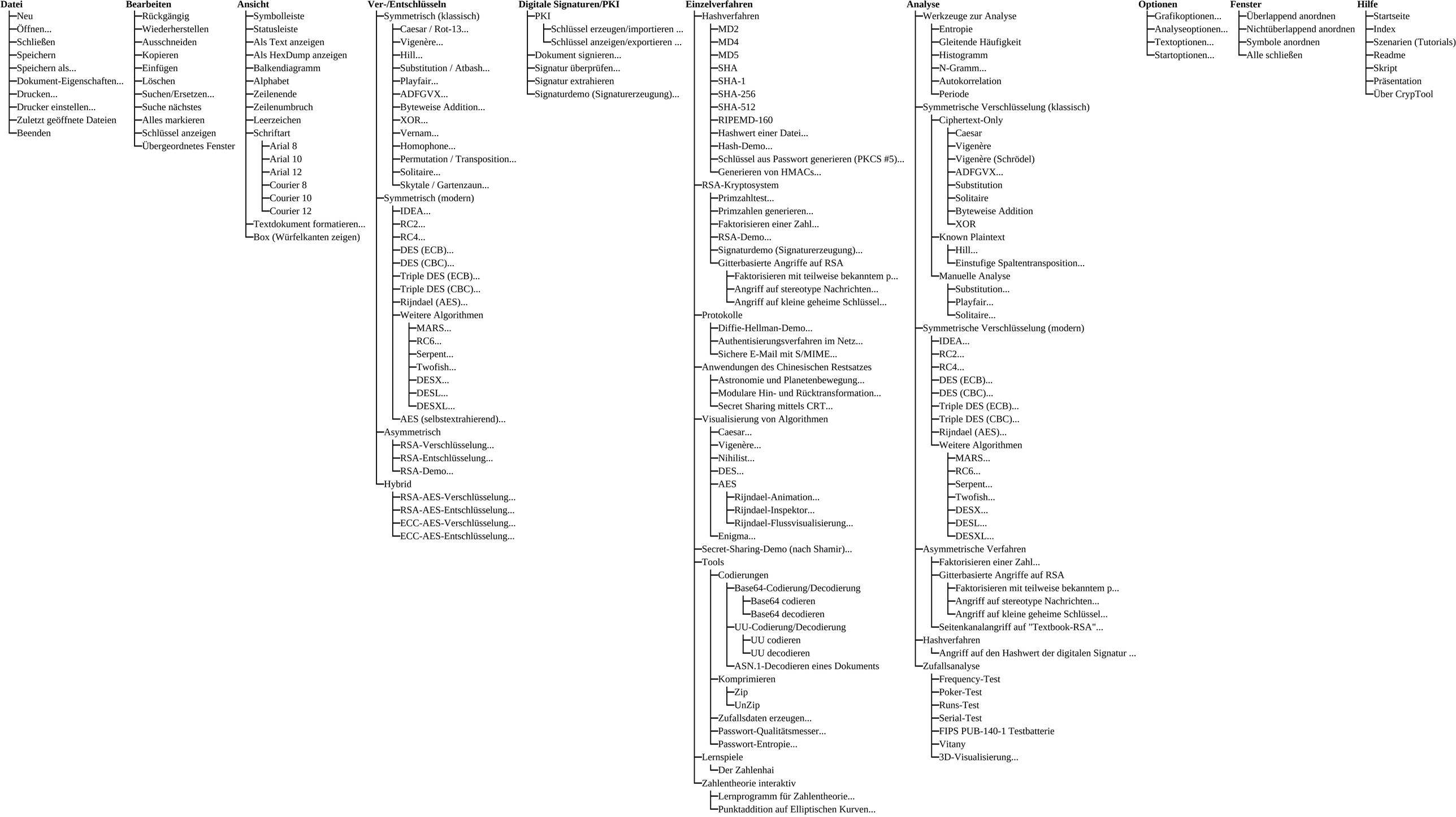
Datei
Neu
Öffnen...
Schließen
Speichern
Speichern als...
Dokument-Eigenschaften...
Drucken...
Drucker einstellen...
Zuletzt geöffnete Dateien
Beenden
Bearbeiten
Rückgängig
Wiederherstellen
Ausschneiden
Kopieren
Einfügen
Löschen
Suchen/Ersetzen...
Suche nächstes
Alles markieren
Schlüssel anzeigen
Übergeordnetes Fenster
Ansicht
Symbolleiste
Statusleiste
Als Text anzeigen
Als HexDump anzeigen
Balkendiagramm
Alphabet
Zeilenende
Zeilenumbruch
Leerzeichen
Schriftart
Arial 8
Arial 10
Arial 12
Courier 8
Courier 10
Courier 12
Textdokument formatieren...
Box (Würfelkanten zeigen)
Ver-/Entschlüsseln
Symmetrisch (klassisch)
Caesar / Rot-13...
Vigenère...
Hill...
Substitution / Atbash...
Playfair...
ADFGVX...
Byteweise Addition...
XOR...
Vernam...
Homophone...
Permutation / Transposition...
Solitaire...
Skytale / Gartenzaun...
Symmetrisch (modern)
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
Rijndael (AES)...
Weitere Algorithmen
MARS...
RC6...
Serpent...
Twofish...
DESX...
DESL...
DESXL...
AES (selbstextrahierend)...
Asymmetrisch
RSA-Verschlüsselung...
RSA-Entschlüsselung...
RSA-Demo...
Hybrid
RSA-AES-Verschlüsselung...
RSA-AES-Entschlüsselung...
ECC-AES-Verschlüsselung...
ECC-AES-Entschlüsselung...
Digitale Signaturen/PKI
PKI
Schlüssel erzeugen/importieren ...
Schlüssel anzeigen/exportieren ...
Dokument signieren...
Signatur überprüfen...
Signatur extrahieren
Signaturdemo (Signaturerzeugung)...
Einzelverfahren
Hashverfahren
MD2
MD4
MD5
SHA
SHA-1
SHA-256
SHA-512
RIPEMD-160
Hashwert einer Datei...
Hash-Demo...
Schlüssel aus Passwort generieren (PKCS #5)...
Generieren von HMACs...
RSA-Kryptosystem
Primzahltest...
Primzahlen generieren...
Faktorisieren einer Zahl...
RSA-Demo...
Signaturdemo (Signaturerzeugung)...
Gitterbasierte Angriffe auf RSA
Faktorisieren mit teilweise bekanntem p...
Angriff auf stereotype Nachrichten...
Angriff auf kleine geheime Schlüssel...
Protokolle
Diffie-Hellman-Demo...
Authentisierungsverfahren im Netz...
Sichere E-Mail mit S/MIME...
Anwendungen des Chinesischen Restsatzes
Astronomie und Planetenbewegung...
Modulare Hin- und Rücktransformation...
Secret Sharing mittels CRT...
Visualisierung von Algorithmen
Caesar...
Vigenère...
Nihilist...
DES...
AES
Rijndael-Animation...
Rijndael-Inspektor...
Rijndael-Flussvisualisierung...
Enigma...
Secret-Sharing-Demo (nach Shamir)...
Tools
Codierungen
Base64-Codierung/Decodierung
Base64 codieren
Base64 decodieren
UU-Codierung/Decodierung
UU codieren
UU decodieren
ASN.1-Decodieren eines Dokuments
Komprimieren
Zip
UnZip
Zufallsdaten erzeugen...
Passwort-Qualitätsmesser...
Passwort-Entropie...
Lernspiele
Der Zahlenhai
Zahlentheorie interaktiv
Lernprogramm für Zahlentheorie...
Punktaddition auf Elliptischen Kurven...
Analyse
Werkzeuge zur Analyse
Entropie
Gleitende Häufigkeit
Histogramm
N-Gramm...
Autokorrelation
Periode
Symmetrische Verschlüsselung (klassisch)
Ciphertext-Only
Caesar
Vigenère
Vigenère (Schrödel)
ADFGVX...
Substitution
Solitaire
Byteweise Addition
XOR
Known Plaintext
Hill...
Einstufige Spaltentransposition...
Manuelle Analyse
Substitution...
Playfair...
Solitaire...
Symmetrische Verschlüsselung (modern)
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
Rijndael (AES)...
Weitere Algorithmen
MARS...
RC6...
Serpent...
Twofish...
DESX...
DESL...
DESXL...
Asymmetrische Verfahren
Faktorisieren einer Zahl...
Gitterbasierte Angriffe auf RSA
Faktorisieren mit teilweise bekanntem p...
Angriff auf stereotype Nachrichten...
Angriff auf kleine geheime Schlüssel...
Seitenkanalangriff auf "Textbook-RSA"...
Hashverfahren
Angriff auf den Hashwert der digitalen Signatur ...
Zufallsanalyse
Frequency-Test
Poker-Test
Runs-Test
Serial-Test
FIPS PUB-140-1 Testbatterie
Vitany
3D-Visualisierung...
Optionen
Grafikoptionen...
Analyseoptionen...
Textoptionen...
Startoptionen...
Fenster
Überlappend anordnen
Nichtüberlappend anordnen
Symbole anordnen
Alle schließen
Hilfe
Startseite
Index
Szenarien (Tutorials)
Readme
Skript
Präsentation
Über CrypTool