

Inhalt:

VORWORT DES HERAUSGEBERS.....	1
INFORMATIK, TECHNIK, WIRTSCHAFT, RECHT UND MATHEMATIK – GEHT DAS ZUSAMMEN?.....	2
1 BEGRIFFE UND HISTORIE <i>BERND EYLERT</i>.....	4
1.1 IT-SICHERHEIT	4
1.2 STEGANOGRAPHIE.....	5
1.3 VERSCHLÜSSELUNGSTERMINOLOGIE UND FRÜHE METHODEN	6
2 ZUGANGSSICHERUNG <i>BERND EYLERT</i>.....	10
2.1 MECHANISCHE SCHUTZMAßNAHMEN.....	10
2.2 ELEKTRONISCHE SCHUTZMAßNAHMEN	12
2.3 PHYSIKALISCHE ANFORDERUNGEN AN ZUGANGSSYSTEME	13
2.4 ALGORITHMEN, SCHLÜSSEL UND WEITERE TERMINI.....	14
2.5 ANFORDERUNGEN AN EIN KRYPTOGRAPHISCHES SICHERHEITSSYSTEM	16
3 KRYPTOLOGISCHE GRUNDLAGEN <i>BERND UND DOROTHEE EYLERT</i>.....	18
3.1 MATHEMATISCHE GRUNDLAGEN	18
3.2 MATHEMATISCHE STRUKTUREN	29
3.3 BERECHNUNG DES LOGARITHMUS MODULO M	34
3.4 EUKLIDISCHER ALGORITHMUS	35
3.5 SATZ VON EULER	37
4 VERTEILTE GEHEIMNISSE <i>JOHANNES BLÖMER</i>.....	39
4.1 EINE EINFACHE METHODE ZUM TEILEN VON GEHEIMNISSEN.....	40
4.2 MODULARE GEHEIMNISTEILUNG	41
4.3 GEOMETRISCHES GEHEIMNISTEILEN	43
4.4 ALLGEMEINES GEHEIMNISTEILEN.....	44
5 AUSGEWÄHLTE VERSCHLÜSSELUNGSVERFAHREN <i>BERND UND DOROTHEE EYLERT</i>.....	48
5.1 ASYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN - PKI	48
5.1.1 DIFFIE-HELLMAN-VERFAHREN.....	49
5.1.2 ELGAMAL-VERFAHREN	51
5.1.3 RSA-ALGORITHMUS.....	52
5.2 SYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN	58
5.2.1 ONE-TIME-PAD.....	58
5.2.2 BLOCKCODES.....	60
5.2.3 ENCRYPTION FUNCTIONS.....	62
5.3 KRYPTOLOGISCHE ZWITTER – HASHFUNKTIONEN	64
6 SIGNATURVERFAHREN <i>JANETT MOHNKE</i>.....	68
6.1 DIGITALE SIGNATUR	68
6.2 DIE IDEE	68
6.3 SIGNATUR MIT RSA	71
6.4 SIGNATUR MIT ELGAMAL	71

7	ELLIPTISCHE KURVEN <i>BERND EYLERT UND ERNST G GIESSMANN</i>	74
7.1	FUNKTIONENTHEORETISCHE HERLEITUNG <i>BERND EYLERT</i>	74
7.1.1	FERMAT UND DIE ELLIPTISCHEN KURVEN	74
7.1.2	URSPRUNG DES BEGRIFFS ELLIPTISCHE KURVEN	75
7.1.3	ELLIPTISCHE FUNKTIONEN	77
7.1.4	WEIERSTRASS'SCHE p -FUNKTION	78
7.1.5	ELLIPTISCHE KURVE	79
7.2	ANWENDUNGEN MIT ELLIPTISCHEN KURVEN <i>ERNST G GIESSMANN</i>	80
7.2.1	OPERATIONEN	81
7.2.2	EC-DH UND EC-ELGAMAL	83
7.2.3	STANDARDISIERTE KURVEN	85
7.2.4	SIGNATURALGORITHMEN	86
7.2.5	SCHUTZ DURCH RANDOMISIERUNG	88
8	SICHERHEITSKONZEPTE FÜR INFORMATIONSSYSTEME <i>BERND EYLERT</i>	90
8.1	IT-STRUKTURANALYSE	92
8.2	SCHUTZBEDARFSFESTSTELLUNG	93
8.2.1	SCHUTZZIELE	94
8.2.2	SCHUTZBEDARFSKATEGORIEN	96
8.3	IT-GRUNDSCHUTZANALYSE	96
8.3.1	SICHERHEITSANALYSE	98
8.3.2	RISIKOANALYSE	98
8.4	REALISIERUNGSPLANUNG	101
8.5	STANDARDS DER QUALITÄTSSICHERUNG	103
9	RECHTSFRAGEN DER IT-SICHERHEIT <i>JULIANE HOLTZ</i>	104
9.1	RECHTLICHE RAHMENBEDINGUNGEN DER IT-SICHERHEIT	104
9.1.1	DATENSCHUTZRECHT	104
9.1.2	RISIKOMANAGEMENT	112
9.1.3	ARCHIVIERUNGSPFLICHT	114
9.1.4	VERKEHRSSICHERUNGSPFLICHTEN	116
9.1.5	VERTRAGLICHE VEREINBARUNGEN	117
9.2	RECHTSRAHMEN FÜR DIE ERSTELLUNG ELEKTRONISCHER SIGNATUREN	118
9.3	ZIVILRECHTLICHE HAFTUNGSRISIKEN UND STRAFRECHTLICHE VERANTWORTUNG	119
9.3.1	ZIVILRECHTLICHE HAFTUNG	120
9.3.2	STRAFRECHTLICHE VERANTWORTLICHKEIT	121
9.4	ARBEITSRECHTLICHE ASPEKTE	123
10	ANHANG	126
10.1	LITERATURVERZEICHNIS	126
10.2	ABKÜRZUNGSVERZEICHNIS	129
10.3	STICHWORTVERZEICHNIS	131