

Datei	Bearbeiten	Ansicht	Ver-/Entschlüsseln	Digitale Signaturen/PKI	Einzelverfahren	Analyse	Optionen	Fenster	Hilfe
<ul style="list-style-type: none"><li>Neu</li><li>Öffnen...</li><li>Schließen</li><li>Speichern</li><li>Speichern als...</li><li>Dokument-Eigenschaften...</li><li>Drucken...</li><li>Drucker einstellen...</li><li>Zuletzt geöffnete Dateien</li><li>Beenden</li></ul>	<ul style="list-style-type: none"><li>Rückgängig</li><li>Wiederherstellen</li><li>Ausschneiden</li><li>Kopieren</li><li>Einfügen</li><li>Löschen</li><li>Suchen/Ersetzen...</li><li>Suche nächstes</li><li>Alles markieren</li><li>Schlüssel anzeigen</li><li>Übergeordnetes Fenster</li></ul>	<ul style="list-style-type: none"><li>Symbolleiste</li><li>Statusleiste</li><li>Als Text anzeigen</li><li>Als HexDump anzeigen</li><li>Balkendiagramm</li><li>Alphabet</li><li>Zeilenende</li><li>Zeilenumbruch</li><li>Leerzeichen</li><li>Schriftart<ul style="list-style-type: none"><li>Arial 8</li><li>Arial 10</li><li>Arial 12</li><li>Courier 8</li><li>Courier 10</li><li>Courier 12</li></ul></li><li>Box (Würfelkanten zeigen)</li></ul>	<ul style="list-style-type: none"><li>Symmetrisch (klassisch)<ul style="list-style-type: none"><li>Caesar / Rot-13...</li><li>Vigenère...</li><li>Hill...</li><li>Substitution / Atbash...</li><li>Playfair...</li><li>ADFGVX...</li><li>Byteweise Addition...</li><li>XOR...</li><li>Vernam...</li><li>Homophone...</li><li>Permutation / Transposition...</li><li>Solitaire...</li></ul></li><li>Symmetrisch (modern)<ul style="list-style-type: none"><li>IDEA...</li><li>RC2...</li><li>RC4...</li><li>DES (ECB)...</li><li>DES (CBC)...</li><li>Triple DES (ECB)...</li><li>Triple DES (CBC)...</li><li>Rijndael (AES)...</li><li>Weitere Algorithmen<ul style="list-style-type: none"><li>MARS...</li><li>RC6...</li><li>Serpent...</li><li>Twofish...</li><li>DESX...</li><li>DESL...</li><li>DESXL...</li></ul></li></ul></li><li>AES (selbstextrahierend)...</li><li>Asymmetrisch<ul style="list-style-type: none"><li>RSA-Verschlüsselung...</li><li>RSA-Entschlüsselung...</li><li>RSA-Demo...</li></ul></li><li>Hybrid<ul style="list-style-type: none"><li>RSA-AES-Verschlüsselung...</li><li>RSA-AES-Entschlüsselung...</li><li>ECC-AES-Verschlüsselung...</li><li>ECC-AES-Entschlüsselung...</li></ul></li></ul>	<ul style="list-style-type: none"><li>PKI<ul style="list-style-type: none"><li>Schlüssel erzeugen/importieren ...</li><li>Schlüssel anzeigen/exportieren ...</li></ul></li><li>Dokument signieren...</li><li>Signatur überprüfen...</li><li>Signatur extrahieren</li><li>Signatordemo (Signaturerzeugung)...</li></ul>	<ul style="list-style-type: none"><li>Hashverfahren<ul style="list-style-type: none"><li>MD2</li><li>MD4</li><li>MD5</li><li>SHA</li><li>SHA-1</li><li>SHA-256</li><li>SHA-512</li><li>RIPEMD-160</li><li>Hashwert einer Datei...</li><li>Hash-Demo...</li><li>Schlüssel aus Passwort generieren (PKCS #5)...</li><li>Generieren von MACs...</li></ul></li><li>RSA-Kryptosystem<ul style="list-style-type: none"><li>Primzahltest...</li><li>Primzahlen generieren...</li><li>Faktorisieren einer Zahl...</li><li>RSA-Demo...</li><li>Signatordemo (Signaturerzeugung)...</li><li>Gitterbasierte Angriffe auf RSA<ul style="list-style-type: none"><li>Faktorisieren mit teilweise bekanntem p...</li><li>Angriff auf stereotype Nachrichten...</li><li>Angriff auf kleine geheime Schlüssel...</li></ul></li></ul></li><li>Protokolle<ul style="list-style-type: none"><li>Diffie-Hellman-Demo...</li><li>Authentisierungsverfahren im Netz...</li></ul></li><li>Anwendungen des Chinesischen Restsatzes<ul style="list-style-type: none"><li>Astronomie und Planetenbewegung...</li><li>Modulare Hin- und Rücktransformation...</li><li>Secret Sharing mittels CRT...</li></ul></li><li>Visualisierung von Algorithmen<ul style="list-style-type: none"><li>Caesar...</li><li>Vigenère...</li><li>Nihilist...</li><li>DES...</li><li>AES<ul style="list-style-type: none"><li>Rijndael-Animation...</li><li>Rijndael-Inspektor...</li></ul></li><li>Enigma...</li></ul></li><li>Secret-Sharing-Demo (nach Shamir)...</li><li>Tools<ul style="list-style-type: none"><li>Codierungen<ul style="list-style-type: none"><li>Base64-Codierung/Decodierung<ul style="list-style-type: none"><li>Base64 codieren</li><li>Base64 decodieren</li></ul></li><li>UU-Codierung/Decodierung<ul style="list-style-type: none"><li>UU codieren</li><li>UU decodieren</li></ul></li><li>ASN.1-Decodieren eines Dokuments</li></ul></li><li>Komprimieren<ul style="list-style-type: none"><li>Zip</li><li>UnZip</li></ul></li><li>Zufallsdaten erzeugen...</li><li>Passwort-Qualitätsmesser...</li><li>Passwort-Entropie...</li><li>Textdokument formatieren...</li></ul></li><li>Lernspiele<ul style="list-style-type: none"><li>Der Zahlenhai</li></ul></li><li>Zahlentheorie interaktiv<ul style="list-style-type: none"><li>Lernprogramm für Zahlentheorie...</li><li>Punktaddition auf Elliptischen Kurven...</li></ul></li></ul>	<ul style="list-style-type: none"><li>Werkzeuge zur Analyse<ul style="list-style-type: none"><li>Entropie</li><li>Gleitende Häufigkeit</li><li>Histogramm</li><li>N-Gramm...</li><li>Autokorrelation</li><li>Periode</li></ul></li><li>Symmetrische Verschlüsselung (klassisch)<ul style="list-style-type: none"><li>Ciphertext-Only<ul style="list-style-type: none"><li>Caesar</li><li>Vigenère</li><li>ADFGVX...</li><li>Substitution</li><li>Solitaire</li><li>Byteweise Addition</li><li>XOR</li></ul></li><li>Known-Plaintext<ul style="list-style-type: none"><li>Hill...</li></ul></li><li>Manuelle Analyse<ul style="list-style-type: none"><li>Substitution...</li><li>Playfair...</li><li>Solitaire</li></ul></li></ul></li><li>Symmetrische Verschlüsselung (modern)<ul style="list-style-type: none"><li>IDEA...</li><li>RC2...</li><li>RC4...</li><li>DES (ECB)...</li><li>DES (CBC)...</li><li>Triple DES (ECB)...</li><li>Triple DES (CBC)...</li><li>Rijndael (AES)...</li><li>Weitere Algorithmen<ul style="list-style-type: none"><li>MARS...</li><li>RC6...</li><li>Serpent...</li><li>Twofish...</li><li>DESX...</li><li>DESL...</li><li>DESXL...</li></ul></li></ul></li><li>Asymmetrische Verfahren<ul style="list-style-type: none"><li>Faktorisieren einer Zahl...</li><li>Gitterbasierte Angriffe auf RSA<ul style="list-style-type: none"><li>Faktorisieren mit teilweise bekanntem p...</li><li>Angriff auf stereotype Nachrichten...</li><li>Angriff auf kleine geheime Schlüssel...</li></ul></li><li>Seitenkanalangriff auf "Textbook-RSA" ...</li></ul></li><li>Hashverfahren<ul style="list-style-type: none"><li>Angriff auf den Hashwert der digitalen Signatur ...</li></ul></li><li>Zufallsanalyse<ul style="list-style-type: none"><li>Frequency-Test</li><li>Poker-Test</li><li>Runs-Test</li><li>Serial-Test</li><li>FIPS PUB-140-1 Testbatterie</li><li>Vitany</li><li>3D-Visualisierung...</li></ul></li></ul>	<ul style="list-style-type: none"><li>Grafikoptionen...</li><li>Analyseoptionen...</li><li>Textoptionen...</li><li>Startoptionen...</li><li>Weitere Optionen...</li></ul>	<ul style="list-style-type: none"><li>Überlappend anordnen</li><li>Nichtüberlappend anordnen</li><li>Symbole anordnen</li><li>Alle schließen</li></ul>	<ul style="list-style-type: none"><li>Startseite</li><li>Index</li><li>Szenarien (Tutorials)</li><li>Readme</li><li>Skript</li><li>Präsentation</li><li>Über CrypTool</li></ul>