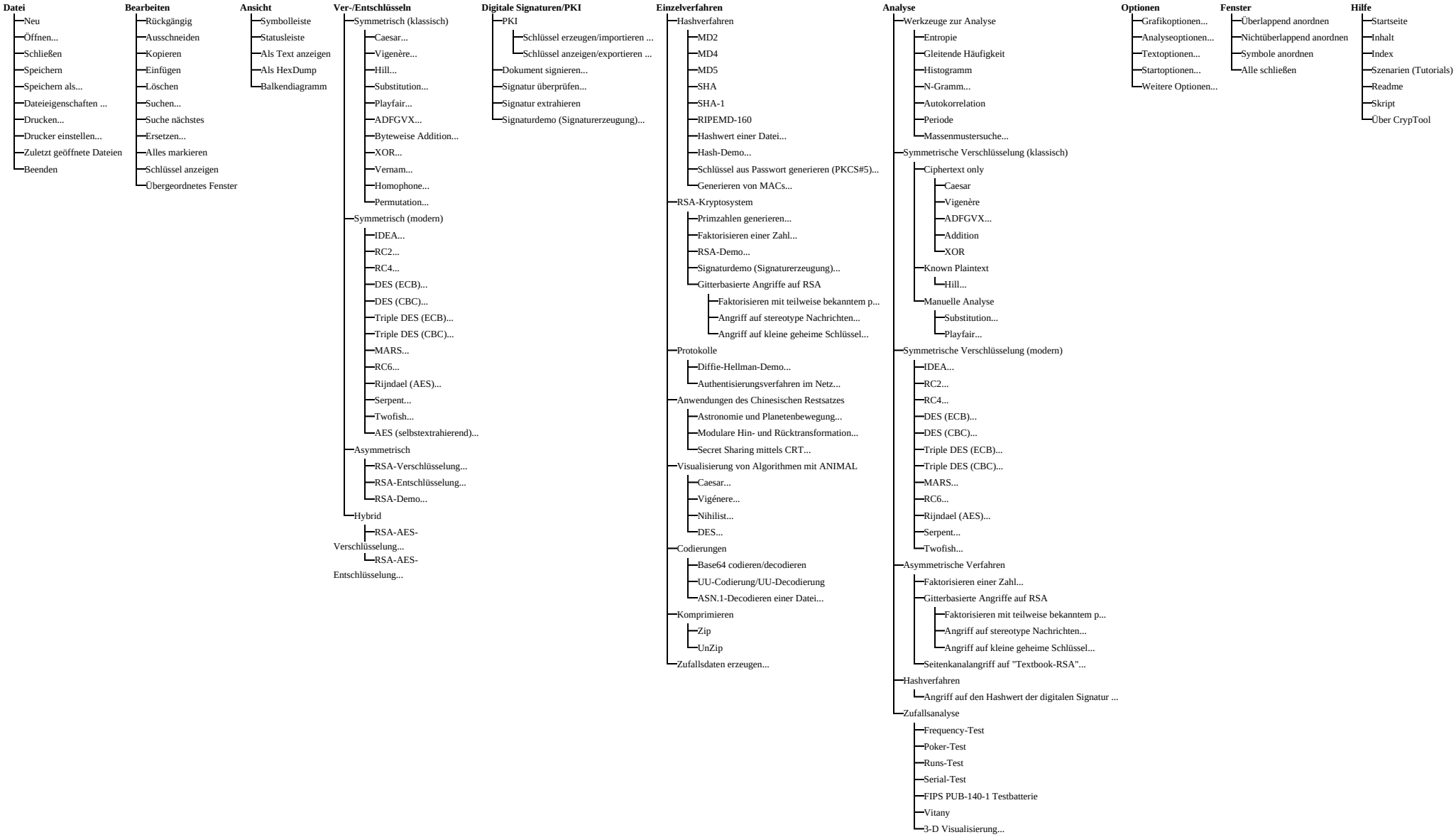
Datei
Neu
Öffnen...
Schließen
Speichern
Speichern als...
Dateieigenschaften ...
Drucken...
Drucker einstellen...
Zuletzt geöffnete Dateien
Beenden
Bearbeiten
Rückgängig
Ausschneiden
Kopieren
Einfügen
Löschen
Suchen...
Suche nächstes
Ersetzen...
Alles markieren
Schlüssel anzeigen
Übergeordnetes Fenster
Ansicht
Symbolleiste
Statusleiste
Als Text anzeigen
Als HexDump
Balkendiagramm
Ver-/Entschlüsseln
Symmetrisch (klassisch)
Caesar...
Vigenère...
Hill...
Substitution...
Playfair...
ADFGVX...
Byteweise Addition...
XOR...
Vernam...
Homophone...
Permutation...
Symmetrisch (modern)
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
MARS...
RC6...
Rijndael (AES)...
Serpent...
Twofish...
AES (selbstextrahierend)...
Asymmetrisch
RSA-Verschlüsselung...
RSA-Entschlüsselung...
RSA-Demo...
Hybrid
RSA-AES-Verschlüsselung...
RSA-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
RIPEMD-160
Hashwert einer Datei...
Hash-Demo...
Schlüssel aus Passwort generieren (PKCS#5)...
Generieren von MACs...
RSA-Kryptosystem
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...
Anwendungen des Chinesischen Restsatzes
Astronomie und Planetenbewegung...
Modulare Hin- und Rücktransformation...
Secret Sharing mittels CRT...
Visualisierung von Algorithmen mit ANIMAL
Caesar...
Vigénere...
Nihilist...
DES...
Codierungen
Base64 codieren/decodieren
UU-Codierung/UU-Decodierung
ASN.1-Decodieren einer Datei...
Komprimieren
Zip
UnZip
Zufallsdaten erzeugen...
Analyse
Werkzeuge zur Analyse
Entropie
Gleitende Häufigkeit
Histogramm
N-Gramm...
Autokorrelation
Periode
Massenmustersuche...
Symmetrische Verschlüsselung (klassisch)
Ciphertext only
Caesar
Vigenère
ADFGVX...
Addition
XOR
Known Plaintext
Hill...
Manuelle Analyse
Substitution...
Playfair...
Symmetrische Verschlüsselung (modern)
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
MARS...
RC6...
Rijndael (AES)...
Serpent...
Twofish...
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
3-D Visualisierung...
Optionen
Grafikoptionen...
Analyseoptionen...
Textoptionen...
Startoptionen...
Weitere Optionen...
Fenster
Überlappend anordnen
Nichtüberlappend anordnen
Symbole anordnen
Alle schließen
Hilfe
Startseite
Inhalt
Index
Szenarien (Tutorials)
Readme
Skript
Über CrypTool