Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Luonnos luento-ohjelmaksi 23. tammikuuta 1998	Tuomas Aura

Tähän suunnitelmaan tulee muutoksia!

päivä	aihe	Schneier
23.1.	aloitusluento	
	tietoturvallisuus	
	kryptografia	1
	salakirjoitus	2.2
	informaatioteoriaa	11.1–11.2
	avaimet	7.1, 7.5–7.6
30.1.	symmetrinen salaus 1	
	SP-verkko ja Feistel-salaus	14.10
	DES	12
	lohkosalauksen käyttömoodit	9
6.2.	symmetrinen salaus 2	
	moninkertainen salaus	15
	differentiaalinen kryptoanalyysi	12.4-12.5
	saranapuolelta sisään	ei kirjassa
13.2	symmetrinen salaus 3	
	IDEA	13.9, 14.2
	satunnaisbittigeneraattorit	2.8,16.1-16.5,17.4
	bittivirtasalaus	
	jaetut salaisuudet	3.6-3.7,23.2
20.2.	julkinen avain 1	
	yksisuuntaiset hajautusfunktiot	2.3-2.4,18.1,(18.5), (18.7),18.11 alku, 7.4,14.11
	MAC	18.14
	julkisen avaimen algoritmit	2.5-2.7,19.1,7.2-7.3
	lukuteoriaa	11.3-11.6
27.2.	julkinen avain 2	
	RSA	19.3
	RSA salauksessa	
	RSA allekirjoituksessa	
	salauksen käyttö	10
	multicast	3.5,22.7,22.1
6.3.	julkinen avain 3	
	Diffie-Hellman	22.1
	ElGamal	19.6
	käyttäjän tunnistaminen	ei kirjassa
	nollatietotodistukset	5.1,23.11
	tunnistusprotokollat	5.2,21.2
13.3.	kauppa 1	
	allekirjoitukset	4.3-4.6,5.3,23.12
	sopimukset	5.5,5.7-5.9
	aikaleimat	4.1
	pelit	4.9-4.11
20.3.	kauppa 2	
	sähköinen rahaliikenne	6.4
	anonyymi käteinen, ecash	
27.3.	avaintenhallinta 1	
	avaintenjakelu ja autentikointi	2.1,3.1-3.3
	hyökkäyksiä protokollia vastaan	
	suunnitteluperiaatteita	ei kirjassa
3.4.	avaintenhallinta 2	
	X.509	24.9
	Kerberos	24.5
	SSH, SSL	ei kirjassa
	sertifikaatit	8
10.4.	pääsisäisloma	
17.4.	avaintenhallinta 3	
	protokollien verifiointi	3.4, ei kirjassa
	tilakonemallit	
	loogiset todistusmenetelmät	
24.4.	tiedon kätkeminen	
	kopiosuojaus	3.8
	omistusmerkintä	ei kirjassa
	subliminaaliset kanavat	4.2,23.3
	steganografia	1.2, ei kirjassa

Tenttialueeseen kuuluvat taulukkoon merkitys osat Schneierin kirjasta. Sen lisäksi voidaan kysyä asioita, joita on käsitelty luennoilla, laskuharjoituksissa tai opetusmonisteissa.