

1	Der Weg zur RSA-Signatur	1
1.1	Digitale Signatur – das Szenario	1
1.2	Euklidischer Algorithmus	3
1.3	Modulo-Rechnung und kleiner Fermat'scher Satz	5
1.4	Binärzahl und binäre Entwicklung	8
1.5	RSA-Signatur	9
1.6	Wiederholtes Quadrieren	12
2	DSA- und ECDSA-Signatur	15
2.1	Gruppen und der Satz von Cauchy	15
2.2	Diskreter Logarithmus	18
2.3	DSA-Signatur	19
2.4	Reellwertige elliptische Kurven	22
2.5	Diskreter Logarithmus auf modularen elliptischen Kurven	25
2.6	Die ECDSA-Signatur	28
3	Rund um die digitale Signatur	31
3.1	Verschlüsseln und Entschlüsseln	31
3.2	Hashwerte – ein digitaler Fingerabdruck	34
3.3	Miller-Rabin-Primzahlen	37
3.4	Zufallsgeneratoren	39
3.5	Authentifikation und Challenge-Response	41
3.6	Fazit und Ausblick	43
	Was Sie aus diesem <i>essential</i> mitnehmen können	47
	Literatur	49