

Dati	Bearbeiten	Ansicht	Ver-/Entschlüsseln	Digitale Signaturen/PKI	Einzelverfahren	Analyse	Optionen	Fenster	Hilfe
<ul style="list-style-type: none">NeuÖffnen...SchließenSpeichernSpeichern als...Dokument-Eigenschaften...Drucken...Drucker einstellen...Zuletzt geöffnete DateienBeenden	<ul style="list-style-type: none">RückgängigWiederherstellenAusschneidenKopierenEinfügenLöschenSuchen/Ersetzen...Suche nächstesAlles markierenSchlüssel anzeigenÜbergeordnetes Fenster	<ul style="list-style-type: none">SymbolleisteStatusleisteAls Text anzeigenAls HexDump anzeigenBalkendiagrammAlphabetZeilenendeZeilenumbruchLeerzeichenSchriftart<ul style="list-style-type: none">Arial 8Arial 10Arial 12Courier 8Courier 10Courier 12Box (Würfelkanten zeigen)	<ul style="list-style-type: none">Symmetrisch (klassisch)<ul style="list-style-type: none">Caesar / Rot-13...Vigenère...Hill...Substitution / Atbash...Playfair...ADFGVX...Byteweise Addition...XOR...Vernam...Homophone...Permutation / Transposition...Solitaire...Symmetrisch (modern)<ul style="list-style-type: none">IDEA...RC2...RC4...DES (ECB)...DES (CBC)...Triple DES (ECB)...Triple DES (CBC)...Rijndael (AES)...Weitere Algorithmen<ul style="list-style-type: none">MARS...RC6...Serpent...Twofish...DESX...DESL...DESXL...AES (selbstextrahierend)...Asymmetrisch<ul style="list-style-type: none">RSA-Verschlüsselung...RSA-Entschlüsselung...RSA-Demo...Hybrid<ul style="list-style-type: none">RSA-AES-Verschlüsselung...RSA-AES-Entschlüsselung...ECC-AES-Verschlüsselung...ECC-AES-Entschlüsselung...	<ul style="list-style-type: none">PKI<ul style="list-style-type: none">Schlüssel erzeugen/importieren ...Schlüssel anzeigen/exportieren ...Dokument signieren...Signatur überprüfen...Signatur extrahierenSignatordemo (Signaturerzeugung)...	<ul style="list-style-type: none">Hashverfahren<ul style="list-style-type: none">MD2MD4MD5SHASHA-1SHA-256SHA-512RIPEMD-160Hashwert einer Datei...Hash-Demo...Schlüssel aus Passwort generieren (PKCS #5)...Generieren von MACs...RSA-Kryptosystem<ul style="list-style-type: none">Primzahltest...Primzahlen generieren...Faktorisieren einer Zahl...RSA-Demo...Signatordemo (Signaturerzeugung)...Gitterbasierte Angriffe auf RSA<ul style="list-style-type: none">Faktorisieren mit teilweise bekanntem p...Angriff auf stereotype Nachrichten...Angriff auf kleine geheime Schlüssel...Protokolle<ul style="list-style-type: none">Diffie-Hellman-Demo...Authentisierungsverfahren im Netz...Anwendungen des Chinesischen Restsatzes<ul style="list-style-type: none">Astronomie und Planetenbewegung...Modulare Hin- und Rücktransformation...Secret Sharing mittels CRT...Visualisierung von Algorithmen<ul style="list-style-type: none">Caesar...Vigenère...Nihilist...DES...AES<ul style="list-style-type: none">Rijndael-Animation...Rijndael-Inspektor...Enigma...Secret-Sharing-Demo (nach Shamir)...Tools<ul style="list-style-type: none">Codierungen<ul style="list-style-type: none">Base64-Codierung/Decodierung<ul style="list-style-type: none">Base64 codierenBase64 decodierenUU-Codierung/Decodierung<ul style="list-style-type: none">UU codierenUU decodierenASN.1-Decodieren eines DokumentsKomprimieren<ul style="list-style-type: none">ZipUnZipZufallsdaten erzeugen...Passwort-Qualitätsmesser...Passwort-Entropie...Textdokument formatieren...Lernspiele<ul style="list-style-type: none">Der ZahlenhaiZahlentheorie interaktiv<ul style="list-style-type: none">Lernprogramm für Zahlentheorie...Punktaddition auf Elliptischen Kurven...	<ul style="list-style-type: none">Werkzeuge zur Analyse<ul style="list-style-type: none">EntropieGleitende HäufigkeitHistogrammN-Gramm...AutokorrelationPeriodeSymmetrische Verschlüsselung (klassisch)<ul style="list-style-type: none">Ciphertext-Only<ul style="list-style-type: none">CaesarVigenèreADFGVX...SubstitutionSolitaireByteweise AdditionXORKnown-Plaintext<ul style="list-style-type: none">Hill...Manuelle Analyse<ul style="list-style-type: none">Substitution...Playfair...SolitaireSymmetrische Verschlüsselung (modern)<ul style="list-style-type: none">IDEA...RC2...RC4...DES (ECB)...DES (CBC)...Triple DES (ECB)...Triple DES (CBC)...Rijndael (AES)...Weitere Algorithmen<ul style="list-style-type: none">MARS...RC6...Serpent...Twofish...DESX...DESL...DESXL...Asymmetrische Verfahren<ul style="list-style-type: none">Faktorisieren einer Zahl...Gitterbasierte Angriffe auf RSA<ul style="list-style-type: none">Faktorisieren mit teilweise bekanntem p...Angriff auf stereotype Nachrichten...Angriff auf kleine geheime Schlüssel...Seitenkanalangriff auf "Textbook-RSA"...Hashverfahren<ul style="list-style-type: none">Angriff auf den Hashwert der digitalen Signatur ...Zufallsanalyse<ul style="list-style-type: none">Frequency-TestPoker-TestRuns-TestSerial-TestFIPS PUB-140-1 TestbatterieVitany3D-Visualisierung...	<ul style="list-style-type: none">Grafikoptionen...Analyseoptionen...Textoptionen...Startoptionen...Weitere Optionen...	<ul style="list-style-type: none">Überlappend anordnenNichtüberlappend anordnenSymbole anordnenAlle schließen	<ul style="list-style-type: none">StartseiteIndexSzenarien (Tutorials)ReadmeSkriptPräsentationÜber CrypTool