüpteerib krüptogramme tuntud kaasaegsete algoritmide abil (71-80% õpitud kogusest). Oskab programmeerida **mõningate (vähemalt nelja)** lihtsamate algoritmide realisatsioone. D - Krüpteerib avateksti ja dekrüpteerib krüptogramme **vähemalt kahe** (üks sümmeetriline ja teine asümmeetriline) tuntud kaasaegsete algoritmide abil. Oskab programmeerida **mõningate (üle kahte)** lihtsamate algoritmide realisatsioone. E - Krüpteerib avateksti ja dekrüpteerib krüptogramme **vähemalt ühe** tuntud kaasaegse algoritmi abil. Oskab programmeerida **vähemalt ühte** lihtsama algoritmi realisatsiooni.
Informatsioon kursuse sisu kohta, kursuse jaotumine teemade kaupa sh kontakttundide ajad	Läbitavad teemad loengute kaupa. 30.01.2012 - Krüptograafia ajalugu
	01.02.2012 - Sissejuhatus krüptograafiasse, mõisted, probleemid, definitsioonid
	01.02.2012 - Praktikum. Sõnade krüpteerimine Caesari šifri, Vigenere-i šifri abil. CocoVilla ja ekspertsüsteem kübersündmuste

	liigitamiseks. Turvaklasside moodustamine ja turvaklassidele vastavate turvameetmete valimine.
	06.02. 2012 - Sümmeetrilised krüptoalgoritmid. Põhialused, plokkšiffer, jadašiffer. Feisteli võrk. DES (Data Encryption Standard).
	08.02.2012 - Sümmeetrilised krüptoalgoritmid . Blowfish, IDEA. Erinevad meetodid juhuarvude genereerimiseks.
	08.02.2012 - Praktikum (Plokkšiffer, jadašiffer, Feisteli võrk)
	13.02.2012 - Krüpteerimise standardid. Advanced Encryption Standards (AES). Algoritmid MARS, Serpent, Twofish
	15.02.2012 - Algoritmid Rijndael ja RC6. Algoritmid ja nende matemaatilised alused.
	15.02.2012 - Praktikum (Rijndael)
	20.02.2012 - Avatud võtmega krüpteerimine. Asümmeetrilised krüptosüsteemid. RSA
	22.02.2012 - Krüptoräsid **(**Hash- funktsioonid) ja autentimine. Kasutatavaimad algoritmid. MD5, SHA-1, SHA-2.
	22.02.2012 - Praktikum. Krüptoräsid.
	27.02.2012 - Digiallkirjastamine. Nõudmised digiallkirjale, standardid
	29.02.2012 - Võtmete vahetamise algoritmid ja autentimine. Vaadeldakse võtmete vahetamiseks kolmanda osapoole kasutatavaid algoritme.
	29.02.2012 - Praktikum. Eestis kasutatav digiallkiri
	05.03.2012 - Paroolide murdmine vastavate tabelitega (rainbow table). „Sool“ paroolide krüpteerimisel. Protokoll IPSec, võtmevahetus IKE protokolliga.
	07.03.2012 - Protokollid SSH, SSL ja TLS
	07.03.2012 - Praktikum. Paroolide testimine krüptoräside MD5 ja

	SHA-1abil
	12.03.2012 - Kontrolltöö
	14.03.2012 - Kodutööde kaitsmine
	14.03.2012 - Kodutööde kaitsmine + võlgade likvideerimine

Õppeainet kureeriv üksus:	Informaatika instituut
Kursuseprogrammi koostaja	Erika Matsak
Allkiri:	
Kuupäev:	01.23.2012