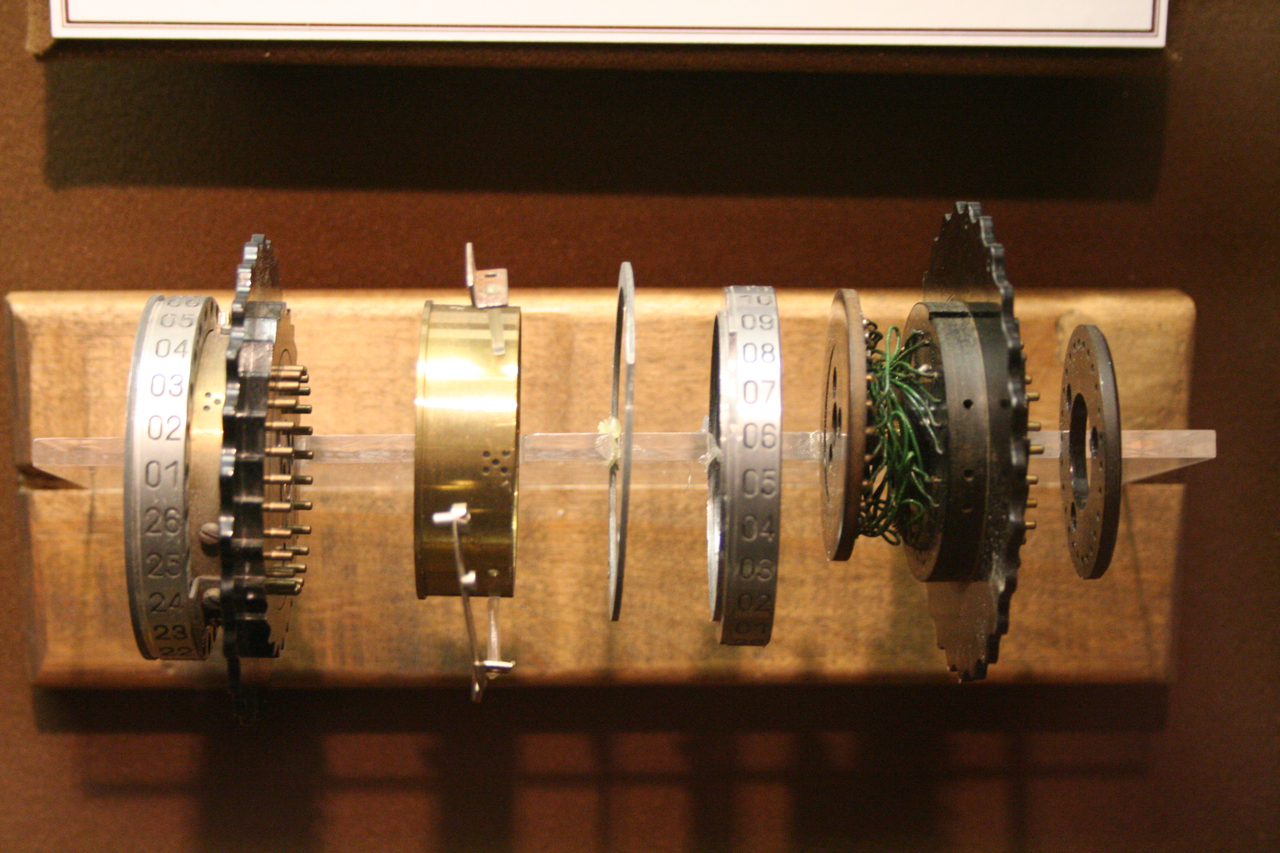
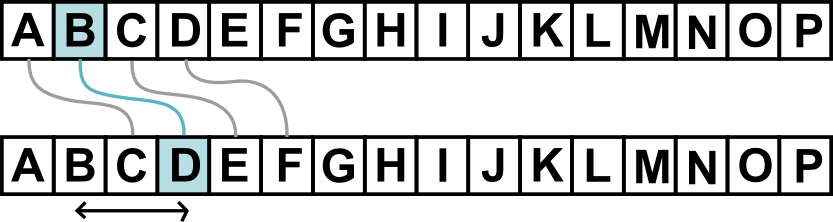
## Die Alberti-Chiffrierscheibe



## Rotor-Chiffriermaschine Enigma



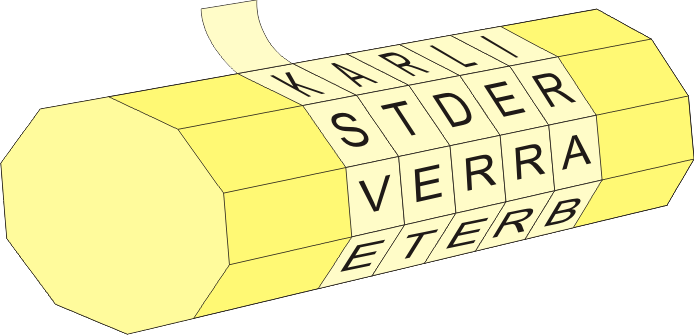
## Cäsar-Chiffre



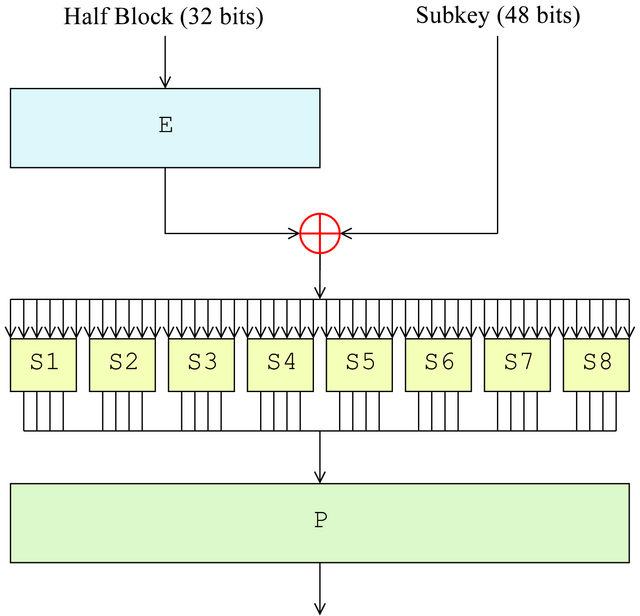
Falls zum Beispiel d = 3, dann:

A 🡪 D, ...

## Verschlüsselung mit Skytale

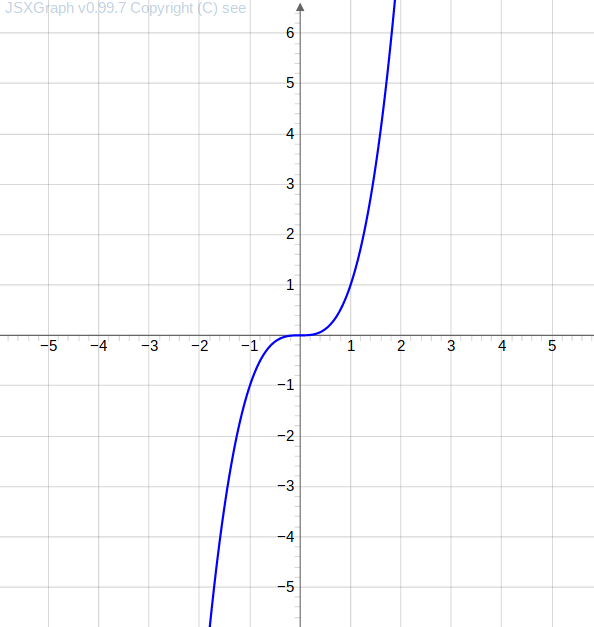


## DES-F-Funktion

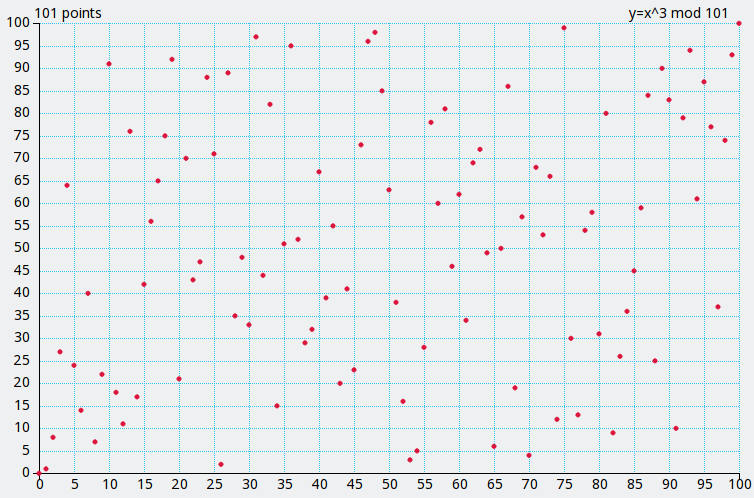


|  |  |
| --- | --- |
| Half block (32 bits) | Halber Block (32 Bit) |
| Subkey (48 bits) | Teilschlüssel (48 Bit) |

## Die Parabel der kubischen Funktion x ↦x3

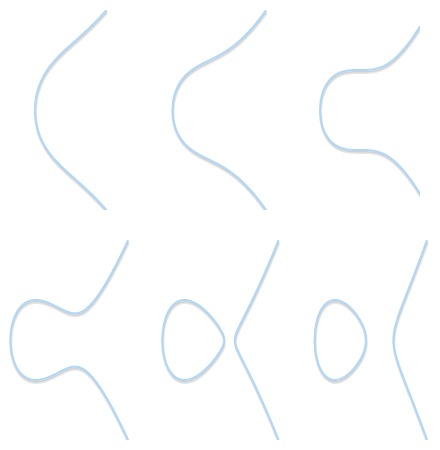


## Der Graph der kubischen Funktion Y = X3 über ℤ / 101 ℤ

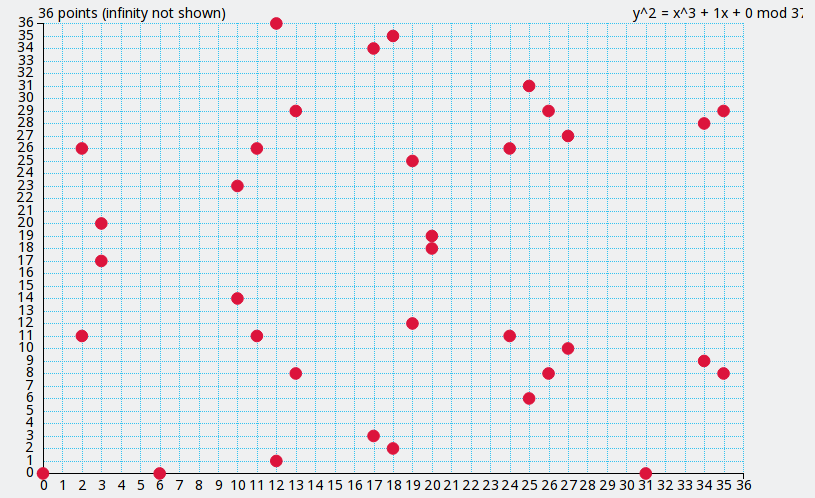


|  |  |
| --- | --- |
| 101 Points | 101 Punkte |

## Reelle elliptische Kurven

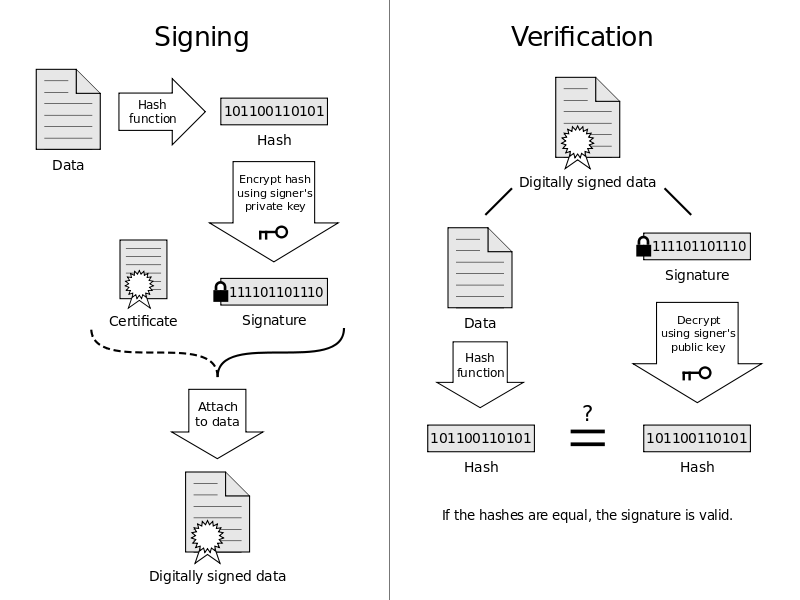


## Endliche elliptische Kurve



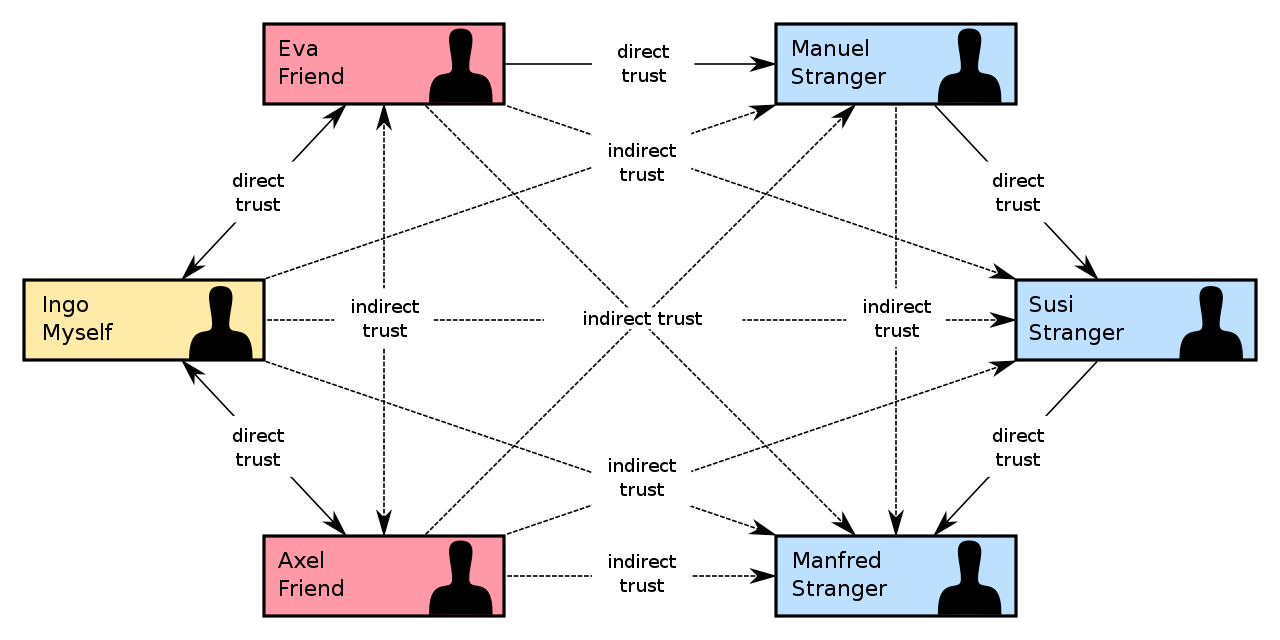
|  |  |
| --- | --- |
| 36 points (infinity not shown) | 36 Punkte (Unendlichkeit nicht dargestellt) |

## Digitale Signatur eines Dokuments und ihre Überprüfung



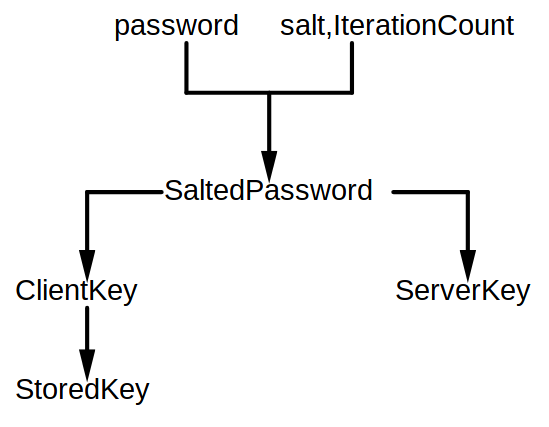
|  |  |
| --- | --- |
| Signing | Signatur |
| data | Daten |
| hash function | Hashfunktion |
| hash | Hash |
| encrypt hash using signer’s private key | Hash mit dem privaten Schlüssel des Unterzeichners verschlüsseln |
| signature | Signatur |
| certificate | Zertifikat |
| attach to data | An Daten anhängen |
| digitally signed data | Digital signierte Daten |
| Verification | Verifizierung |
| decrypt using signer’s public key | Entschlüsselung mit dem öffentlichen Schlüssel des Unterzeichners |
| If the hashes are equal, the signature is valid. | Wenn die Hashes gleich sind, ist die Signatur gültig. |

## Web of Trust



|  |  |
| --- | --- |
| friend | Freund(in) |
| direct trust | direktes Vertrauen |
| stranger | Fremde(r) |
| indirect trust | indirektes Vertrauen |
| myself | Ich |

## Abhängigkeitsdiagramm – jede orientierte Kante ist die Ausgabe einer Einwegfunktion



|  |  |
| --- | --- |
| password | Passwort |
| salt, iteration count | Salt, Anzahl der Iterationen |
| salted password | Passwort mit Salt |
| client key | Client-Schlüssel |
| server key | Server-Schlüssel |
| stored key | gespeicherter Schlüssel |

## Ausgehende Differenzen ΔY für drei eingehende Differenzen ΔX (horizontal aufgelistet) und alle möglichen Eingaben X (vertikal aufgelistet)

|  |  |  |  |
| --- | --- | --- | --- |
| [X / Δ X | 1011 | 1000 | 0100 |
| 0000 | 0010 | 1101 | 1100 |
| 0001 | 0010 | 1110 | 1011 |
| 0010 | 0111 | 0101 | 0110 |
| 0011 | 0010 | 1011 | 1001 |
| 0100 | 0101 | 0111 | 1100 |
| 0101 | 1111 | 0110 | 1011 |
| 0110 | 0010 | 1011 | 0110 |
| 0111 | 1101 | 1111 | 1001 |
| 1000 | 0010 | 1101 | 0110 |
| 1001 | 0111 | 1110 | 0011 |
| 1010 | 0010 | 0101 | 0110 |
| 1011 | 0010 | 1011 | 1011 |
| 1100 | 1101 | 0111 | 0110 |
| 1101 | 0010 | 0110 | 0011 |
| 1110 | 1111 | 1011 | 0110 |
| 1111 | 0101 | 1111 | 1011 |

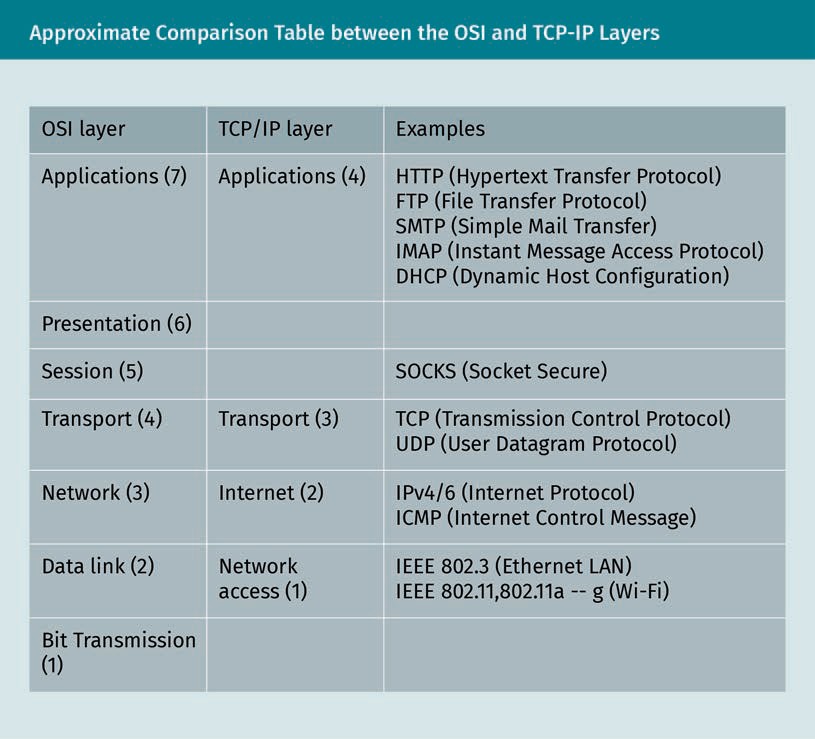
## Häufigkeit der ausgehenden Differenzen ΔY (horizontal aufgelistet) für einige eingehende Differenzen ΔX (vertikal aufgelistet)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ΔX / ΔY | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 4 | 0 | 4 | 2 | 0 | 0 |
| 2 | 0 | 0 | 0 | 2 | 0 | 6 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 |
| A | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 0 | 2 | 0 | 0 | 4 | 0 |
| B | 0 | 0 | 8 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 |
| F | 0 | 2 | 0 | 0 | 6 | 0 | 0 | 0 | 0 | 4 | 0 | 2 | 0 | 0 | 2 | 0 |

## Substitutionswahrscheinlichkeit

|  |  |  |  |
| --- | --- | --- | --- |
| Substitution | Ein | Aus | Wahrscheinlichkeit |
| S12 | B | 2 | 8/16 |
| S23 | 4 | 6 | 6/16 |
| S32 | 2 | 5 | 6/16 |
| S33 | 2 | 5 | 6/16 |

## Tabelle für den ungefähren Vergleich zwischen den OSI- und TCP-IP-Schichten

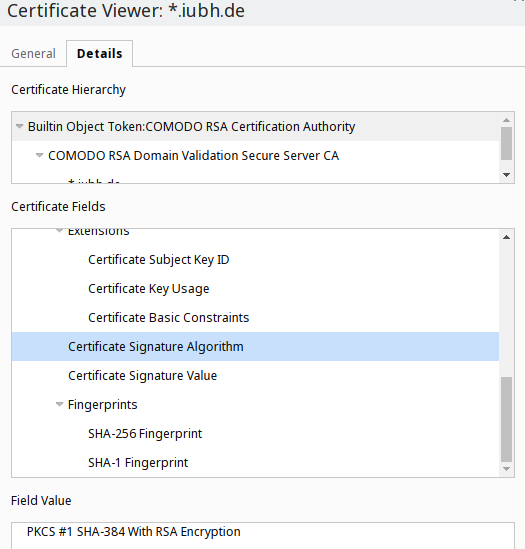


|  |  |
| --- | --- |
| OSI layer | OSI-Schicht |
| Applications (7) | Anwendungen (7) |
| Presentation (6) | Darstellung (6) |
| Session (5) | Sitzung (5) |
| Transport (4) | Transport (4) |
| Network (3) | Vermittlung (3) |
| Data link (2) | Sicherung (2) |
| Bit transmission (1) | Bitübertragung (1) |
| TCP/IP layer | TCP/IP-Schicht |
| Applications (4) | Anwendungen (4) |
| Transport (3) | Transport (3) |
| Internet (2) | Internet (2) |
| Network access (1) | Netzwerkzugang (1) |
| Examples | Beispiele |
| HTTP (hypertext transfer protocol) | HTTP (HyperText Transfer Protocol) |
| FTP (file transfer protocol) | FTP (File Transfer Protocol) |
| SMTP (simple mail transfer) | SMTP (Simple Mail Transfer Protocol) |
| IMAP (instant message access protocol) | IMAP (Instant Message Access Protocol) |
| DHCP (dynamic host configuration) | DHCP (Dynamic Host Configuration) |
| SOCKS (socket secure) | SOCKS (Socket Secure) |
| TCP (transmission control protocol) | TCP (Transmission Control Protocol) |
| UDP (user diagram protocol) | UDP (User Diagram Protocol) |
| IPv4/6 (internet protocol) | IPv4/6 (Internet Protocol) |
| ICMP (internet control message) | ICMP (Internet Control Message) |
| IEEE 802.3 (ethernet LAN) | IEEE 802.3 (Ethernet-LAN) |
| IEEE 802.11, 802.11a—g (Wi-Fi) | IEEE 802.11, 802.11a–g (WLAN) |

## Übliche Ports bekannter Protokolle

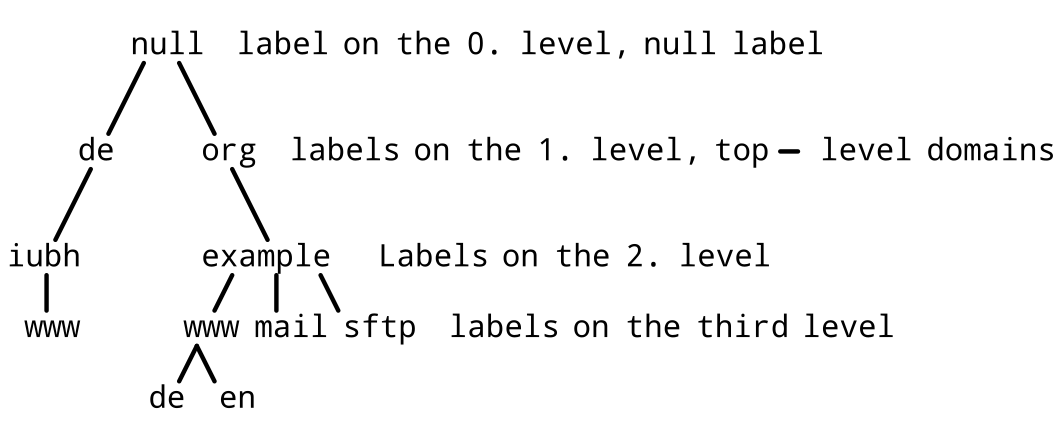
|  |  |
| --- | --- |
| Port | Port |
| Protocol | Protokoll |
| FTP The file transfer protocol control | FTP: Die Steuerung des File Transfer Protocol |
| SSH Secure logins, file transfers (scp, sftp) and port forwarding | SSH: Sichere Anmeldungen, Dateiübertragungen (scp, sftp) und Portweiterleitung |
| SMTP Simple Mail Transfer Protocol (E-mail) | SMTP: Simple Mail Transfer Protocol (E-Mail) |
| DNS Domain Name System | DNS: Domain Name System |
| HTTP HyperText Transfer Protocol (WWW) | HTTP: HyperText Transfer Protocol (WWW) |
| IMAP4 Internet Message Access Protocol (E-mail) | IMAP4: Internet Message Access Protocol (E-Mail) |
| HTTPS used for securely transferring web pages | HTTPS: Für die sichere Übertragung von Webseiten |

## Zertifikat X.509



|  |  |
| --- | --- |
| Certificate Viewer: \*.iu.org | Zertifikatsbetrachter: \*.iu.org |
| General | Allgemein |
| Details | Details |
| Certificate Heirarchy | Zertifikathierarchie |
| Builtin Object Token:COMODO RSA Certification Authority | Integriertes Objekt-Token: COMODO-RSA-Zertifizierungsstelle |
| COMODO RSA Domain Validation Secure Server CA | COMODO RSA Domain Validation Secure Server CA |
| Certificate Fields | Zertifikatsfelder |
| Extensions | Erweiterungen |
| Certificate Subject Key ID | Zertifikat-Betreff-Schlüssel-ID |
| Certificate Key Usage | Zertifikat-Schlüsselnutzung |
| Certificate Basic Constraints | Zertifikat: Grundlegende Beschränkungen |
| Certificate Signature Algorithm | Zertifikat-Signaturalgorithmus |
| Certificate Signature Value | Zertifikat-Signaturwert |
| Fingerprints | Fingerabdrücke |
| SHA-256 Fingerprint | SHA-256-Fingerabdruck |
| SHA-1 Fingerprint | SHA-1-Fingerabdruck |
| Field Value | Feldwert |
| PKCS #1 SHA-384 With RSA Encryption | PKCS #1 SHA-384 mit RSA-Verschlüsselung |

## FQDNs dargestellt als Pfade eines Baums



|  |  |
| --- | --- |
| null | null |
| de | de |
| org | org |
| iubh | iubh |
| example | Beispiel |
| www | www |
| mail | mail |
| sftp | sftp |
| de | de |
| en | en |
| label on the 0. level, null label | Kennzeichnung auf der 0. Ebene, null-Label |
| labels on the 1. level, top — level domains | Kennzeichnung auf der 1. Ebene, Top-Level-Domains |
| labels on the 2. level | Kennzeichnung auf der 2. Ebene |
| labels on the third level | Kennzeichnung auf der 3. Ebene |

## Nachrichten, die sich Knoten für Knoten durch ein gemischtes Netzwerk bewegen, während jeder von ihnen die mehrschichtige Verschlüsselung mit einem privaten Schlüssel entschlüsselt

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

## Farbkarte der Primärfarbabstufungen

