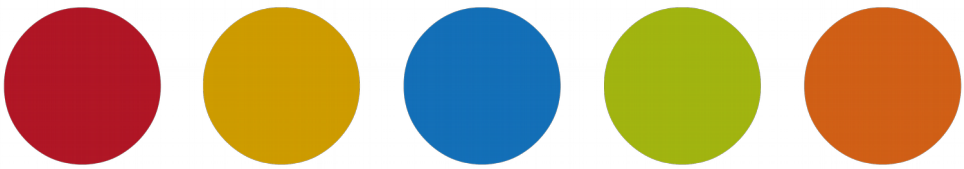
# Informatische Grundlagen

## Skript

Arbeitsmaterial

| | |
|---|---|
| Schulung: | Informatik und Wirtschaftsinformatik |

Stand: 19. Apr 2020





Christine Janischek
Berufliches Schulzentrum Wangen

## 1 Arbeitsplatzorganisation

# Arbeitsplatzorganisation

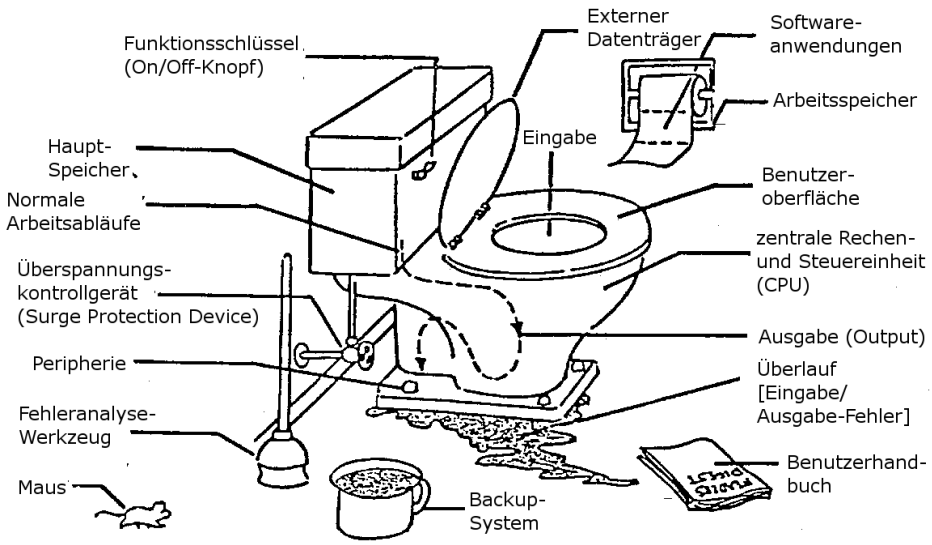
## Netzwerk, Workstation

| Thema: | Netzwerk, Arbeitsplatzrechner und Peripheriegeräte<br>Grundlagen Arbeitsplatz |
|---|---|

Ein Netzwerk besteht i.d.R. aus vielen Computern. Heutzutage werden diese Computer vielfach zentral verwaltet. Diese Schaltzentrale nennt sich Server. Bei kleinen Netzwerken reicht eine Schaltzentrale aus in großen Netzwerken existieren i.d.R. Viele Schaltzentralen, die sich die Arbeit teilen.

Informatiksysteme

## Computertechnologie Verstehen

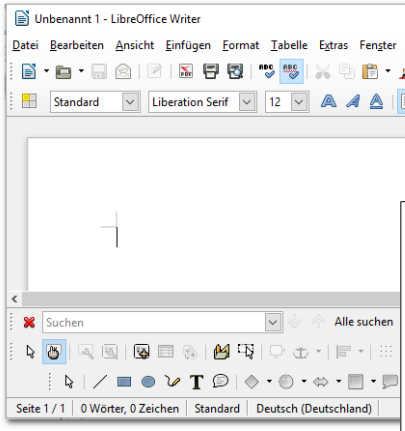



Ob Server oder Arbeitsplatzrechner die Bestandteile sind im Kern ähnlich >>gestrickt<<:

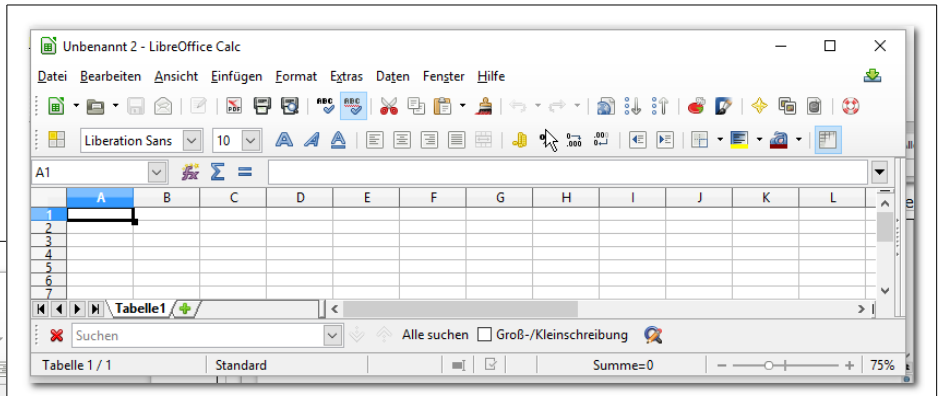
Arbeitsauftrag:

1. Identifizieren Sie so viele Arbeitsplatzbestandteile wie möglich.
   Erstellen Sie handschriftlich eine Mindmap (trennen Sie zwischen Arbeitsplatzrechner und Peripheriegeräten).
2. Melden Sie sich erstmals am Arbeitsplatz an und ändern Sie ihr Passwort.
3. Öffnen Sie über die Schaltfläche → Arbeitsplatz das Verzeichnis → Eigene Dateien.
4. Erzeugen Sie ein Unterrichtsverzeichnis (z. B. INF, WINF).
5. Übertragen Sie die Mindmap aus Aufgabe 1. in die Unterrichtsdokumentation.

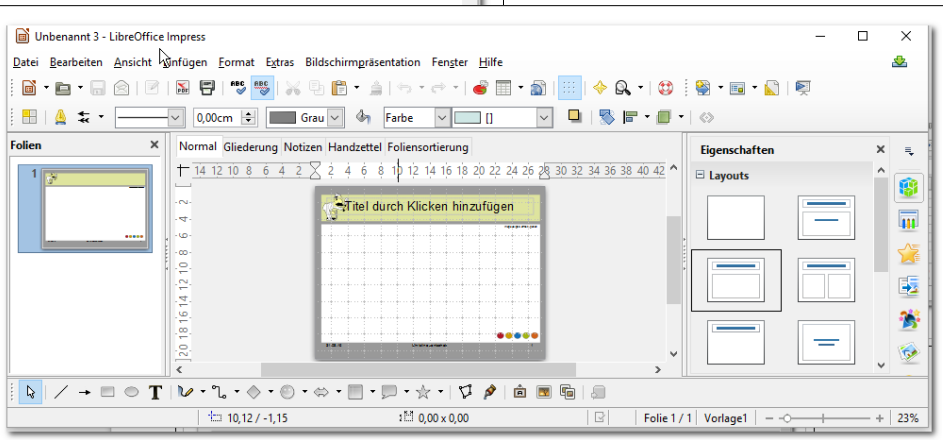
| Thema: | Arbeitsplatzorganisation<br>Grundlagen Office Pakete |
|---|---|




Textverarbeitung



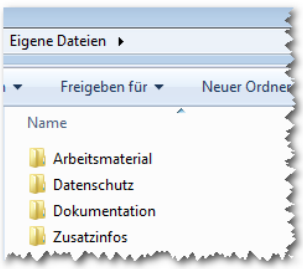

Tabellenkalkulation




Präsentationsprogramm

Arbeitsauftrag:

1. Öffnen Sie über die Schaltfläche → Arbeitsplatz das Verzeichnis → Eigene Dateien.
2. Erzeugen Sie darin die angezeigte Verzeichnisstruktur.
3. Kopieren Sie die Vorlage für die Unterrichtsdokumentation aus dem Verzeichnis Vorlage (→ Tauschverzeichnis) in das Verzeichnis Vorlage (→ Eigene Dateien).
4. Kopieren Sie die Datei → Noten.odt in das Verzeichnis → Zusatzinfos.
5. Welche Bedeutung hat die Dateiendung → .ott ?
6. Welche Dateiendungen verwenden andere Office Pakete?
7. Erzeugen Sie den Gliederungspunkt → Grundlagen in ihrer Unterrichtsdokumentation und dokumentieren Sie Ihre Vorgehensweisen und bezeichnen Sie alle Leisten des Textverarbeitungsprogrammes.
8. Welche Funktion übernimmt die Anwendung FSCapture?




Verzeichnis- oder Ordnerstruktur

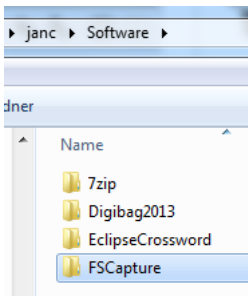
| Thema:  | Arbeitsplatzorganisation<br>Übung Grundlagen |
|---|---|

Übung

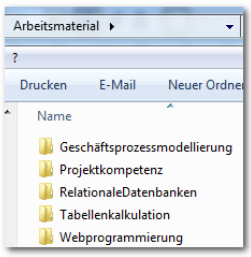
Arbeitsauftrag:

1. Öffnen Sie über die Schaltfläche → Arbeitsplatz das Laufwerk → Eigene Dateien.
2. Kopieren Sie die Software FSCapture in das Software-Verzeichnis in ihren eigenen Dateien.
3. Erzeugen Sie im Arbeitsmaterialverzeichnis die Unterordner (→ Ordnerstruktur)
4. Dokumentieren Sie diesen Vorgang ausführlich (Ordner anlegen).
5. Erzeugen Sie ein Datei (z.B. Textdatei).
6. Löschen Sie eine Datei (z.B. Textdatei).
7. Nutzen Sie den Gliederungspunkt → Grundlagen in ihrer Unterrichtsdokumentation und dokumentieren Sie den Vorgang mit Hilfe von FSCapture.
8. Aktualisieren Sie das Inhaltsverzeichnis Ihrer Unterrichtsdokumentation und dokumentieren Sie den Vorgang mit Hilfe von FSCapture.

FSCapture

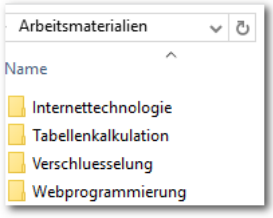



Verzeichnis- oder Ordnerstruktur



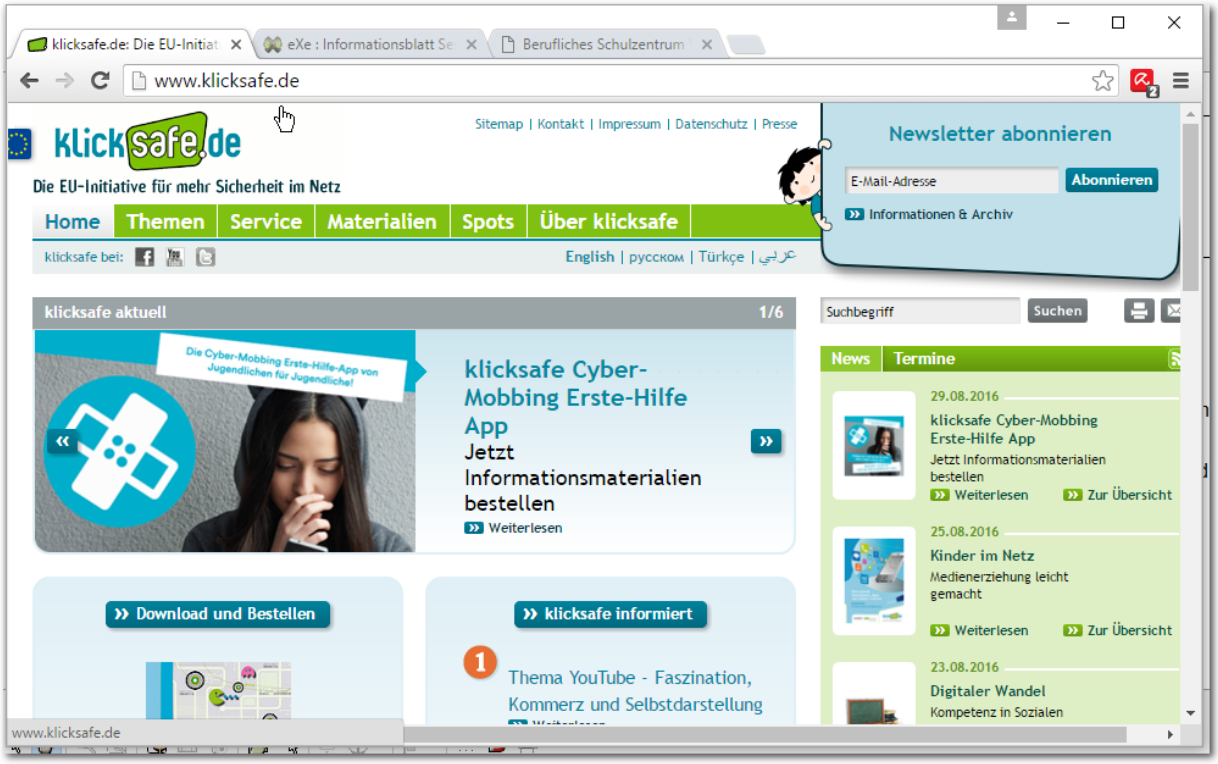

Themen im BK

Verzeichnis- oder Ordnerstruktur




Themen im WG

| Thema: | Angriffssicherheit (Security) und Betriebssicherheit (Safety)<br>Übung<br>* Unterrichtsmaterial zur vorläufigen Handreichung Wirtschaftsinformatik |
|---|---|




## Klicksafe Materialien

Arbeitsauftrag:

1. Recherchieren Sie auf den Seiten von Klicksafe die aktuelle Brochure zum Thema → Suchen im Internet, laden Sie sich das Dokument herunter und speichern Sie die Datei in Ihrem Arbeitsmaterialverzeichnis ab.
2. Recherchieren Sie auf den Seiten von Klicksafe die aktuelle Brochure zum Thema → Datenschutz und Persönlichkeitsrechte, laden Sie sich das Dokument herunter und speichern Sie die Datei in Ihrem Arbeitsmaterialverzeichnis ab.
3. Recherchieren Sie auf den Seiten von Klicksafe die aktuelle Brochure zum Thema → Internet Tipps für Jugendliche, laden Sie sich das Dokument herunter und speichern Sie die Datei in Ihrem Arbeitsmaterialverzeichnis ab.
4. Recherchieren Sie auf den Seiten von Klicksafe die aktuelle Brochure zum Thema → Nicht alles was geht, ist auch erlaubt, laden Sie sich das Dokument herunter und speichern Sie die Datei in Ihrem Arbeitsmaterialverzeichnis ab.

Studieren Sie die Dokumente und picken Sie sich ein Thema heraus das Sie persönlich interessiert. Notieren Sie das Thema und mindestens zwei wichtige thematische Aspekte (Erkenntnisse).

Zusatzaufgabe:

**Recherchieren Sie ein Dokument das für Ihre Eltern vermutlich interessant sein könnte, laden Sie sich das Dokument herunter und speichern Sie die Datei in Ihrem Arbeitsmaterialverzeichnis ab.**

## 2 Netze

# Netze

## Adressen, Protokolle,Dienste

| Thema: | Grundlagen der Internettechnologie<br>Information<br>* Unterrichtsmaterial zur vorläufigen Handreichung Wirtschaftsinformatik |
|---|---|

# Funktionsweise von Netzwerken

## Datennetze

Datennetze waren das Ergebnis von Geschäftsanwendungen, die für Mikrocomputer geschrieben wurden. Da die Mikrocomputer nicht miteinander verbunden waren, gab es keine effiziente Möglichkeit, Daten gemeinsam zu nutzen. Die Verwendung von Disketten war für Unternehmen kein rationelles oder kostengünstiges Mittel für den Austausch von Daten. Im so genannten „Turnschuhnetz“ wurden mehrere Kopien der Daten erstellt. Immer wenn eine Datei geändert wurde, musste sie erneut an alle übrigen Benutzer weitergegeben werden, die diese Datei benötigten. Wenn die Datei von zwei Benutzern geändert wurde und diese die Datei anschließend gemeinsam verwenden wollten, gingen die von einem der Benutzer vorgenommenen Änderungen verloren. Die Unternehmen benötigten eine Lösung für die folgenden drei Probleme:

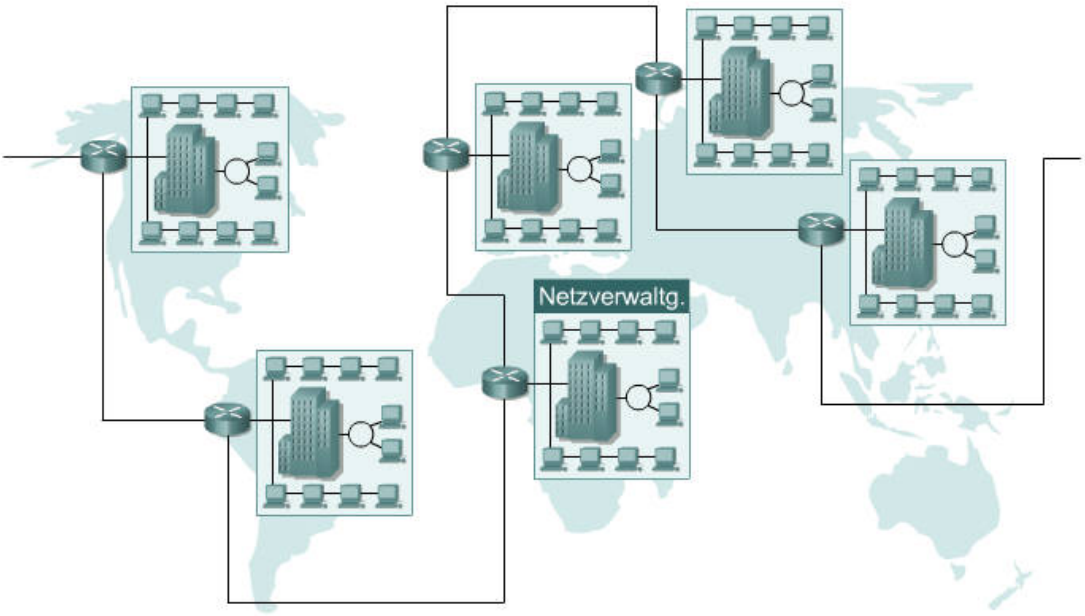
- Vermeiden unnötiger mehrfacher Beschaffung von Geräten und Ressourcen.
- Effiziente Kommunikation.
- Einrichten und Verwalten eines Netzes.

Die Unternehmen erkannten, dass mit Computernetzen die Produktivität erhöht und Kosten eingespart werden konnten. Nahezu ebenso schnell, wie neue Netztechnologien und -produkte aufkamen, wurden Netze eingerichtet und erweitert. Die erste Phase der Entwicklung von Netzen verlief ungeordnet. Zu Beginn der 80er Jahre fand jedoch ein enormer Aufschwung statt. Die Mitte der 80er Jahre entstandene Netztechnologien wurden in verschiedenen Hardware- und Software-Implementierungen erstellt. Jedes Unternehmen, das Hardware und Software für Netze herstellte, verwendete seine eigenen Standards. Diese individuellen Standards wurden wegen der Konkurrenz mit anderen Unternehmen entwickelt. Als Folge davon waren viele Netztechnologien untereinander nicht kompatibel. Die Kommunikation zwischen Netzen mit unterschiedlichen technischen Spezifikationen wurde immer schwieriger. Zur Implementierung neuer Technologien musste häufig die Netzausrüstung ausgetauscht werden.

Eine der ersten Lösungen hierfür war die Erstellung von Standards für lokale Netze (LANs). LAN-Standards enthielten einen offenen Satz von Richtlinien, an denen sich die Unternehmen bei der Erstellung der Hardware und Software für Netze orientierten. Dadurch wurde die von verschiedenen Unternehmen angebotene Ausrüstung kompatibel, und die LAN-Implementierungen wurden stabil.

Mit vereinzelten LANs ist jede Abteilung des Unternehmens eine kleine elektronische Insel. Je mehr Computer in den Unternehmen eingesetzt wurden, desto unzureichender wurden die LANs.

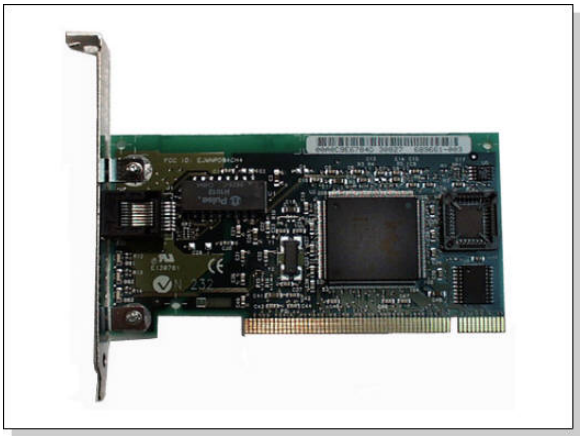
Eine neue Technologie wurde benötigt, um Informationen unternehmensintern und unternehmensübergreifend effizient und schnell gemeinsam nutzen zu können. Es wurden also Stadtnetze (Metropolitan Area Networks, MANs) und Weitverkehrsnetze (Wide Area Networks, WANs) angelegt. Da WANs die Netzteilnehmer eines großen geografischen Gebietes verbinden, konnten jetzt Unternehmen auch über große Entfernungen miteinander kommunizieren:




Komponenten eines Netzes

Komponenten, die direkt mit einem Netzsegment verbunden sind, werden als Geräte bezeichnet. Diese Geräte lassen sich in zwei Klassen einteilen. Die erste Klasse sind Endbenutzergeräte. Hierzu gehören Computer, Drucker, Scanner und andere Geräte, deren Dienste für den Benutzer direkt zur Verfügung stehen. Die zweite Klasse sind Netzkopplungselemente. Hierzu gehören alle Geräte, die Endbenutzergeräte untereinander verbinden, so dass diese miteinander kommunizieren können.

Endbenutzergeräte, über die die Benutzer eine Verbindung mit dem Netz herstellen, werden auch als Hosts bezeichnet. Mithilfe dieser Geräte können die Benutzer Informationen gemeinsam nutzen, erstellen und abrufen. Die Hostgeräte können auch ohne Netz arbeiten. Der Funktionsumfang ist jedoch ohne Netz erheblich eingeschränkt. Über Netzwerkkarten werden die Hostgeräte mit den Netzmedien verbunden. Diese Verbindung wird zum Senden von E-Mails, zum Drucken von Berichten, zum Scannen von Bildern oder für den Zugriff auf Datenbanken verwendet.

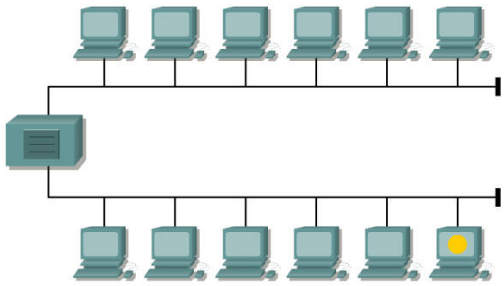


Eine Netzwerkkarte ist eine Leiterplatte, die in den Erweiterungssteckplatz am Bus einer Hauptplatine gesteckt wird. Es kann sich dabei auch um ein Peripheriegerät handeln. Netzwerkkarten werden gelegentlich als Netzadapter bezeichnet. Netzwerkkarten von Laptop- oder Notebook-Computern haben in der Regel die Größe einer PCMCIA-Karte. Jede Netzwerkkarte wird durch einen eindeutigen Code, die sogenannte MAC (Media Access Control)-Adresse, identifiziert. Mit dieser Adresse wird die Datenkommunikation für den Host im Netz gesteuert. Wie der Name schon sagt, steuert eine Netzwerkkarte den Zugriff des Hosts auf das Netz.

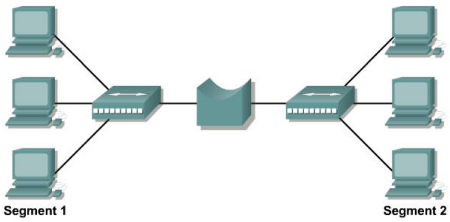
In der Netzwerkindustrie gibt es keine Standardsymbole für Endbenutzergeräte. Sie werden ähnlich wie die echten Geräte dargestellt, so dass sie ohne weiteres zu erkennen sind.

Netzkopplungselemente übernehmen den Transport der Daten, die zwischen den Endbenutzergeräten übertragen werden. Netzkopplungselemente dienen dazu, Kabelverbindungen zu verlängern, Verbindungen zu konzentrieren, Datenformate zu konvertieren und die Datenübertragung zu steuern. Repeater, Hubs, Bridges, Switches und Router sind Beispiele für Geräte, die diese Funktionen ausführen.

Ein **Repeater** ist ein Netzkopplungselement, das Signale auffrischt. Repeater frischen analoge oder digitale Signale auf, die durch Übertragungsverluste aufgrund von Dämpfung verzerrt wurden. Im Unterschied zu Routern eignen sich Repeater nicht für ein intelligentes Routing.

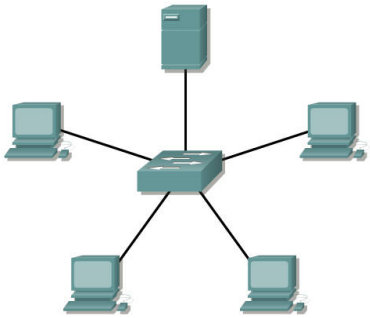


**Hubs** konzentrieren Verbindungen. Sie fassen eine Reihe von Hosts zu einer Gruppe zusammen, so dass sie im Netz als eine Einheit fungiert. Dies geschieht passiv; die Datenübertragung selbst bleibt davon unberührt. Aktive Hubs konzentrieren Hosts und frischen außerdem Signale auf.

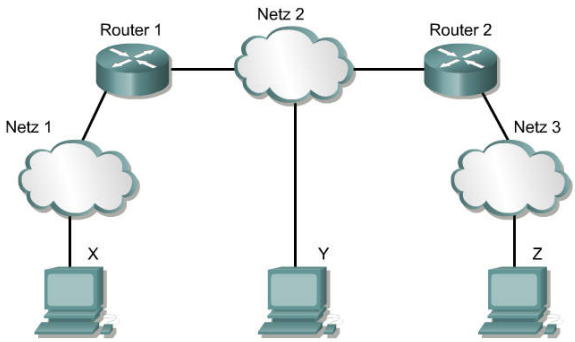



**Bridges** konvertieren Datenformate im Netz und übernehmen grundlegende Aufgaben der Datenübertragung. Über Bridges werden Verbindungen zwischen LANs hergestellt. Außerdem prüfen Bridges die Daten, um festzustellen, ob diese die Bridge passieren sollen. Auf diese Weise arbeiten die einzelnen Abschnitte des Netzes effizienter.

**Workgroup-Switches** verfügen ebenfalls über intelligente Funktionen für die Datenübertragung. Sie können feststellen, ob die Daten in einem LAN bleiben sollen, und übertragen Daten nur über die Verbindung, von der diese Daten angefordert werden. Ein weiterer Unterschied zwischen einer Bridge und einem Switch besteht darin, dass Datenübertragungsformate von einem Switch nicht konvertiert werden.

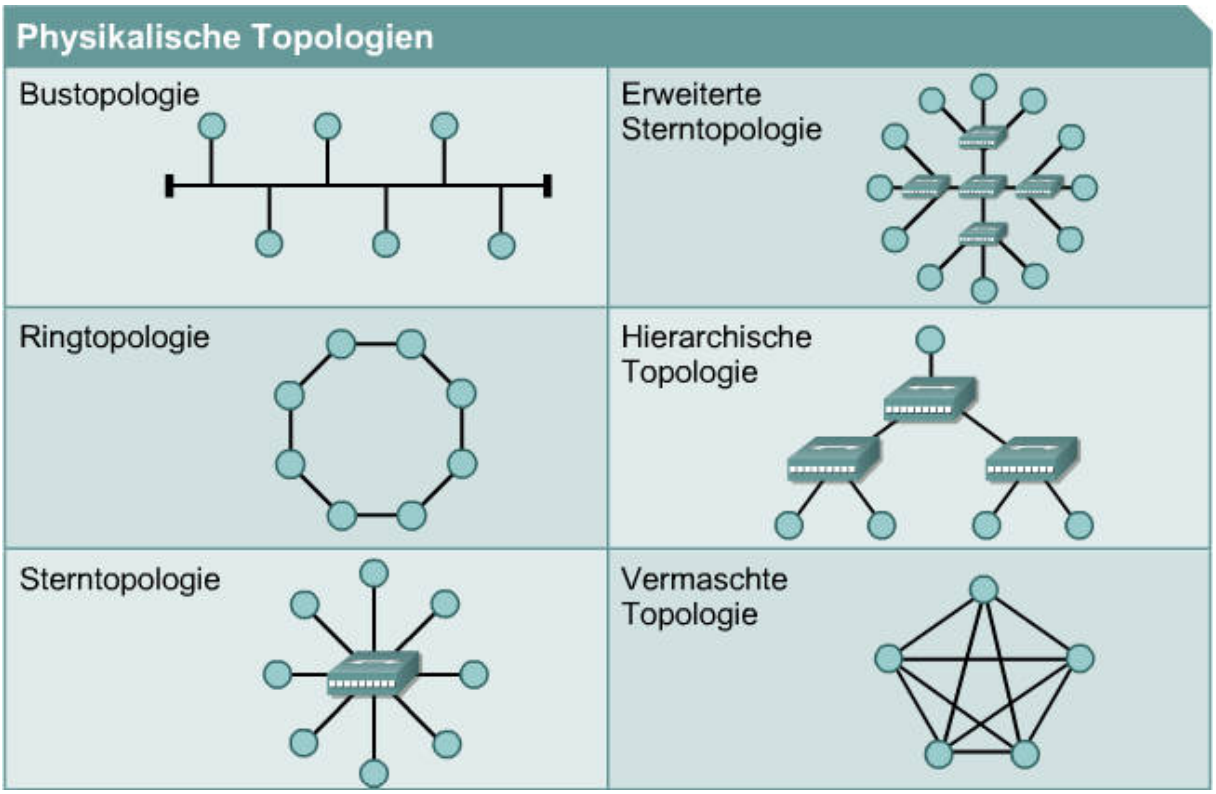


**Router** verfügen über alle oben genannten Fähigkeiten. Router können Signale auffrischen, mehrere Verbindungen konzentrieren, Datenübertragungsformate konvertieren und die Datenübertragung steuern. Sie können außerdem eine Verbindung mit einem WAN herstellen und somit LANs miteinander verbinden, die räumlich weit voneinander entfernt sind. Keines der anderen Geräte eignet sich für diese Art der Verbindung.



Netztopologien

Durch die Netztopologie wird die Struktur des Netzes definiert. Der eine Teil der Topologiedefinition ist die physikalische Topologie, die eigentliche Anordnung der Kabel oder Medien. Der andere Teil ist die logische Topologie, die bestimmt, wie die Hosts auf die Medien zugreifen, um Daten zu senden. In der Regel werden die folgenden physikalischen Topologien verwendet:



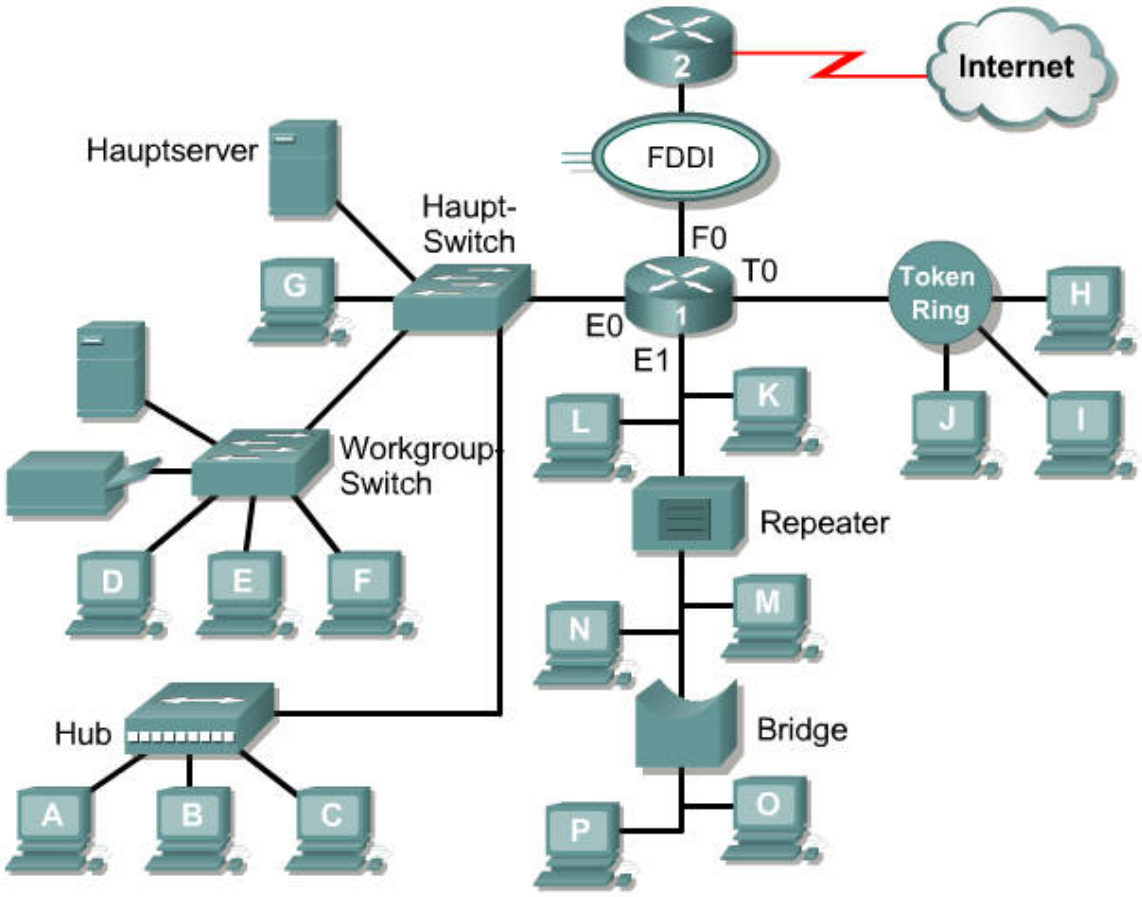

- Eine Bustopologie arbeitet mit einem einzelnen Backbone-Kabel, an dem überall Geräte angeschlossen werden. Alle Hosts werden direkt mit diesem Backbone verbunden.
- Eine Ringtopologie verbindet einen Host mit dem nächsten Host und den letzten Host mit dem ersten Host. Dadurch entsteht ein physikalischer Kabelring.
- In einer Sterntopologie sind alle Kabel mit einem zentralen Punkt verbunden.
- In einer erweiterten Sterntopologie werden einzelne Sterne über ihre Hubs oder Switches miteinander verknüpft. Durch diese Topologie lassen sich Umfang und Abdeckung des Netzes erweitern.
- Eine hierarchische Topologie ähnelt einer erweiterten Sterntopologie. Anstatt jedoch die Hubs oder Switches miteinander zu verknüpfen, wird das System an einen Computer gekoppelt, der den Verkehr innerhalb der Topologie steuert.
- Eine vermaschte Topologie soll einen möglichst weitgehenden Schutz vor der Unterbrechung von Diensten gewährleisten. Für die vernetzten Steuerungssysteme eines Kernkraftwerks könnte z. B. eine vermaschte Topologie verwendet werden. Wie Sie in der Grafik sehen, hat jeder Host seine eigenen Verbindungen mit allen anderen Hosts. Obwohl es im Internet viele Wege zu einem Standort gibt, wird hier nicht die voll vermaschte Topologie eingesetzt.

Die logische Topologie eines Netzes bestimmt, wie die Hosts über das Medium kommunizieren. Die beiden am häufigsten anzutreffenden Arten von logischen Topologien sind die Broadcast- und die Token-Passing-Topologie.

In einer Broadcast-Topologie sendet jeder Host seine Daten an alle anderen Hosts im Netzmedium. Es gibt keine feste Reihenfolge, in der die Stationen das Netz verwenden.

Die zweite logische Topologie ist die Token-Passing-Topologie. Bei dieser Topologie wird ein elektronisches Token nacheinander an jeden Host übertragen. Mit diesem Token erhält der Host die Genehmigung, Daten über das Netz zu senden. Wenn der Host keine Daten zu versenden hat, leitet er die Erlaubnis an den nächsten Host weiter und der Vorgang wiederholt sich. Zwei Beispiele für Netze, die mit Token-Passing arbeiten, sind Token Ring und Fiber Distributed Data Interface (FDDI).

Das folgende Diagramm zeigt verschiedene Topologien, die über Netzkopplungselemente verbunden sind. Es zeigt ein nicht zu komplexes Netz, mit dem z. B. Schulen oder kleinere Unternehmen arbeiten.




Client-Server-Architektur

Einer der Hauptgründe für das rasante Anwachsen des World Wide Webs sind die benutzerfreundlichen Zugriffsmöglichkeiten auf Informationen. Ein Webbrowser ist eine Client/Server-Anwendung, d. h. er benötigt sowohl eine Client- als auch eine Serverkomponente, um ordnungsgemäß funktionieren zu können. Ein Webbrowser stellt Daten in Multimediaformaten auf Webseiten dar, die Text, Grafiken, Audio- und Videoelemente enthalten. Die Webseiten werden in einer Formatsprache namens HyperText Markup Language (HTML) erstellt. HTML weist einen Webbrowser an, ein bestimmte Webseite in einer speziellen Art darzustellen. Darüber hinaus legt HTML die Positionen fest, an denen Text, Dateien und Objekte eingefügt werden, die vom Webserver an den Webbrowser übertragen werden sollen.

Hyperlinks ermöglichen die einfache Navigation im World Wide Web. Ein Hyperlink ist ein Objekt, ein Wort, ein Satz oder ein Bild auf einer Webseite. Wenn auf den Hyperlink geklickt wird, öffnet der Browser eine neue Webseite. Die Webseite

enthält (häufig in ihrer nicht sichtbaren HTML-Beschreibung) eine Adressangabe, die als Uniform Resource Locator (URL) bezeichnet wird.

Wenn ein Webbrowser aufgerufen wird, zeigt er in der Regel eine Startseite, die so genannte „Homepage“, an. Die URL der Startseite wurde bereits in den Konfigurationseinstellungen des Webbrowsers gespeichert, kann aber jederzeit geändert werden. Von der Startseite aus können Sie auf einen der Hyperlinks der Webseite klicken oder eine URL in die Adresszeile des Browsers eingeben. Der Webbrowser untersucht dann das Protokoll, um festzustellen, ob er ein anderes Programm aufrufen muss. Anschließend ermittelt er mithilfe von DNS die **IP-Adresse** des Webservers. Danach wird eine Sitzung mit dem Webserver eingeleitet. Die Daten, die an den HTTP-Server übertragen werden, enthalten die Pfadinformation zur Webseite. Die Daten können auch einen speziellen Dateinamen für eine HTML-Seite enthalten. Ist kein Name angegeben, wird der Standardname aus den Konfigurationseinstellungen des Servers verwendet.

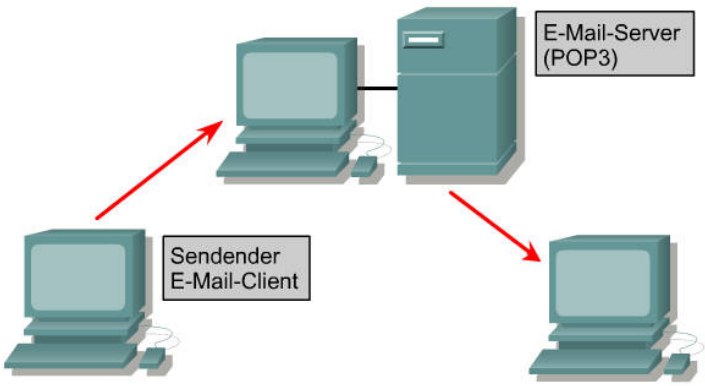
Der Server antwortet auf die Anfrage, indem er alle Text-, Audio-, Video- und Grafikdateien entsprechend den Angaben in den HTML-Anweisungen an den Web-Client sendet. Der Client-Browser stellt alle diese Dateien wieder zusammen, um eine Ansicht der Webseite zu erzeugen, und beendet anschließend die Sitzung. Wenn auf eine andere Seite geklickt wird, die sich auf demselben oder auf einem anderen Server befindet, beginnt der gesamte Vorgang erneut.

### Internetdienste und Internetprotokolle

#### World Wide Web und HTTP

HyperText Transfer Protocol (HTTP) wird im World Wide Web eingesetzt, das den Teil des Internets bildet, der am schnellsten wächst und am meisten verwendet wird.

Im Uniform Resource Locator (URL) „http://www.cisco.com/edu/“ gibt „http://“ dem Browser das zu verwendende Protokoll an. Der zweite Teil – „www“ – ist der Host-Name oder der Name eines bestimmten Computers mit einer eigenen IP-Adresse. Der letzte Teil – „edu“ – identifiziert die Position des Ordners auf dem Server, der die Standard-Webseite enthält.




Nachdem eine E-Mail-Nachricht gesendet wurde, gelangt sie zunächst zum "Postamt", das für den Benutzer zuständig ist. Der Empfänger holt die Nachricht dann von diesem "Postamt" ab.

| http:// | www. | cisco.com | /edu/ |
|---|---|---|---|
| Teilt dem Browser mit, welches Protokoll verwendet werden muss. | Identifiziert den Host-Namen bzw. den Namen eines bestimmten Computers. | Repräsentiert die Domäne der Website. | Gibt den Ordner auf dem Server an, in dem sich die Seite befindet. Da kein genauer Name für die Seite angegeben ist, wird der Browser die Standardseite, die durch den Server angegeben ist, laden. |

Email und SMTP bzw. POP3

E-Mail-Server verwenden das Simple Mail Transfer Protocol (SMTP), um E-Mail-Nachrichten zu senden und zu empfangen. Das SMTP-Protokoll überträgt E-Mail-Nachrichten im ASCII-Format.

Wenn ein E-Mail-Server eine Nachricht für einen lokalen Client empfängt, speichert er sie, bis der Client die Nachricht abruft. Mail-Clients haben verschiedene Möglichkeiten, um die für sie bestimmten Nachrichten abzurufen. Sie können über spezielle Programme direkt auf die Dateien auf dem E-Mail-Server zugreifen oder zum Abrufen ihrer Nachrichten ein Netzprotokoll verwenden. Die gebräuchlichsten E-Mail-Client-Protokolle sind POP3 und IMAP4. Beide verwenden zum Transport der Daten TCP. Diese speziellen Protokolle werden aber von den meisten E-Mail-Clients nur zum Abrufen der E-Mail-Nachrichten eingesetzt. Zum Senden der Nachrichten wird dagegen fast immer SMTP verwendet. Aufgrund der unterschiedlichen Protokolle – und möglicherweise auch zwei verschiedenen Servern – kann es vorkommen, dass ein E-Mail-Client zwar Nachrichten senden, aber nicht empfangen kann (oder umgekehrt). Deshalb sollte für Probleme, die beim Senden und Empfangen von E-Mail-Nachrichten auftreten, grundsätzlich eine getrennte Fehlerbehebung erfolgen.

Bei der Überprüfung der Konfiguration eines E-Mail-Clients muss festgestellt werden, ob die SMTP- und POP- bzw. IMAP-Einstellungen korrekt sind. Mithilfe einer Telnet-Verbindung zum SMTP-Port (25) oder POP3-Port (110) kann auf einfache Weise getestet werden, ob ein E-Mail-Server erreichbar ist. Durch Eingabe des folgenden Befehls in der Windows-Befehlszeile können Sie überprüfen, ob der SMTP-Dienst auf dem E-Mail-Server mit der IP-Adresse 192.168.10.5 erreichbar ist:

C:\>telnet 192.168.10.5 25

Das SMTP-Protokoll bietet nur eine geringe Sicherheit und erfordert keine Authentisierung. Netzadministratoren treffen oft Vorkehrungen, die den Zugriff externer Hosts auf den SMTP-Server zum Senden oder Empfangen von E-Mail-Nachrichten verhindern. Unberechtigte Benutzer können den Server dann nicht als Relay-Station für E-Mail-Nachrichten nutzen.

**FTP**

FTP (File Transfer Protocol) ist ein zuverlässiger verbindungsorientierter Dienst, der Dateien mit Hilfe von TCP zwischen Systemen überträgt, die FTP unterstützen. Der Hauptzweck von FTP besteht darin, Dateien von einem Computer an einen anderen zu übertragen. Dabei werden die Dateien von den Servern kopiert und auf die Clients verschoben bzw. von den Clients kopiert und auf die Server verschoben. Wenn Dateien von einem Server kopiert werden, stellt FTP zunächst eine Befehlsverbindung zwischen dem Client und dem Server her. Danach wird eine zweite Verbindung zwischen den Computern eingerichtet, über die die Daten übertragen werden. Die Datenübertragung kann im ASCII-Modus oder im binären Modus erfolgen. Der Modus bestimmt, welche Kodierung für die Datendatei verwendet wird. Im OSI-Modell findet dieser Vorgang auf der Darstellungsschicht statt. Nach dem Ende der Dateiübertragung wird die Datenverbindung auto-

matisch abgebaut. Wenn der komplette Vorgang des Kopierens und Verschiebens von Dateien abgeschlossen ist und der Benutzer sich abmeldet und die Sitzung beendet, wird die Befehlsverbindung unterbrochen.

**Telnet und SSH**

Telnet-Client-Software ermöglicht die Anmeldung bei einem entfernten Internet-Host, auf dem ein Telnet-Server-Anwendung ausgeführt wird. Danach können Befehle über die Befehlszeile ausgeführt werden. Ein Telnet-Client wird als lokaler Host bezeichnet. Der Telnet-Server, auf dem spezielle Software installiert ist (ein so genannter Daemon), ist der entfernte Host.

Um eine Verbindung von einem Telnet-Client aus herzustellen, muss die Verbindungsoption gewählt werden. Danach wird normalerweise ein Dialogfeld zur Eingabe eines Host-Namens und eines Terminaltyps geöffnet. Der Host-Name ist die IP-Adresse oder der DNS-Name des entfernten Computers. Der Terminaltyp legt fest, welche Art von Terminalemulation der Telnet-Client durchführen soll. Die Telnet-Operation beansprucht die Verarbeitungsleistung des übertragenden Computers nicht. Sie überträgt lediglich die Tastenanschläge an den entfernten Host und sendet die resultierende Bildschirmausgabe an den lokalen Monitor zurück. Alle Verarbeitungs- und Speichervorgänge finden auf dem entfernten Computer statt.

Telnet arbeitet auf der Anwendungsschicht des TCP/IP-Modells und damit auf den oberen drei Schichten des OSI-Referenzmodells. Befehle werden auf der Anwendungsschicht verarbeitet. Auf der Darstellungsschicht erfolgt die Formatierung (normalerweise ASCII). Die Übertragung findet auf der Sitzungsschicht statt. Im TCP/IP-Modell werden alle diese Funktionen als Teil der Anwendungsschicht betrachtet.

**Adressierung von Internetrechnern**

Damit zwei Systeme miteinander kommunizieren können, müssen sich diese gegenseitig identifizieren und lokalisieren können. Ein Computer kann mit mehr als einem Netz verbunden sein. In einer solchen Situation muss dem System auch mehr als eine Adresse zugewiesen werden. Jede Adresse bezeichnet die Verbindung des Computers mit einem unterschiedlichen Netz. Alle Verbindungspunkte oder Schnittstellen auf einem Gerät verfügen über eine Adresse in einem Netz. Dies ermöglicht anderen Computern, das Gerät in einem bestimmten Netz zu finden. Die Kombination aus Netzadresse und der Host-Adresse erzeugt eine eindeutige Adresse für jedes Gerät in einem Netz. Jedem Computer in einem Netz muss eine eindeutige Kennung oder eine IP-Adresse zugewiesen werden. Diese Adresse, ermöglicht es einem Computer, einen anderen Computer in einem Netz zu finden. Alle Computer müssen auch über eine eindeutige physikalische Adresse verfügen, die als MAC-Adresse bezeichnet wird. Diese werden durch den Hersteller der Netzwerkkarte zugewiesen.

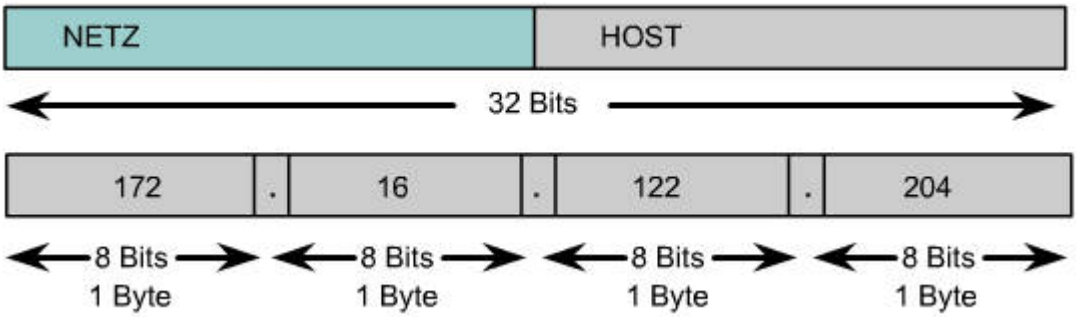
Eine IP-Adresse ist eine 32-Bit-Sequenz aus Einsen und Nullen. Abbildung zeigt ein Beispiel für eine 32-Bit-Zahl. Um den Umgang mit IP-Adressen zu erleichtern, werden diese als vier durch Punkte getrennte Dezimalzahlen geschrieben. So lautet z. B. die IP-Adresse eines Computers 192.168.1.2, und die eines anderen 128.10.2.1. Diese Schreibweise wird als „dezimale Punktnotation“ bezeichnet. Jeder Teil der Adresse wird als Oktett bezeichnet, da dieser aus acht Binärziffern besteht. So lautet beispielsweise die Adresse 192.168.1.8 in der Binärnotation 11000000.10101000.00000001.00001000. Das Verfahren der dezimalen Punktnotation ist leichter zu verstehen als das binäre Verfahren mit Einsen und Nullen. Diese dezimale Punktnotation verhindert auch eine große Anzahl von Transpositionsfehlern, die sich aus der reinen Verwendung von Binärzahlen ergeben würde.

Sowohl die binären als auch die dezimalen Zahlen in Abbildung repräsentieren die gleichen Werte. Jedoch lässt sich die Adresse in der dezimalen Punktnotation besser verstehen. Dies ist eines der allgemeinen Probleme mit Binärzahlen: Die langen Zeichenketten mit sich wiederholenden Einsen und Nullen steigern die Fehlerwahrscheinlichkeit.

Im Gegensatz zu den Binärwerten 11000000.10101000.00000001.00001000 und 11000000.10101000.00000001.00001001 lässt sich die Beziehung zwischen den Zahlen 192.168.1.8 and 192.168.1.9 leichter erkennen (in diesem Fall, dass es sich um aufeinander folgende Zahlen handelt).

Ein Router verwendet IP zur Weiterleitung von Paketen von einem Absendernetz zu einem Zielnetz. Die Pakete müssen eine Kennung für sowohl das Absendernetz als auch das Zielnetz enthalten. Mithilfe der IP-Adresse des Zielnetzes sendet ein Router ein Paket an das korrekte Netz. Wenn das Paket bei einem mit dem Zielnetz verbundenen Router ankommt, verwendet der Router die IP-Adresse zur Lokalisierung des spezifischen Computers im Netz. Die Funktionsweise

dieses Systems ist dem eines nationalen Postdienstes sehr ähnlich. Beim Versenden der Post dient die Postleitzahl zur Weiterleitung an das Postamt am Zielort. Dieses Postamt verwendet wiederum den Straßennamen, um das endgültige Ziel am jeweiligen Ort zu lokalisieren.




Jede IP-Adresse hat außerdem zwei Teile. Der erste Teil identifiziert das Netz, mit dem das System verbunden ist, und der zweite Teil identifiziert das System. Wie gezeigt, liegt jedes Oktett im Bereich zwischen 0 und 255. Jedes dieser Oktette lässt sich in 256 Untergruppen einteilen, und diese lassen sich wiederum in weitere 256 Untergruppen mit jeweils 256 Adressen unterteilen. Durch Referenzierung der Gruppenadresse direkt oberhalb einer Gruppe in der Hierarchie können alle Gruppen, die von dieser Adresse abzweigen, als einzelne Einheit referenziert werden.

Diese Art von Adresse wird als hierarchische Adresse bezeichnet, da sie unterschiedliche Ebenen enthält. Eine IP-Adresse kombiniert diese zwei Kennungen in einer Zahl. Bei dieser Zahl muss es sich um eine eindeutige Zahl handeln, da doppelte Adressen das Routing unmöglich machen würden. Der erste Teil identifiziert die Netzadresse des Systems. Der zweite Teil, der als Host-Teil bezeichnet wird, identifiziert, welche spezifischen Computer sich im Netz befinden.

IP-Adressen werden in Klassen unterteilt, um große, mittlere und kleine Netze zu definieren. Adressen der Klasse A werden größeren Netzen zugewiesen. Adressen der Klasse B werden für mittlere Netze und Adressen der Klasse C werden für kleine Netze verwendet. Der erste Schritt bei der Ermittlung, welcher Teil der Adresse das Netz und welcher den Host identifiziert, besteht darin, die Klasse einer IP-Adresse zu benennen.

| IP-Adressklasse | IP-Adressbereich (Dezimalwert des ersten Oktetts) |
|---|---|
| Klasse A | 1-126 (00000001-01111110) * |
| Klasse B | 128-191 (10000000-10111111) |
| Klasse C | 192-223 (11000000-11011111) |
| Klasse D | 224-239 (11100000-11101111) |
| Klasse E | 240-255 (11110000-11111111) |

| Thema: | Grundlagen zur IP-Adressierung<br>Wiederholung und Übung<br>* Unterrichtsmaterial zur vorläufigen Handreichung Wirtschaftsinformatik |
|---|---|

Lernziel

- ✗ Nennen Sie die fünf verschiedenen IP-Adressklassen.
- ✗ Beschreiben Sie die Eigenschaften und die Verwendungsmöglichkeiten für die verschiedenen IP-Adressklassen.
- ✗ Ermitteln Sie die Klasse einer IP-Adresse anhand der Netzadresse.
- ✗ Bestimmen Sie, welcher Teil oder welches Oktett einer IP-Adresse die Netz-ID und welcher Teil die Host-ID ist.
- ✗ Bestimmen Sie gültige und ungültige Host-IP-Adressen basierend auf den Regeln der IP-Adressierung.
- ✗ Definieren Sie den Adressbereich und die Standard-Subnetzmaske für jede Klasse.

Hintergrund/Vorbereitung

In dieser Übung werden Sie sich mit verschiedenen IP-Adressklassen befassen und erfahren, wie TCP/IP-Netze funktionieren. Obwohl es sich in erster Linie um eine schriftliche Übung handelt, empfiehlt es sich trotzdem, ein paar echte IP-Netzadressen mit den Befehlzeilendienstprogrammen **ipconfig** für Windows NT/2000/XP oder **winipcfg** für Windows zu untersuchen. Mit IP-Adressen werden einzelne TCP/IP-Netze und Hosts (Computer und Drucker) in Netzen eindeutig identifiziert, um die Kommunikation zwischen den einzelnen Geräten zu ermöglichen. Arbeitsstationen und Server in einem TCP/IP-Netz werden „Hosts“ genannt. Jeder besitzt eine eindeutige IP-Adresse, die als „Host-Adresse“ bezeichnet wird. TCP/IP ist das weltweit am weitesten verbreitete Protokoll. Für das Internet oder World Wide Web wird ausschließlich die IP-Adressierung verwendet. Damit ein Host auf das Internet zugreifen kann, benötigt er eine IP-Adresse.

Diese besteht grundsätzlich aus zwei Teilen:

- ✗ Einem Netzabschnitt
- ✗ Einem Host-Abschnitt

Der Netzabschnitt der IP-Adresse wird einem Unternehmen oder einer Organisation vom Internet Network Information Center (InterNIC) zugewiesen. Router verwenden die IP-Adresse, um Datenpakete zwischen Netzen auszutauschen. IP-Adressen sind 32 Bits lang (bei der aktuellen Version von IPv4) und in vier Oktette mit jeweils acht Bits unterteilt. Diese operieren auf der Vermittlungsschicht, Schicht 3 des OSI-Modells (Open System Interconnection), was der Internetschicht des TCP/IP-Modells entspricht. Es gibt folgende Methoden, um IP-Adressen zuzuweisen:

- ✗ Statisch – manuell durch einen Netzadministrator
- ✗ Dynamisch – automatisch durch einen DHCP-Server (Dynamic Host Configuration Protocol)

Die IP-Adresse einer Arbeitsstation (Host) ist eine „logische Adresse“, d. h., sie kann geändert werden. Die MAC-Adresse (Media Access Control) der Arbeitsstation ist eine physikalische Adresse mit 48 Bits. Diese Adresse ist in der Regel fest an die Netzwerkkarte gebunden und kann nur durch deren Austausch geändert werden. Die Kombination aus logischer IP-Adresse und physikalischer MAC-Adresse ermöglicht die Übermittlung von Datenpaketen an das richtige Ziel.

Es gibt fünf verschiedene IP-Adressklassen. Abhängig von der Klasse werden für den Netz- und Host-Abschnitt unterschiedlich viele Bits verwendet. In dieser Übung werden Sie die verschiedenen IP-Adressklassen und die jeweiligen Ei-

genschaften kennen lernen. Für das allgemeine Verständnis von TCP/IP und Internetworks ist es unerlässlich, dass Sie sich mit IP-Adressen auskennen.

Folgende Ressourcen werden benötigt:

- ✗ PC-Arbeitsstation, auf der Windows 9x/NT/2000/XP installiert ist
- ✗ Zugriff auf die Windows-Zubehör-Anwendung Rechner

Schritt 1: Wiederholen Sie die IP-Adressklassen und ihre Eigenschaften.

Adressklassen

Es gibt fünf Klassen von IP-Adressen, A bis E. Davon werden nur die drei ersten Klassen kommerziell genutzt. In der folgenden Tabelle wird zunächst eine Netzadresse der Klasse A vorgestellt. In der ersten Spalte steht die IP-Adressklasse. Die zweite Spalte ist das erste Oktett, das für eine bestimmte Adressklasse im angegebenen Bereich liegen muss. Die Adresse der Klasse A muss mit einer Zahl von 1 bis 126 beginnen. Das erste Bit einer Adresse der Klasse A ist immer Null, das heißt, das höherwertige Bit oder 128er-Bit kann nicht verwendet werden. 127 ist für Schleifentests reserviert. Mit dem ersten Oktett wird die Netz-ID für ein Netz der Klasse A definiert.

Standard-Subnetzmaske

Die Standard-Subnetzmaske verwendet ausschließlich binäre Einsen (Dezimalzahl 255), um die ersten acht Bits der Adresse der Klasse A zu maskieren. Die Standard-Subnetzmaske hilft Routern und Hosts zu ermitteln, ob der Ziel-Host in diesem oder einem anderen Netz liegt. Da es nur 126 Netze der Klasse A gibt, können die verbleibenden 24 Bits (drei Oktette) für Hosts verwendet werden. Jedes Netz der Klasse A kann 224 oder über 16 Millionen Hosts besitzen. Das Netz wird häufig in kleinere Gruppen aufgeteilt, so genannte Subnetze. Dazu wird eine benutzerdefinierte Subnetzmaske verwendet, die in der nächsten Übung behandelt wird.

Netz- und Host-Adresse

Der Netz- oder der Host-Abschnitt der Adresse darf nicht ausschließlich aus Einsen oder Nullen bestehen. Die Adresse 118.0.0.5 der Klasse A ist beispielsweise eine gültige IP-Adresse, da der Netzabschnitt (die ersten acht Bits entsprechen dem Wert 118) nicht ausschließlich aus Nullen besteht, und der Host-Abschnitt (die letzten 24 Bits) nicht ausschließlich aus Nullen oder Einsen. Wenn der Host-Abschnitt ausschließlich aus Nullen bestünde, würde es sich um die Netzadresse handeln. Wenn der Host-Abschnitt nur aus Einsen bestünde, wäre es die Broadcast-Adresse für dieses Netz. Der Wert jedes einzelnen Oktetts kann jeweils nicht größer als die Dezimalzahl 255 oder die Binärzahl 11111111 sein.

| Klasse | Dezimalbereich des ersten Oktetts | Höherwertige Bits des ersten Oktetts | Netz-/Host-ID (N=Netz, H=Host) | Standard-Subnetzmaske | Anzahl der Netze | Hosts pro Netz (verwendbare Adressen) |
|---|---|---|---|---|---|---|
| **A** | 1 – 126 * | 0 | N.H.H.H | 255.0.0.0 | 126 ($2^7$ – 2) | 16,777,214 ($2^{24}$ – 2) |
| **B** | 128 – 191 | 10 | N.N.H.H | 255.255.0.0 | 16,382 ($2^{14}$ – 2) | 65,534 ($2^{16}$ – 2) |
| **C** | 192 – 223 | 110 | N.N.N.H | 255.255.255.0 | 2,097,150 ($2^{21}$ – 2) | 254 ($2^8$ – 2) |
| **D** | 224 – 239 | 1110 | Reserviert für Multicasting | | | |
| **E** | 240 – 254 | 11110 | Experimentell, wird für Forschungszwecke verwendet | | | |

Schritt 2: Ermitteln Sie die grundlegende IP-Adressierung.

Beantworten Sie folgende Fragen. Sie benötigen dazu neben Ihren Kenntnissen zu IP - Adressklassen die Tabelle mit den IP-Adressen.

1. In welchem Bereich liegen die Dezimal- und Binärzahlen des ersten Oktetts für alle möglichen IP-Adressen der Klasse B?

Dezimalbereich: Von: _____ Bis: _____

Binärbereich: Von: _____ Bis: _____

2. Welches bzw. welche Oktette stellen den Netzabschnitt einer IP-Adresse der Klasse C dar?_____

3. Welches bzw. welche Oktette stellen den Host-Abschnitt einer IP-Adresse der Klasse A dar? _____

4. Wie viele Hosts können bei einer Netzadresse der Klasse C maximal verwendet werden?_____

5. Wie viele Netze der Klasse B gibt es? _____

6. Wie viele Hosts kann jedes Netz der Klasse B besitzen? _____

7. Wie viele Oktette enthält eine IP-Adresse? _____ Wie viele Bits pro Oktett? _____

Schritt 3: Bestimmen Sie den Host- und Netzabschnitt der IP-Adresse.

Geben Sie für die folgenden Host-IP-Adressen Folgendes an:

- ✗ Klasse der Adresse
- ✗ Netzadresse oder -ID
- ✗ Host-Abschnitt
- ✗ Broadcast-Adresse für dieses Netz
- ✗ Standard-Subnetzmaske

Der Host-Abschnitt besteht für die Netz-ID ausschließlich aus Nullen. Geben Sie nur die Oktette für den Host an. Der Host Abschnitt besteht für einen Broadcast ausschließlich aus Einsen. Der Netzabschnitt der Adresse besteht für eine Subnetzmaske ausschließlich aus Einsen. Geben Sie die richtigen Werte in folgende Tabelle ein:

| Host-IP-Adresse | **Adressklasse** | **Netzadresse** | **Host-Adresse** | **Netz-Broadcast-Adresse** | **Standard-Subnetzmaske** |
|---|---|---|---|---|---|
| **216.14.55.137** | | | | | |
| **123.1.1.15** | | | | | |
| **150.127.221.244** | | | | | |
| **194.125.35.199** | | | | | |
| **175.12.239.244** | | | | | |

Schritt 4: Beantworten Sie folgende Fragen für die IP-Adresse 142.226.0.15 und die Subnetzmaske 255.255.255.0:

Wie lautet das binäre Äquivalent für das zweite Oktett? _____

Welcher Klasse gehört die Adresse an? _____

Wie lautet die Netzadresse dieser IP-Adresse? _____

Ist dies eine gültige Host-IP-Adresse (J/N)? _____

Warum bzw. warum nicht? _____

Schritt 5: Geben Sie an, welche Host-IP-Adressen für kommerzielle Netze gültig sind.

Geben Sie an, welche der folgenden Host-IP-Adressen für kommerzielle Netze gültig sind und begründen Sie Ihre Antwort. „Gültig“ bedeutet, dass die Adresse einer beliebigen der folgenden Komponenten zugeordnet werden könnte:

- ✗ Arbeitsstation
- ✗ Server
- ✗ Drucker
- ✗ Router-Schnittstelle
- ✗ Ein beliebiges anderes kompatibles Gerät

Geben Sie die richtigen Werte in folgende Tabelle ein:

| Host-IP-Adresse | Gültige Adresse? (Ja/Nein) | Warum bzw. warum nicht? |
|---|---|---|
| 150.100.255.255 | | |
| 175.100.255.18 | | |
| 195.234.253.0 | | |
| 100.0.0.23 | | |
| 188.258.221.176 | | |
| 127.34.25.189 | | |
| 224.156.217.73 | | |

## 3 Verschlüsselung

# Verschlüsselung

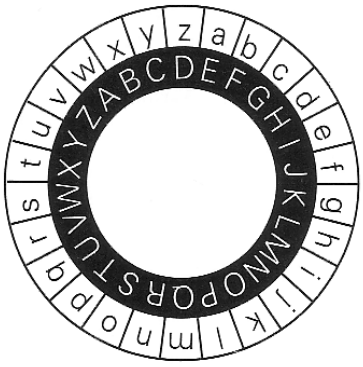
## Sicherheit, Ceasar

| Thema: | Verschlüsselung<br>Caesarchiffre<br>* Landesinstitut für Schulentwicklung |
|---|---|

Eine Tabelle zur Caesarchiffre

Die Mappe enthält drei Tabellenblätter:

Es sind Blätter zur Eingabe, zur Verschlüsselung und zur Entschlüsselung.




Die Caesarmethode

Man legt zunächst einen Schlüsselwert fest, z.B. 4.

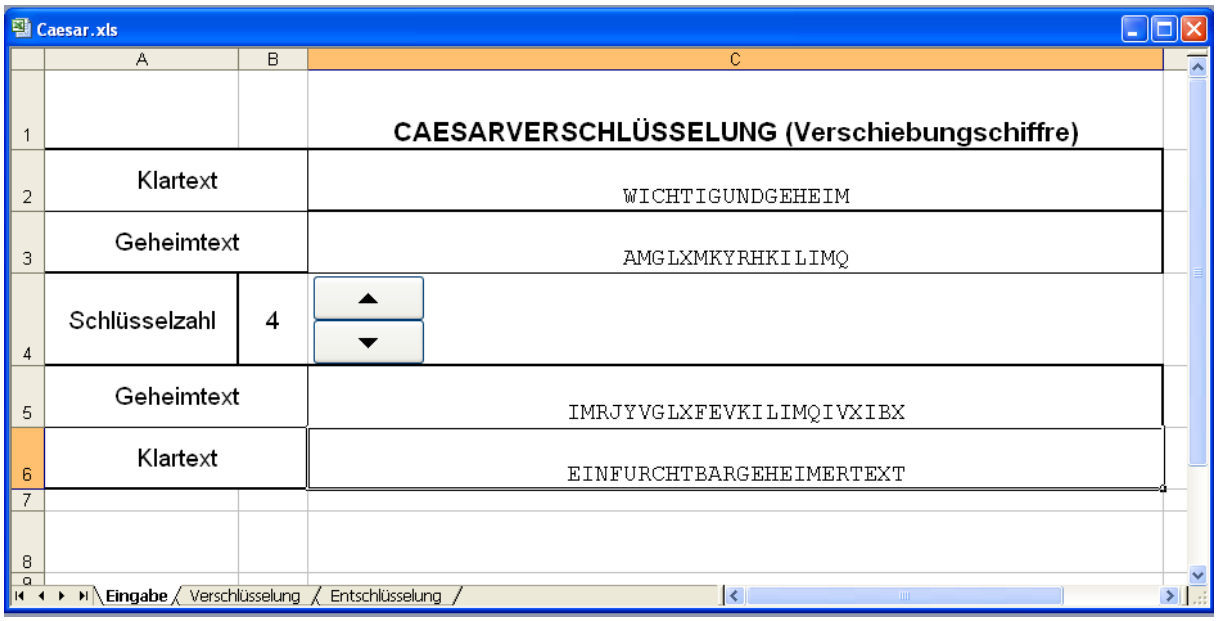
Der Text wird nun verschlüsselt, indem man jeden Buchstaben des Klartextes im Alphabet um 4 Stellen nach rechts „verschiebt". Aus A wird E, aus B wird F, … , aus V wird Z, aus W wird A. Dabei kann man sich Klartext- und Geheimtextalphabet angeordnet vorstellen auf zwei gegeneinander verdrehbaren Scheiben.

Die Entschlüsselung erfolgt dann in der „Gegenrichtung".

Wir benötigen drei Tabellen:

1. Die Eingabetabelle
2. Die Verschlüsselungstabelle
3. Die Entschlüsselungstabelle

## Die Eingabetabelle



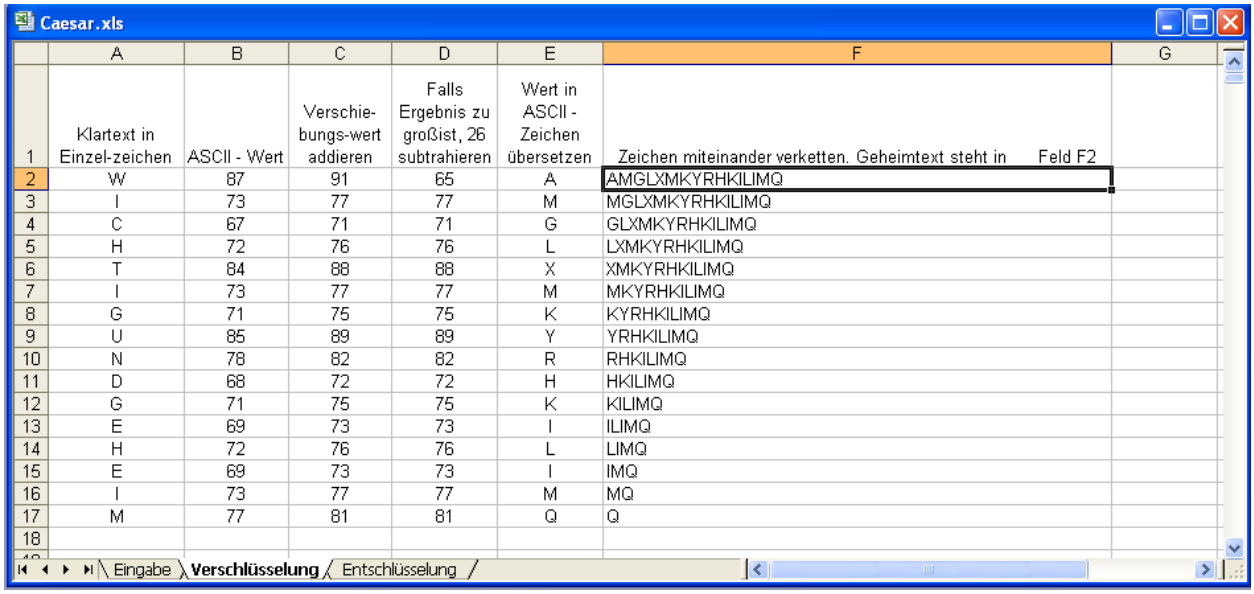

Die Tabelle enthält Eingabe- und Ausgabefelder

| Zelle | Inhalt | Name |
|---|---|---|
| C2 | Eingegebener Klartext | Klartext |
| C5 | Eingegebener Geheimtext | Geheimtext |
| B4 | Schlüsselzahl, eingestellt mit Drehfeld | Verschiebzahl |
| C3 | Formel: =verschlüsselt | |
| C6 | Formel: =entschlüsselt | |

Die Verschlüsselungstabelle

Ablauf der Verschlüsselung:

- Text in Buchstaben zerlegen
- ASCII-Wert ermitteln (für Großbuchstaben liegen diese zwischen 65 und 90)
- Verschiebungszahl addieren
- Falls das Ergebnis größer als 90 ist (ASCII-Wert von Z), 26 subtrahieren.
- Das zu diesem Wert gehörige Zeichen bestimmen
- Die einzelnen Zeichen wieder zu einer Zeichenkette verbinden.



Caesar.xls

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Klartext in Einzel-zeichen | ASCII - Wert | Verschie-bungs-wert addieren | Falls Ergebnis zu groß ist, 26 subtrahieren | Wert in ASCII - Zeichen übersetzen | Zeichen miteinander verketten. Geheimtext steht in Feld F2 | |
| 2 | W | 87 | 91 | 65 | A | AMGLXMKYRHKILIMQ | |
| 3 | I | 73 | 77 | 77 | M | MGLXMKYRHKILIMQ | |
| 4 | C | 67 | 71 | 71 | G | GLXMKYRHKILIMQ | |
| 5 | H | 72 | 76 | 76 | L | LXMKYRHKILIMQ | |
| 6 | T | 84 | 88 | 88 | X | XMKYRHKILIMQ | |
| 7 | I | 73 | 77 | 77 | M | MKYRHKILIMQ | |
| 8 | G | 71 | 75 | 75 | K | KYRHKILIMQ | |
| 9 | U | 85 | 89 | 89 | Y | YRHKILIMQ | |
| 10 | N | 78 | 82 | 82 | R | RHKILIMQ | |
| 11 | D | 68 | 72 | 72 | H | HKILIMQ | |
| 12 | G | 71 | 75 | 75 | K | KILIMQ | |
| 13 | E | 69 | 73 | 73 | I | ILIMQ | |
| 14 | H | 72 | 76 | 76 | L | LIMQ | |
| 15 | E | 69 | 73 | 73 | I | IMQ | |
| 16 | I | 73 | 77 | 77 | M | MQ | |
| 17 | M | 77 | 81 | 81 | Q | Q | |
| 18 | | | | | | | |

Eingabe | Verschlüsselung | Entschlüsselung

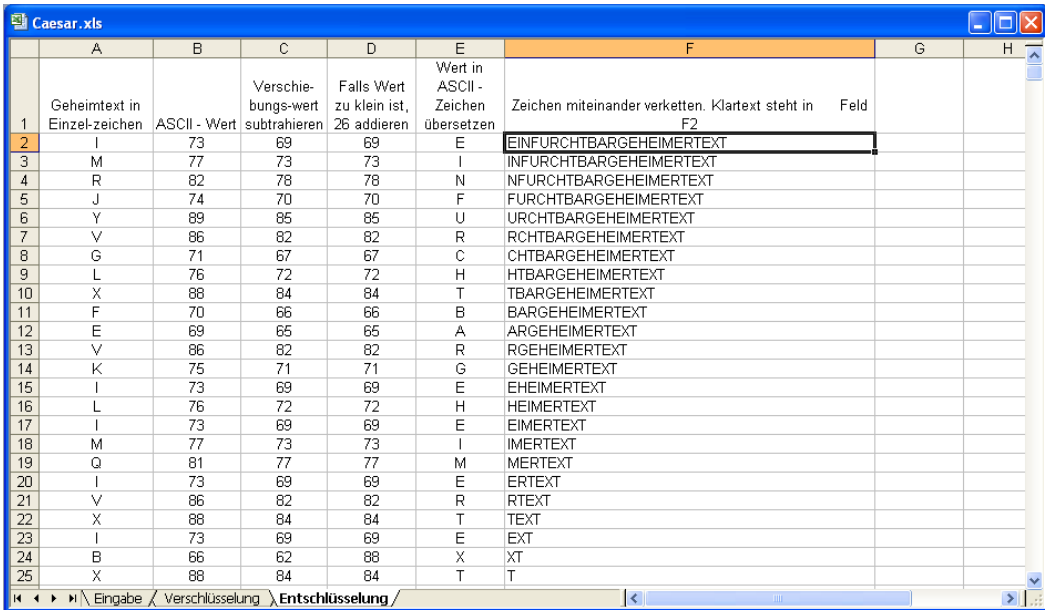
| Zelle | Formel | Kommentar |
|---|---|---|
| A2 | =TEIL(klartext;ZEILE(A1);1) | Die Funktion Zeile erspart einem eine Spalte mit den fortlaufenden Zahlen 1,2,3,… |
| B2 | =WENN(A2<>"";CODE(A2);"") | Die Wenn-Formeln sind nötig, um Fehlerwerte zu vermeiden, falls die Formeln auf leere Felder angewendet werden. |
| C2 | =WENN(B2<>"";B2+Verschiebzahl;"") | |
| D2 | =WENN(UND(C2<>"";C2>90);C2-26;C2) | |
| E2 | =WENN(D2<>"";ZEICHEN(D2);"") | |
| F2 | =VERKETTEN(E2;F3)<br>Name: verschlüsselt | Hängt an den Buchstaben, der im Feld links steht, die Zeichenkette aus dem Feld darunter. |

Alle Formeln können beliebig weit nach unten kopiert werden!

## Die Entschlüsselungstabelle

Die Entschlüsselung läuft im wesentlichen genauso ab wie die Verschlüsselung.

- Text in Buchstaben zerlegen
- ASCII-Wert ermitteln (für Großbuchstaben liegen diese zwischen 65 und 90)
- Verschiebungszahl subtrahieren
- Falls das Ergebnis kleiner als 65 ist (ASCII-Wert von A), 26 addieren.
- Das zu diesem Wert gehörige Zeichen bestimmen
- Die einzelnen Zeichen wieder zu einer Zeichenkette verbinden.



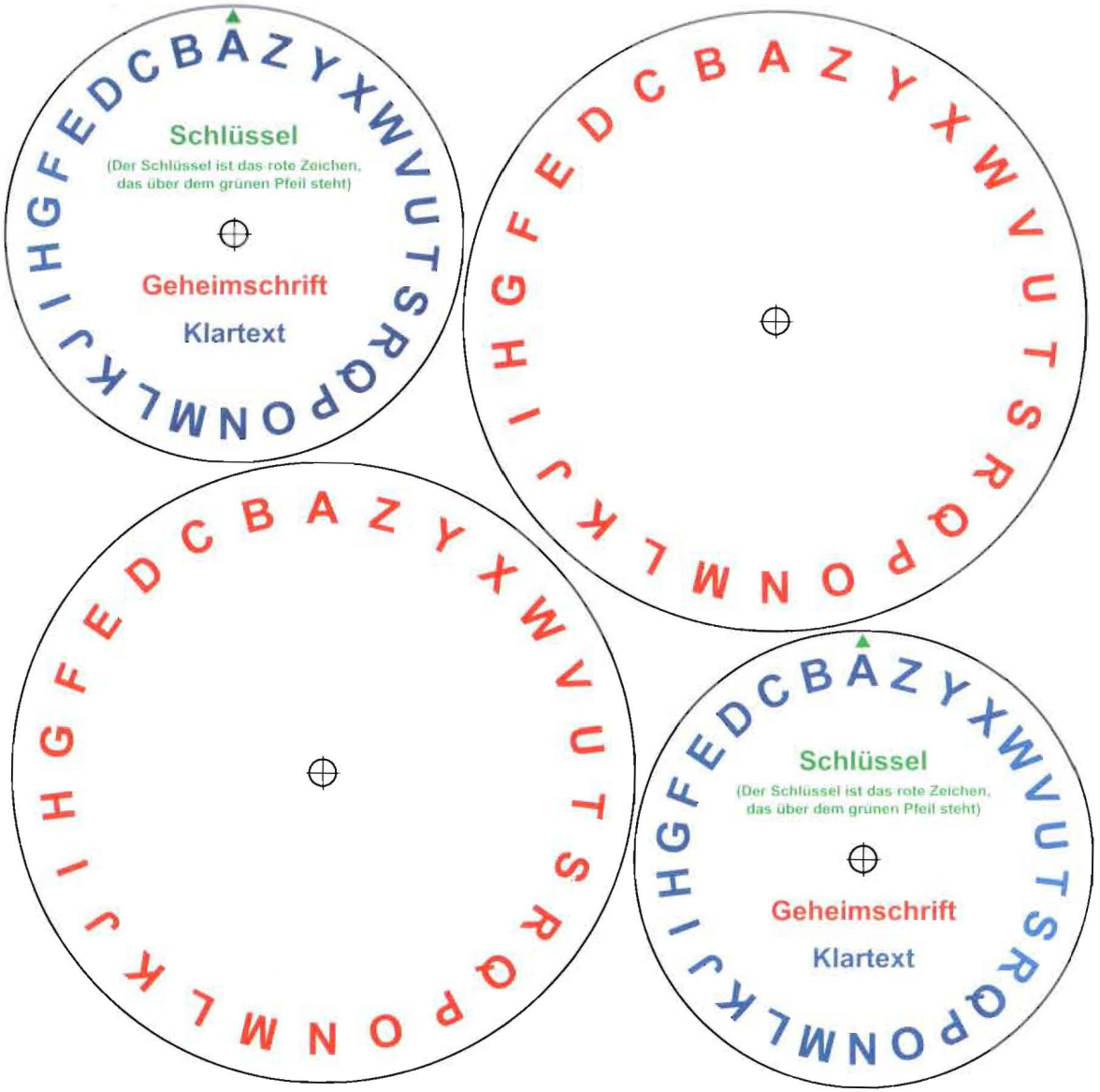
Caesar.xls

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | Geheimtext in Einzel-zeichen | ASCII - Wert | Verschie-bungs-wert subtrahieren | Falls Wert zu klein ist, 26 addieren | Wert in ASCII - Zeichen übersetzen | Zeichen miteinander verketten. Klartext steht in F2 Feld | | |
| 2 | I | 73 | 69 | 69 | E | EINFURCHTBARGEHEIMERTEXT | | |
| 3 | M | 77 | 73 | 73 | I | INFURCHTBARGEHEIMERTEXT | | |
| 4 | R | 82 | 78 | 78 | N | NFURCHTBARGEHEIMERTEXT | | |
| 5 | J | 74 | 70 | 70 | F | FURCHTBARGEHEIMERTEXT | | |
| 6 | Y | 89 | 85 | 85 | U | URCHTBARGEHEIMERTEXT | | |
| 7 | V | 86 | 82 | 82 | R | RCHTBARGEHEIMERTEXT | | |
| 8 | G | 71 | 67 | 67 | C | CHTBARGEHEIMERTEXT | | |
| 9 | L | 76 | 72 | 72 | H | HTBARGEHEIMERTEXT | | |
| 10 | X | 88 | 84 | 84 | T | TBARGEHEIMERTEXT | | |
| 11 | F | 70 | 66 | 66 | B | BARGEHEIMERTEXT | | |
| 12 | E | 69 | 65 | 65 | A | ARGEHEIMERTEXT | | |
| 13 | V | 86 | 82 | 82 | R | RGEHEIMERTEXT | | |
| 14 | K | 75 | 71 | 71 | G | GEHEIMERTEXT | | |
| 15 | I | 73 | 69 | 69 | E | EHEIMERTEXT | | |
| 16 | L | 76 | 72 | 72 | H | HEIMERTEXT | | |
| 17 | I | 73 | 69 | 69 | E | EIMERTEXT | | |
| 18 | M | 77 | 73 | 73 | I | IMERTEXT | | |
| 19 | Q | 81 | 77 | 77 | M | MERTEXT | | |
| 20 | I | 73 | 69 | 69 | E | ERTEXT | | |
| 21 | V | 86 | 82 | 82 | R | RTEXT | | |
| 22 | X | 88 | 84 | 84 | T | TEXT | | |
| 23 | I | 73 | 69 | 69 | E | EXT | | |
| 24 | B | 66 | 62 | 88 | X | XT | | |
| 25 | X | 88 | 84 | 84 | T | T | | |

Eingabe | Verschlüsselung | Entschlüsselung

| Zelle | Formel | Kommentar |
|---|---|---|
| A2 | =TEIL(Geheimtext;ZEILE(A1);1) | Die Funktion Zeile erspart einem eine Spalte mit den fortlaufenden Zahlen 1,2,3,… |
| B2 | =WENN(A2<>"";CODE(A2);"") | Die Wenn-Formeln sind nötig, um Fehlerwerte zu vermeiden, falls die Formeln auf leere Felder angewendet werden. |
| C2 | =WENN(B2<>"";B2-Verschiebzahl;"") | |
| D2 | =WENN(UND(C2<>"";C2<65);C2+26;C2) | |
| E2 | =WENN(D2<>"";ZEICHEN(D2);"") | |
| F2 | =VERKETTEN(E2;F3)<br>Name: entschlüsselt | Hängt an den Buchstaben, der im Feld links steht, die Zeichenkette aus dem Feld darunter. |

Wieder werden die Formeln alle nach unten kopiert!


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Ä
Schlüssel
(Der Schlüssel ist das rote Zeichen, das über dem grünen Pfeil steht)
Geheimschrift
Klartext
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Ä
Schlüssel
(Der Schlüssel ist das rote Zeichen, das über dem grünen Pfeil steht)
Geheimschrift
Klartext