GWDG
Nachrichten

für die Benutzerinnen und Benutzer des Rechenzentrums

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Ausgabe 9/2011

Inhalt

IMPRESSUM

GWDG-Nachrichten für die Benutzerinnen und Benutzer des Rechenzentrums
ISSN 0940-4686
34. Jahrgang, Ausgabe 9/2011 **Erscheinungsweise: monatlich**
www.gwdg.de/gwdg-nr **Auflage: 500**

Titelfoto: Der neue Großformatdrucker HP z6200 bei der GWDG

Herausgeber:	**Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen**		
	Am Faßberg 11		
	37077 Göttingen	**Tel.: 0551 201-1510**	**Fax: 0551 201-2150**
Redaktion:	**Dr. Thomas Otto**	**Tel.: 0551 201-1828**	**E-Mail: Thomas.Otto@gwdg.de**
Herstellung:	**Maria Geraci**	**Tel.: 0551 201-1804**	**E-Mail: Maria.Geraci@gwdg.de**
Druck:	**GWDG / AG H**	**Tel.: 0551 201-1523**	**E-Mail: printservice@gwdg.de**

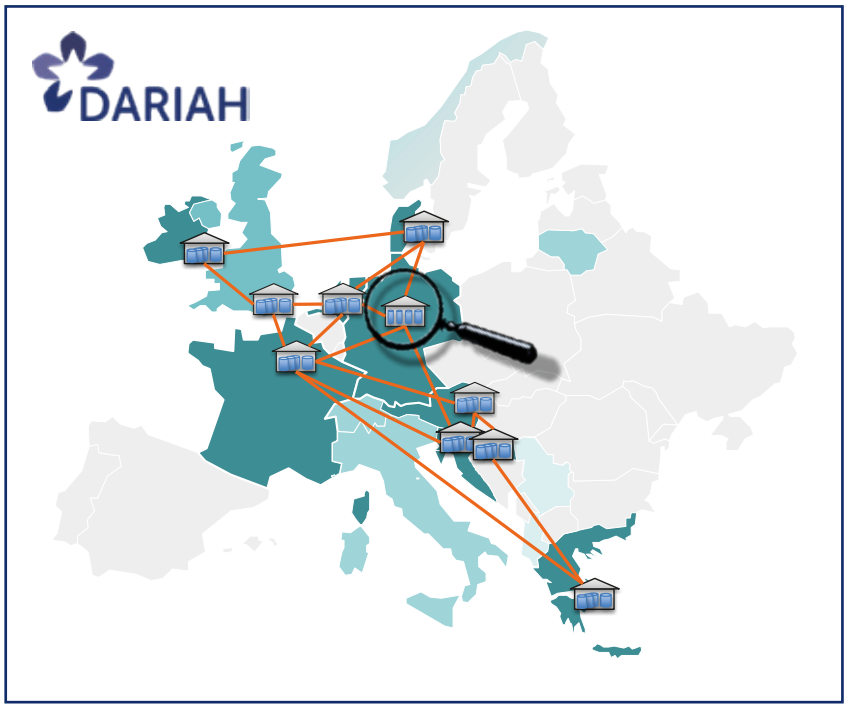
Forschungsinfrastrukturen für die e-Humanities – Beteiligung der GWDG am Projekt DARIAH-DE

Die GWDG ist im Rahmen ihrer Forschungsaktivitäten im Bereich e-Science am Projekt „DARIAH-DE – Aufbau von Forschungsinfrastrukturen für die e-Humanities“ beteiligt. Das Ziel des Projektes ist es, die in den Geistes- und Kulturwissenschaften mit digitalen Methoden und Hilfsmitteln durchgeführte Forschung zu unterstützen und weiter voranzutreiben, verschiedene Disziplinen miteinander zu vernetzen und durch den Aufbau einer Forschungsinfrastruktur den Austausch von Ressourcen, Methoden, Daten und Erfahrungen zu fördern.

DARIAH-DE im europäischen Kontext

Das Projekt DARIAH-DE wird vom BMBF gefördert und ist eingebunden in ein im Rahmen des ESFRI-Prozesses (European Strategy Forum on Research Infrastructures) gefördertes europäisches Verbundprojekt. Im Projekt DARIAH-DE sind insgesamt 18 Partner aus verschiedenen Bereichen der Geisteswissenschaften mit IT-Dienstleistern zu einem Konsortium zusammengeschlossen. Die Projektlaufzeit beträgt zunächst drei Jahre.

In den Geisteswissenschaften vollzieht sich derzeit der Paradigmenwechsel, wie ihn die Natur- und angewandten Wissenschaften schon vor Jahrzehnten erlebt haben. Im Zeitalter von e-Science bzw. e-Research werden auch hier in sogenannten Virtuellen Forschungsumgebungen Theorie, Experiment und Simulation zusammengeführt. Das gemeinsame Nutzen und Bearbeiten von Daten, Ideen, Methoden und Expertenwissen soll ebenso gefördert werden wie der Zugang zu verschiedenen Wissenssammlungen erleichtert und miteinander kompatibel gestaltet werden soll. Daher arbeitet DARIAH-DE mit den Fach-Communities zusammen, um ICT-basierte Lösungen zu erproben und anzuwenden sowie um die Forschung und den disziplinübergreifenden Austausch von Expertenwissen und Methoden zu erleichtern.



Die Aktivitäten im Bereich der Geistes- und Kulturwissenschaften erstrecken sich über verschiedene Gebiete: Forschung, Datenpflege, Dienste-Standardisierung, Schulung, Unterstützung, Standards, Richtlinien, Verknüpfung von Forschungsinfrastrukturen, Langzeitarchivierung, Ressourcen-Allokation und Erhalt der Infrastruktur, um nur einige Beispiele aufzuzählen.

Sowohl die Vernetzung von verschiedenen Forschungsgebieten als auch das Ausloten und Nutzen neuester Informations- und Kommunikationstechnologien eröffnen ganz neue Forschungsmöglichkeiten, -ansätze und Fragestellungen. Eine durchweg hohe Qualität der Forschungsdaten wird durch einen entsprechenden Anforderungskatalog an die teilnehmenden Institutionen und durch individuell zu bestimmende vertrauensbildende Maßnahmen gewährleistet.

Die Forschungspraktiken in den Geistes- und Kulturwissenschaften bedürfen zunehmend der Verfügbarkeit einer hochentwickelten pan-europäischen digitalen Infrastruktur. Das Projekt zielt darauf ab, diesen erforderlichen

technischen Rahmen zu entwickeln und mit der Forschungsinfrastruktur einen neuen Forschungsraum für die Geistes- und Kulturwissenschaftler in Deutschland und über die DARIAH-EU-Einbindung in ganz Europa und darüber hinaus zu schaffen.

Die Ziele der Errichtung einer Forschungsinfrastruktur für die Geistes- und Kulturwissenschaften sind aus Sicht des Wissenschaftlers:

- Generierung neuer Forschungsfragen und Beantwortung „alter" Forschungsfragen durch neue digitale Methoden, wodurch Wettbewerbsvorteile entstehen,
- einfacher Zugang zu weit verstreut liegenden heterogenen Forschungsdaten,
- Nachnutzung der eigenen Forschungsdaten und Daten anderer Wissenschaftler und Disziplinen sowie Verknüpfung der verschiedenen Forschungsdaten miteinander,
- disziplinübergreifendes, kollaboratives Arbeiten und Austausch von Erfahrung, Methoden und Werkzeugen,
- Verantwortungsübergabe der Sicherung von Forschungsdaten an langfristig vertrauenswürdige, verlässliche, stabile Organisationen bzw. Partner,
- die die Daten pflegen und
- den Zugang, die Sichtbarkeit und Zitierbarkeit auf definierte Dauer gewährleisten.

Die Ziele aus Sicht von Forschungseinrichtungen und Datenzentren:

- Zugang, Sichtbarkeit und Zitierbarkeit der Forschungsdaten auf definierte Dauer gewährleisten,
- effizientere Verfahren für die Langzeitarchivierung von Forschungsdaten gemeinsam mit anderen Einrichtungen entwickeln (data curation), wodurch Synergieeffekte und damit Kostenersparnis entstehen,
- den Wissenschaftlern effiziente Instrumente und Dienstleistungen bereitstellen und damit Rahmenbedingungen für wettbewerbsfähige Forschung schaffen.

Für die Gesellschaft ergibt sich zudem ein Nutzen durch:

- effizienten Einsatz von Forschungsmitteln, da z. B. Forschungsdaten nicht mehrfach erhoben werden müssen,
- Einhaltung der „guten wissenschaftlichen Praxis" und Erfüllung des Datenmanagementplans,
- Sichtbarkeit der Forschungsergebnisse, v. a. im internationalen Kontext z. B. durch eine dauerhafte Zitierbarkeit von Forschungsdaten.

e-Infrastruktur und Forschungsdaten

Die GWDG ist in dem Projekt zum einen mit ihrer Initiative zu persistenten Identifizierern (PIDs) für die Wissenschaft im EPIC-Konsortium im Arbeitspaket „e-Infrastruktur" vertreten, womit die Sichtbarkeit der Forschungsergebnisse durch eine dauerhafte Zitierbarkeit ermöglicht wird.

Zum anderen leitet die GWDG das Arbeitspaket „Forschungsdaten" (AP 3). In diesem werden Lösungen für den Zugriff und die Langzeitverfügbarkeit von Forschungsdaten im Hinblick auf die verschiedenen Stadien im Lebenszyklus von Forschungsdaten erarbeitet. Ein besonderer Fokus liegt dabei auf der Interoperabilität von Datenrepositorien heterogenen Datenbestands und verteilter Herkunft sowie auf rechtlichen Aspekten des Zugriffs und der Nachnutzung von Forschungsdaten. Das Arbeitspaket

- errichtet eine virtuelle Beratungsstelle zur Langzeitverfügbarkeit von Forschungsdaten,
- erarbeitet Konzepte für die Evaluierung und Zertifizierung von digitalen Datenrepositorien,
- erarbeitet Empfehlungen und Lizenzmodelle für die Veröffentlichung von Forschungsdaten,
- führt Lizenzverhandlungen auf europäischer Ebene mit für die Geistes- und Kulturwissenschaften unverzichtbaren Datenanbietern,
- begleitet den vollständigen Prozess der Standardisierung von formalen und fachspezifischen Datenmodellen,

- fördert die Erstellung von Ontologien, Normdaten und Registries als Mittel zur semantischen Interoperabilität.

Das AP 3 „Forschungsdaten" konzentriert sich speziell auf das Spannungsfeld zwischen fächerspezifischen und fächerübergreifenden Sichtweisen. Schwerpunktthemen bilden die Interoperabilität und Nachnutzbarkeit von Forschungsdaten, ihre Langlebigkeit sowie darauf aufbauend das Vertrauen von Nutzern. Diese Aspekte können durch Standards gefördert werden, die gut in der Community verankert sind, durch Mechanismen zur Qualitätskontrolle (z. B. Metadaten-Validierung) sowie durch Transparenz in der Historie und dem Revisionsverlauf von Daten, der sogenannten Provenance.

Schwardmann

Kontakt:
Dr. Ulrich Schwardmann
uschwar1@gwdg.de
0551 201-1542

Neue S/W- und Farbdruckerfarm bei der GWDG

Seit August ist eine neue kombinierte S/W- und Farbdruckerfarm mit drei Druckern der Baureihe „Canon imageRUNNER Advance C5030i" bei der GWDG im Einsatz. Sie löst die bisherige S/W-Druckerfarm aus zwei Kyocera-FS-9500-Druckern ab.

In den letzten Jahren ist die Nachfrage nach S/W–Druck auf den Druckern im Benutzerbereich der GWDG immer mehr zurückgegangen, während die Nachfrage nach Ausdrucken in Farbe zugenommen hat. Aus diesem Grund hat sich die GWDG entschieden, die S/W-Drucker im Benutzerbereich der GWDG abzuschaffen und durch Farbdrucker zu ersetzen. Die abgelösten Kyocera-S/W-Drucker werden die Druckerfarm im LRC (SUB-Neubau) erweitern, weil dort die Nachfrage nach kostengünstigen S/W-Ausdrucken weiterhin sehr stark ist (s. Abb. 4). Ebenfalls abgeschafft wurde der in die Jahre gekommene Farbdrucker des Typs Canon CLC3220. Die bisherigen Warteschlangen *zclp3d33, zclp3l33, zclp3s33, zclp4d33, zclp4l33* und *zclp4s33* existieren damit nicht mehr.

Der jetzt schon bei der GWDG vorhandene Farbdrucker Canon imageRUNNER Advance C5030i wurde in die neue Druckerfarm integriert. Dieser Drucker wurde bereits in den GWDG-Nachrichten 3/2010 vorgestellt. Die Warteschlangen *zclp3d50, zclp3l50,*

1 *Die neue S/W- und Farbdruckerfarm bei der GWDG*

Warteschlange	Beschreibung	Bewertung [AE]*
farbe (color)	DIN A4 einseitig farbig	0,0048
zclp3d	DIN A3 doppelseitig Hochformat, farbig	0,0072
zclp3l	DIN A3 doppelseitig Querformat, farbig	0,0072
zclp3s	DIN A3 einseitig, farbig	0,0072
zclp4d	DIN A4 doppelseitig Hochformat, farbig	0,0048
zclp4l	DIN A3 doppelseitig Querformat, farbig	0,0048
zclp4s	DIN A4 einseitig, farbig	0,0048

* 1 AE entspricht 33,- €

2 *Übersicht über die neuen Farbwarteschlangen*

zclp3s50, zclp4d50, zclp4l50 und *zclp4s50* sind unter Windows nicht mehr vorhanden. Daher bitten wir alle Benutzer, diese Warteschlangen auf ihrem Computer zu löschen und auf die in Abb. 2 aufgelisteten Warteschlangen umzusteigen. Auf den UNIX-Dialogservern der GWDG gibt es sie aber weiterhin. Ansonsten werden die Drucker bei Farbausgabe über die Sammelwarteschlangen *color, farbe, zclp4d, zclp4l, zclp4s, zclp3d, zclp3l* sowie *zclp3s* angesteuert, wobei automatisch der Drucker benutzt wird, der zum jeweiligen Zeitpunkt am wenigsten ausgelastet ist. Eine direkte Ansteuerung jedes einzelnen Gerätes ist unter Windows nicht vorgesehen.

Beim S/W-Druck bleibt aus Sicht der Anwender alles beim Alten: Die Warteschlangen *standard, zmlp4d, zmlp4l, zmlp4s, zmlp3d, zmlp3l* sowie *zmlp3s* bleiben weiterhin bestehen. Lediglich auf dem Druck-Server *gwdu111* werden die Daten von der Software GhostScript in S/W konvertiert, bevor sie zum Drucker geschickt werden. Obwohl der Ausdruck letztendlich von Farbdruckern erzeugt wird, sollten die Anwender auch weiterhin die S/W-Warteschlangen nutzen, wenn kein Farbdruck erforderlich ist. Denn eine Farbseite erzeugt für die GWDG etwa sechsmal so hohe Druckkosten wie eine S/W-Seite.

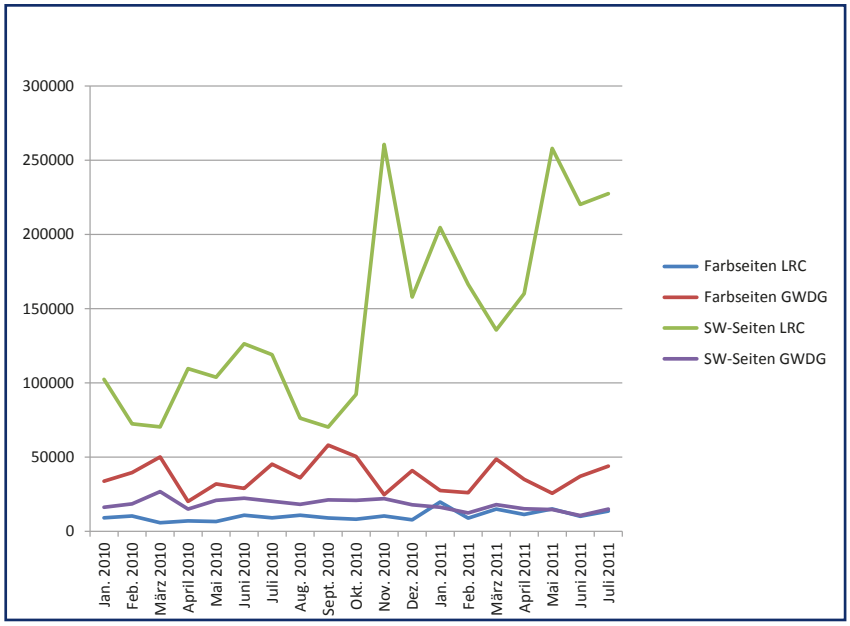
Nolte

Kontakt:
Uwe Nolte
unolte@gwdg.de
0551 201-1547

Warteschlange	Beschreibung	Bewertung [AE]*
standard	S/W DIN A4 doppelseitig	0,0012
zmlp3d	S/W DIN A3 doppelseitig Hochformat	0,0018
zmlp3l	S/W DIN A3 doppelseitig Querformat	0,0018
zmlp3s	S/W DIN A3 einseitig	0,0018
zmlp4d	S/W DIN A4 doppelseitig Hochformat	0,0012
zmlp4l	S/W DIN A3 doppelseitig Querformat	0,0012
zmlp4s	S/W DIN A4 einseitig	0,0012

* 1 AE entspricht 33,- €

3 *Übersicht über die neuen S/W-Warteschlangen*



4 *Druckausgabestatistik von Januar 2010 bis Juli 2011*

Rechenzentrum am Tag der Deutschen Einheit geschlossen

Das Rechenzentrum der GWDG ist am Montag, dem 3. Oktober 2011, dem Tag der Deutschen Einheit, geschlossen.

Falls Sie sich zu der Zeit, an der das Rechenzentrum geschlossen ist, an die GWDG wenden wollen, schicken Sie bitte eine E-Mail an support@gwdg.de. Das dahinter befindliche Ticket-System wird auch während dieser Zeit von Mitarbeiterinnen und Mitarbeitern der GWDG regelmäßig kontrolliert.

Wir bitten alle Benutzerinnen und Benutzer, sich darauf einzustellen.

Grieger

HP z6200 – der neue Großformatdrucker bei der GWDG

Die GWDG freut sich, ihren Benutzern einen neuen Großformatdrucker des Typs HP z6200 anbieten zu können. Hierbei handelt es sich um das Nachfolgemodell des HP z6100, den die GWDG auch weiterhin bereitstellt. Der HP z6200 löst den ausgefallenen Canon W8200pg ab. Dadurch stehen unseren Benutzern jetzt wieder drei Großformatdrucker am Standort GWDG uneingeschränkt zur Verfügung.

Mit seiner Druckgeschwindigkeit von bis zu 140 m^2/Stunde handelt es sich beim HP z6200 laut Angabe des Herstellers um den „schnellsten Drucker in seiner Klasse". Wie sein „Bruder", der HP z6100, ist der HP z6200 ebenfalls mit acht „HP Vivid Fototinten" ausgerüstet. Er besitzt Tinten in den Farben Chromrot, Magenta, Schwarz matt, Fotoschwarz, Gelb, Cyan hell, Grau hell und Magenta hell. Als Besonderheit fällt auf, dass dieser Drucker, statt mit einer Zyan-Tinte, mit einer Chromrot-Tinte ausgerüstet, was eine verbesserte Wiedergabe von Rot-Tönen erlaubt. Die Einschränkungen, die durch den Wegfall der Zyan-Tinte entstehen, sollen dem gegenüber vernachlässigbar sein. Die Aussagen von HP zur Lichtbeständigkeit der Tinten sind in Abb. 2 zu finden.

Zum ersten Mal seit vielen Jahren hat die GWDG beim HP z6200 einen Großformatdrucker mit eingebautem Adobe-zertifiziertem Postscript3-Rip beschafft. Dieses Rip kann sowohl unter Windows als auch unter UNIX oder Mac OS über die Warteschlange *zcixls62* benutzt werden.

Darüber hinaus beherrscht der Drucker die Formate HP-GL/2, HP-RTL, CALS G4, TIFF (unkomprimiert!) und JPEG. D. h., wenn Sie z. B. JPEG-Dateien drucken möchten, können Sie dabei genauso vorgehen, wie in den GWDG-Nachrichten 2/2011 beschrieben.

1 *Der neue Großformatdrucker HP z6200 bei der GWDG*

Standort	Lichtbeständigkeit
Innenbereich im direkten Sonnenlicht, nicht laminiert	Mehr als ein Jahr
Standort ohne direkte Sonneneinstrahlung	Über 200 Jahre

2 *Lichtbeständigkeit in Abhängigkeit vom Standort*

Warteschlange	Beschreibung
zcipls62	„Normale" Warteschlange; kein Skalieren der Druckdaten; Eingabeformat: PostScript; Ausgabeformat an Drucker: jpg; Rip mittels Ghostscript auf gwdu111;Warteschlange für Windows-, UNIX- und Mac-Systeme
zcip4s62	Hochskalieren der Druckdaten auf 400 %; Eingabeformat: PostScript; Ausgabeformat an Drucker: jpg; Rip mittels Ghostscript auf gwdu111; diese Warteschlange ist nur unter UNIX nutzbar
zcixls62	Eingabeformat: PostScript; wird direkt zum Drucker durchgeleitet; Rip mittels eingebautem Rip auf Drucker; Warteschlange ist unter Windows, UNIX und Mac OS nutzbar

3 *Warteschlangen für den HP z6200*

Bitte beachten Sie, dass die alten Warteschlangen (also *zcipls82* und *zcip4s82*), die einst für den abgelösten Canon W8200 eingerichtet wurden, nicht mehr existieren.

Standardmäßig ist der Drucker mit schwer beschichtetem Papier mit einer Grammatur von 130 g/m² und einer Breite von 106 cm bestückt. Pro Ausdruck werden 0,55 AE vom Institutskontingent abgebucht.

Nolte

Kontakt:
Uwe Nolte
unolte@gwdg.de
0551 201-1547

Merkmal	Beschreibung
Drucktechnologie	Thermischer HP-Tintendruck
Druckauflösung	max. 2.400 x 1.200 dpi
Nicht bedruckbare Ränder	oben, unten, rechts und links: 5 mm (1 cm mit GWDG-Druckerteiber!)
Tinten	HP Vivid Fototinten: Chromrot (r), Zyan hell (lc), Magenta (m), Magenta hell (lm), Gelb (y), Grau hell (lg), Fotoschwarz (pK), Mattschwarz (mK)
Tröpfchengröße	4 pl (lc, lm, lg, pK), 6 pl (r, m, y, mK)
Druckgeschwindigkeit	bis zu 140 m²/h
Liniengenauigkeit	+/- 0,1 % der angegebenen Vektorlänge oder +/- 0,2 mm (je nachdem, welcher Wert höher ist)
Druckersprachen	HP-GL/2, HP-RTL, CALS G4,TIFF (unkomprimiert!), JPEG
Speicher	32 GByte Hauptspeicher, 160 GByte Festplatte
Druckkosten pro DIN-A0-Ausdruck	0,55 AE (entspricht 18,00 €)
Warteschlangen	zcipls62, zcip4s62, zcixls62 (Erläuterungen s. Abb. 2)

4 *Technische Daten des HP z6200*

Kontingentzuweisung für das vierte Quartal 2011

Die nächste Zuweisung von Institutskontingenten für die Inanspruchnahme von Leistungen der GWDG erfolgt am Dienstag, dem 4. Oktober 2011. Die Höhe der Kontingente wird den Instituten per Brief oder per E-Mail mitgeteilt. Die Bemessung der Institutskontingente erfolgte nach den Vorläufigen Richtlinien des Beirats der GWDG und den Ergänzungen der Beiratskommission für die Verteilung von IT-Leistung entsprechend dem Verbrauch im Zeitraum vom 01.03.2011 bis 31.08.2011. Nicht verbrauchte Kontingente werden zu 50 % in das nächste Quartal übertragen. Negative Verbrauchswerte werden zu 100 % mit dem neuen Institutskontingent verrechnet.

Jeder Benutzer kann den aktuellen Stand des Institutskontingents durch die Eingabe des Kommandos *kontingent* auf einer Workstation des UNIX-Clusters oder im WWW unter dem URL *http://www.gwdg.de/index.php?id=1678* abfragen. Dort besteht auch die Möglichkeit, Informationen über den Stand des separaten Druckkontingents abzurufen.

Falls in Ausnahmefällen das Institutskontingent nicht ausreichen sollte, können begründete Anträge an die Beiratskommission für die Verteilung von IT-Leistung über den URL *http://www.gwdg.de/index.php?id=799* gestellt werden. Solche Anträge sollen bis zum 17.11.2011 eingereicht werden.

Glässer

Kontakt:
Renate Glässer
renate.glaesser@gwdg.de
0551 201-1883

iPhone, iPad und die Code-Sperre

Die von vielen Nutzern des iPhone und iPad ungeliebte Code-Sperre schützt nicht nur vor dem unberechtigten Zugriff auf den Mail-Account und andere wichtige Zugangsdaten, sondern bietet erst die Voraussetzung für eine sichere Datenverschlüsselung, die Apple bei seinen mobilen Geräten ab iPhone 3GS eingeführt hat.

Mit der Veröffentlichung des iPhone 3GS im Jahre 2009 führte Apple auch die integrierte Hardwareverschlüsselung (256-Bit AES) aller auf dem Gerät gespeicherter Benutzerdaten ein. Die konsequente Unterstützung durch das Betriebssystem erfuhr diese jedoch erst 2010 durch iOS 4, was zur Folge hat, dass bei den ersten Geräten (iPhone 3GS und iPad 1) einige Vorarbeiten erforderlich sind, um in den Genuss dieser Verschlüsselung zu kommen.

Ältere iOS-Geräte

Während die älteren Modelle wie das iPhone Classic und das iPhone 3G die Verschlüsselung gar nicht nutzen können, weil hier die dazu erforderlichen Hardwarevoraussetzungen fehlen, müssen die Besitzer des iPhone 3GS und auch des iPad 1 zunächst einige Vorarbeiten tätigen. Der Grund liegt im veralteten Dateisystem, mit dem diese Geräte unter iOS 3 noch ausgeliefert wurden, und unter dem die Verschlüsselung nicht möglich ist. Dieses Dateisystem blieb übrigens auch nach dem Update auf iOS 4 erhalten, es sei denn, das mobile Gerät wurde irgendwann komplett gelöscht, z. B. über die Wiederherstellungsfunktion in iTunes, denn erst diese vollständige Löschung führt dazu, dass danach auch das neue Dateisystem installiert wird.

Um herauszufinden, ob das eigene Gerät schon mit dem modernen Dateisystem versehen ist, geht man auf „Einstellungen > Allgemein > Code-Sperre“ und prüft, ob dort unten auf der Seite der Satz „Datenschutz ist aktiviert“ aufgeführt ist. Fehlt dieser Satz, dann ist das Dateisystem noch veraltet und somit keine sichere Datenverschlüsselung möglich.

Zur Lösung dieses Problems muss das iPhone/iPad komplett gelöscht werden. Dazu verbindet man es mit iTunes auf dem Mac bzw. dem PC und prüft zunächst, ob bereits das aktuelle Betriebssystem (iOS 4.x) aufgespielt wurde, weil das wiederum die Vorraussetzung für das neue Dateisystem ist. Dann synchronisiert man sein iPhone/iPad über iTunes, um sämtliche Daten des Geräts zu sichern. Danach wird wiederum in iTunes über die Schaltfläche „Wiederherstellen“ eine vollständige Wiederherstellung des Gerätes durchgeführt, wodurch u. a. auch das moderne verschlüsselungsfähige Dateisystem installiert wird. Nach der Wiederherstellung wird in iTunes über die Option „Aus Backup wiederherstellen“ die zuvor erstellte Sicherungskopie ausgewählt und wieder auf das mobile Gerät zurückgespielt. Diese einzelnen Schritte können übrigens auch auf dem folgenden Support-Dokument nachgelesen werden:

http://support.apple.com/kb/HT4175?viewlocale=de_DE

Verschlüsselung aktivieren

Wichtigste Voraussetzung für die Dateiverschlüsselung ist die Aktivierung der „Code-Sperre“ in „Einstellungen > Allgemein > Code-Sperre“. Erst wenn sie im Ruhezustand oder auch im ausgeschalteten Zustand des mobilen Geräts aktiv wird, werden die dort befindlichen Daten verschlüsselt.

Die „Code-Sperre“ wird auch bereits von den Server-Richtlinien des Exchange-Servers der GWDG gefordert. Hier dient sie zum einem zum Schutz vor Missbrauch, falls das Gerät in falsche Hände gelangt. Andererseits dient sie aber auch dem Schutz des Exchange-Servers, weil jeder missbrauchte Account wiederum das Missbrauchspotenzial auf dem Server erhöht, z. B. durch Massenversand von SPAM.

Voreingestellt ist ein „Einfacher Code“, der aus einer vierstelligen PIN besteht. Da diese den Brute-Force-Angriffen zur Ermittlung der Passwörter meist nicht lange standhält, wird von Sicherheitsexperten immer zu einem komplexeren Password geraten, welches man durch Deaktivierung der Option „Einfacher Code“ erreicht. Da man dieses Password im täglichen Betrieb allerdings sehr oft eingeben muss, erweist es sich als sinnvoll, die Komplexität in Abhängigkeit der Eingabemöglichkeiten auf einer Touchscreen-Tastatur zu wählen, um durch diese Prozedur

nicht allzu sehr behindert zu werden.

Datenschutz für die Anwendungen

Über eine entsprechende Programmierschnittstelle stellt Apple die Datenverschlüsselung auch Anwendungsentwicklern zur Verfügung, damit sie diese Sicherheitstechnik in ihren Apps nutzen können. Als prominentes Beispiel dafür dient beispielsweise die als PDF-Betrachter und Dateimanager beliebte App „Good Reader“:

http://www.goodreader.net/goodreader.html

Hier wird der Zugriff auf die von der App verwalteten Dateien über zusätzliche Passwörter geregelt, die sich in Apples Verschlüsselungsverfahren einklinken. Damit werden alle Dateien in Good Reader verschlüsselt, sobald das mit einer Code-Sperre versehene Gerät in den Ruhezustand versetzt ist. Wird es dann per Eingabe der Code-Sperre wieder freigegeben, findet ohne Zutun des Anwenders wieder die Entschlüsselung der Dateien statt. Nur in dieser Phase lassen sich die Dateien über geeignete Programme auf PC beziehungsweise Mac kopieren. Daher ist es auch hier empfehlenswert, das Gerät stets aus Sicherheitsgründen in den Ruhezustand zu versetzen.

Fazit

Sicherlich mag es vielen Anwendern anfangs ein wenig lästig erscheinen, sein iPhone oder iPad ständig per Passworteingabe über die Code-Sperre freigeben zu müssen. Da sich auf diesen mobilen Begleitern im Laufe der Zeit zahllose Zugänge zu den verschiedenartigsten Internetdiensten und Sozialen Netzen einfinden, sollte das doch jegliche Schutzmaßnahmen rechtfertigen.

Reimann

Kontakt:
Michael Reimann
michael.reimann@gwdg.de
0551 201-1826

Personalia

Abschied von der GWDG

Markus Heß und **Philipp Hübel** haben die GWDG

nach erfolgreicher Tätigkeit zum 31. August 2011 verlassen. Beide hatten ihre Ausbildung zum Elektroniker für Geräte und Systeme nach 3,5-jähriger Ausbildungszeit bei der GWDG im Januar 2011 erfolgreich beendet.

Im Anschluss daran haben Herr Heß und Herr Hübel als Facharbeiter die GWDG-Mitarbeiterinnen und -Mitarbeiter tatkräftig beim weiteren Ausbau der Netzwerkverkabelung unterstützt. Insbesondere waren sie damit betraut, die WLAN-Struktur mit Voice over IP im neuen Max-Planck-Institut für Dynamik und Selbstorganisation auf dem Max-Planck-Campus einzurichten. Dabei wurden auch neue und manchmal ungewöhnliche, aber sehr erfolgreiche technische Lösungen erprobt und in Betrieb genommen.

Wir danken Herrn Heß und Herrn Hübel für ihre erfolgreiche Mitarbeit in der GWDG und hoffen, dass die Erfahrungen, die sie bei der GWDG gesammelt haben, nutzbringend bei ihren neuen

Arbeitgebern eingesetzt werden können. Wir wünschen ihnen für die Zukunft weiterhin alles Gute.

Grieger

Neue Auszubildende

Am 1. September 2011 starteten zwei neue Auszubildende bei der GWDG ins Berufsleben. Sie begannen eine 3 1/2-jährige Ausbildung zum „Elektroniker für Geräte und Systeme".

Herr **Robin Kleinhans** hat an der Schule am Hohen Hagen in Dransfeld seinen erweiterten Sekundarabschluss I erlangt.

Herr **Jannik Richter** hat an der Personn-Realschule-Weende den erweiterten Sekundarabschluss I erlangt; er hat bereits im Jahr 2010 sein Schulpraktikum bei der GWDG absolviert.

Beide neuen Auszubildenden zeigten während ihrer bisherigen Schulzeit großes Interesse an der Elektronik und PC-Technik. Dies soll bei der GWDG zu einen qualifizierten Berufsabschluss ausgebaut werden.

Beide sind unter der Telefonnummer 0551 201-1533 zu erreichen. Per E-Mail ist Herr Kleinhans unter *robin.kleinhans@gwdg.de* und Herr Richter unter *jannik.richter@gwdg.de* erreichbar.

Gutsch

Neuer Mitarbeiter in der AG H

Seit dem 1. September 2011 ist Herr **Sven Rosenfeld** in der Arbeitsgruppe „Nutzerservice und Betriebsdienste" (AG H) tätig.

Herr Rosenfeld unterstützt die Kolleginnen und Kollegen der GWDG in der Weiterentwicklung und Pflege des Active Directory sowohl im Client-Bereich als auch der Betreuung der zentralen Dienste und Strukturen. Ein wichtiger Punkt seiner Tätigkeit wird die Mitarbeit bei der Sharepoint-Infrastruktur sein.

In seiner zwölfjährigen Dienstzeit bei der Bundeswehr sammelte Herr Rosenfeld Erfahrungen in der Windows-Systemverwaltung sowohl am Standort als auch unter Einsatzbedingungen.

Im Anschluss begann er ein Studium der Angewandten Informatik, Fachrichtung „Betriebliche IT-Systeme", an der Hochschule Ostwestfalen-Lippe in Höxter, das er kürzlich mit dem Grad Bachelor of Science erfolgreich abschloss.

Während des Studiums arbeitete er in einem Projekt zur IT-Struktur eines Unternehmens mit und konnte so weitere Praxiserfahrung sammeln.

Herr Rosenfeld ist telefonisch unter der Nummer 0551 201-1833 und per E-Mail unter *sven.rosenfeld@gwdg.de* erreichbar.

Heuer

Umstiegshilfe für Office-2003-Nutzer auf Office 2010

Microsoft bietet auf seiner Homepage eine interaktive Umstiegshilfe an, die Benutzern helfen soll, Office 2003-Funktionen in Office 2010 wiederzufinden.

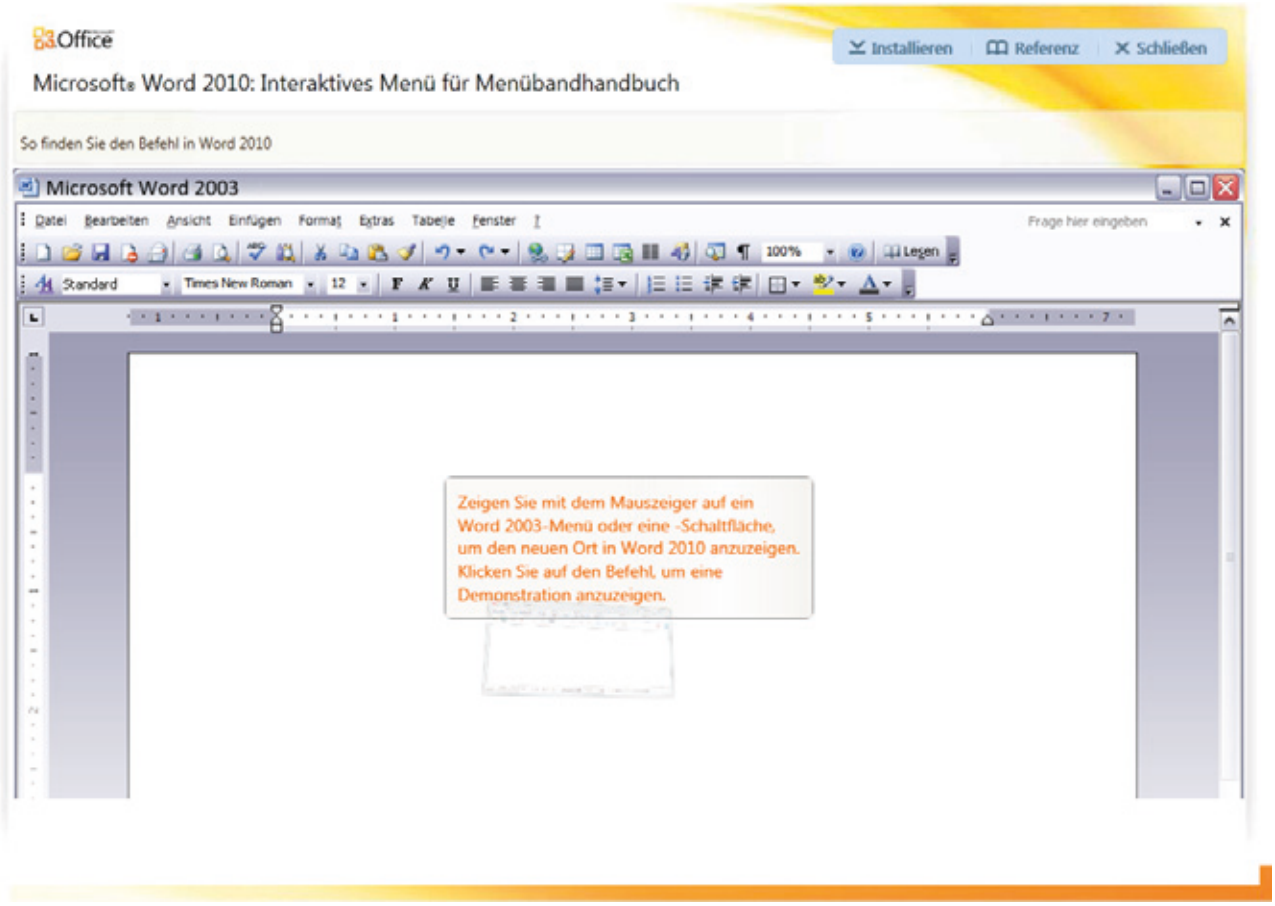
Seit Office 2007 hat Microsoft die Benutzeroberfäche seiner Office-Suite völlig neu gestaltet. Das hatte zur Folge, dass so mancher langjährige Office-2003-Benutzer viele Funktionen in Office 2010 nicht mehr wieder gefunden hat. Unter *http://office2010.microsoft.com/de-de/word-help/erkunden-von-menuband-und-backstage-in-2010-produkten-HA101794130.aspx* stellt Microsoft ein interaktives Handbuch bereit, das zeigt, wo sich ein Befehl aus einem Office-2003-Programm in Office 2010 wiederfindet.

1 *Microsoft stellt seine animierte Online-Hilfe für alle Office-Komponenten bereit*

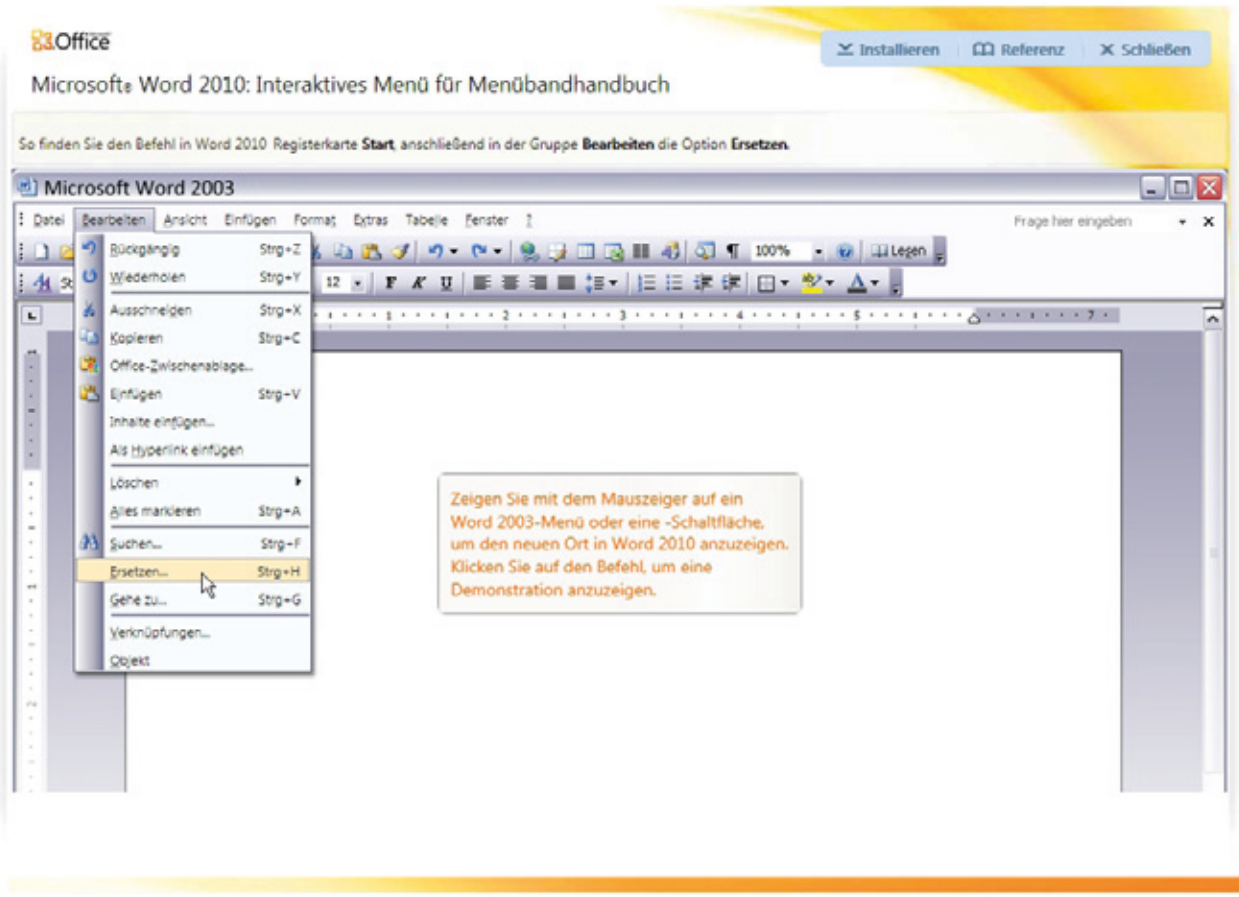
Im Folgenden soll anhand des Office 2003-Befehls „Bearbeiten > Ersetzen…“ demonstriert werden, wie diese Hilfe funktioniert: Klickt man auf den Link „Word-Handbuch öffnen >“, so öffnet sich ein neues Fenster im Browser (s. Abb. 2). Abb. 3 zeigt den nächsten Schritt. Möchte man noch nach anderen Befehlen suchen, so kommt man durch auf einen Klick auf „Anderen Befehl verwenden“ zurück zu Word 2003 (s. Abb. 4). Wenn man möchte, kann man dieses Tool auch lokal installieren (benötigt das Silverlight-Plugin).

Nolte

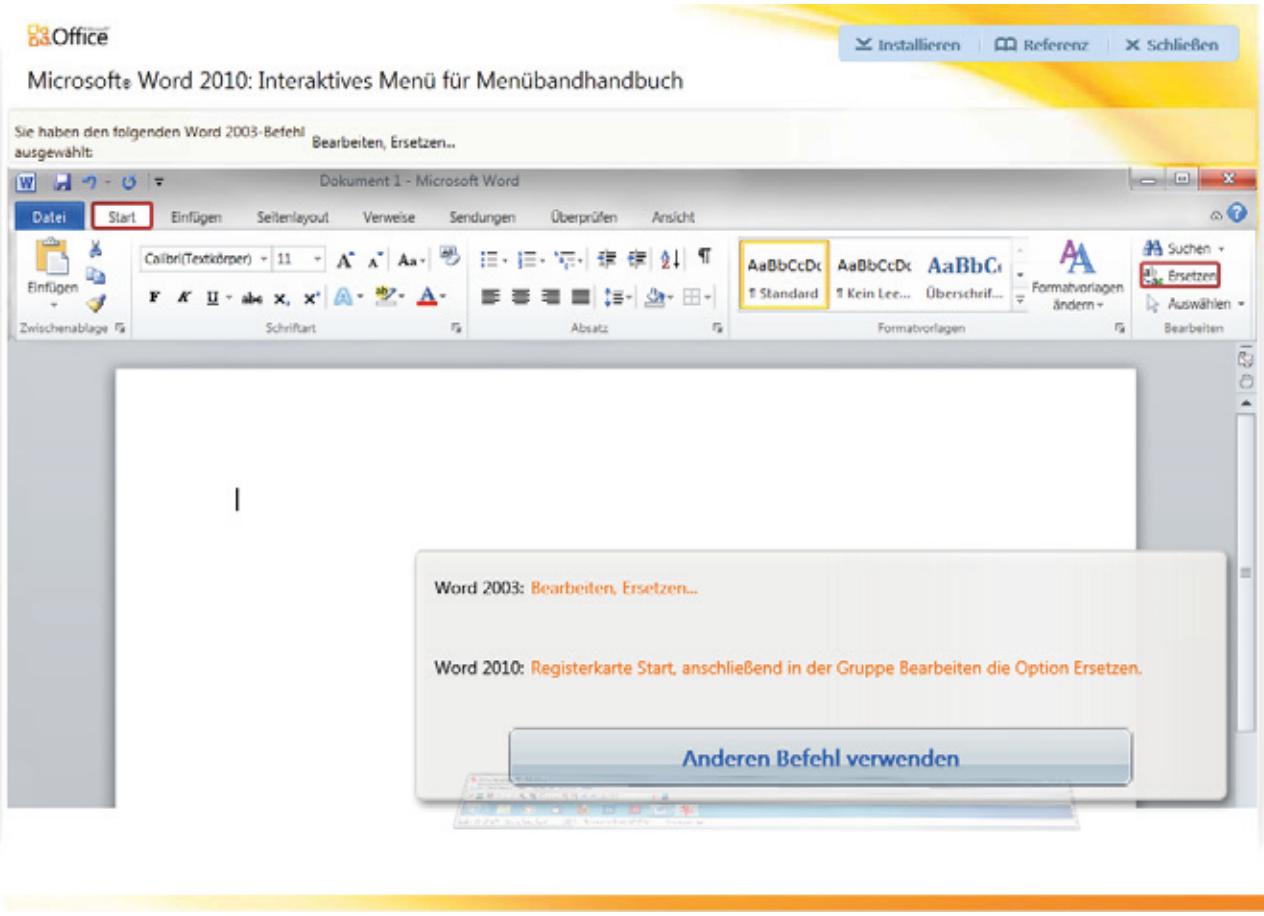
Kontakt:
Uwe Nolte
unolte@gwdg.de
0551 201-1547



2 *Ein nachgebildetes Word 2003 im Browser mit allen Menüs und Schaltflächen*



3 *Aus dem Bearbeiten-Menü wird „Ersetzen…“ ausgewählt*



4 *Durch einen roten Rahmen wird angezeigt, wo sich der Befehl in Word 2010 befindet*

Sicherheit und Vertraulichkeit: Grundlagen der Verschlüsselung

Damit in einem System vernetzter Rechner und im Internet Informationen wie Passwörter, Dokumente und elektronische Post sicher und vertraulich übertragen werden können, werden Verfahren der Kryptologie eingesetzt. In zwei Artikeln der GWDG-Nachrichten soll dem Leser das Thema Verschlüsselung vertraut gemacht werden. In diesem ersten Artikel soll mit der Darstellung der Grundlagen von Verschlüsselungstechniken eine solide theoretische Basis für den Umgang mit den Möglichkeiten, die die aktuellen Computersysteme für die tägliche Arbeit bieten, geschaffen werden. Im zweiten Artikel im nächsten Monat folgt dann eine Beschreibung der aktuellen Möglichkeiten und damit verbunden eine Anleitung zur Nutzung dieser Möglichkeiten, vor allem der Identitätsnachweis mit der digitalen Signatur und die Verschlüsselung von E-Mails.

Verschlüsselte Botschaften

Seit überhaupt Nachrichten geschrieben werden, ist es den Menschen ein Bedürfnis, diese gegebenenfalls auch zu verschlüsseln, denn Vertraulichkeit ist eine wichtige Grundlage für die Beziehungen zwischen Menschen. Auch im weiteren Rahmen zwischen Geschäftspartnern, Firmen, gesellschaftlichen Organisationen und den Staaten dieser Erde sollen vielfach Informationen vor in irgendeiner Weise konkurrierenden Gegnern oder auch Partnern geheim gehalten werden. Anfangs reichten neben dem Einfallsreichtum der Menschen die Schreibwerkzeuge, um Verschlüsselungen durchzuführen, später sind vorgefertigte Hilfsmittel wie Codescheiben und Codetabellen hinzugekommen. Seit Beginn des 20. Jahrhunderts werden elektromechanische Geräte benutzt, auch um sie an Geräte der Nachrichtenübertragung (wie z. B. Fernschreiber) anzuschließen. Normalerweise wurden die verschlüsselten Botschaften nicht nur vom vorgesehenen Empfänger entschlüsselt und gelesen – dieser hatte leichtes Spiel, denn er kannte den Schlüssel –, sondern auch von Leuten, denen die Information eigentlich vorenthalten bleiben sollte. Ein solcher unberechtigter Leser der verschlüsselten Nachricht musste gute Kombinationsfähigkeiten und Geduld besitzen, um schließlich den Klartext lesen zu können. Zum Verschlüsseln wurden zunehmend mathematische Verfahren eingesetzt und mit dem Aufkommen der Computer in der zweiten Hälfte des 20. Jahrhunderts übertrug man diesen die Aufgabe des Verschlüsseln, aber auch – was viel wichtiger war – die Aufgabe des Entschlüsselns, denn dazu war der menschliche Leser wegen des Umfangs des mathematischen Problems, vor das er gestellt war, nicht mehr in der Lage. Die größten Rechenanlagen – beginnend mit dem Colossos in England – wurden für diesen Zweck entwickelt.

Verschlüsselungstechniken werden auch verwendet, um die Identität eines Partners sicher feststellen zu können. Dies kann beim Nachrichtenaustausch über Entfernungen ein Geschäftspartner sein oder eine Institution, bei der man z. B. sicher sein möchte, dass die Webseite, die man angezeigt bekommt, auch wirklich von ihr stammt.

Rudolf Kippenhahn

Die Darstellung der Grundlagen von Verschlüsselungstechniken sind – mit freundlicher Genehmigung des Autors – zu wesentlichen Teilen dem im Rowohlt-Verlag erschienenen Buch „Verschlüsselte Botschaften“ entnommen. Der Autor Rudolf Kippenhahn, Jahrgang 1926, lebt im Göttinger Stadtteil Nikolausberg und lehrte von 1965 an als ordentlicher Professor an der Universität Göttingen. Von 1975 bis 1991 war er Direktor des Max-Planck-Instituts für Astrophysik in Garching bei München.

Das gerade genannte Buch bietet einen leichten Einstieg in das Thema und wird zur gründlichen Einarbeitung in die Kryptologie empfohlen. Einzelne Themen werden nochmals tiefer in den Büchern von Friedrich L. Bauer „Entzifferte Geheimnisse“ und Albrecht Beutelspacher „Kryptologie“ erklärt.

Mit Bleistift und Papier

Für die Durchführung von Ver- und Entschlüsselung reichte bis ins letzte Jahrhundert hinein Papier und Bleistift, hinzu kamen einfache Hilfsmittel. Beginnend mit dem ersten Weltkrieg wurden Maschinen für diesen Zweck konstruiert, z. B. die „Enigma“, die vom deutschen Heer und der Marine eingesetzt wurde. Über diese Maschinen soll hier aber nicht berichtet werden [1].

Die Geheimschrift von Julius Caesar

Wie von Sueton [2] überliefert wurde, hat Gaius Julius Caesar (100 bis 44 v. Chr.) vertrauliche Botschaften an Marcus Tullius Cicero (106 bis 43 v. Chr.) geschickt, die er in einer sehr einfachen Weise verschlüsselte: Die Vorschrift zur Caesar-Verschlüsselung (auch Caesar-Verschiebung genannt) lautete: „Statt dem Buchstaben des Klartextes schreibe den um k Stellen nachfolgenden Buchstabe des Alphabets." Und die sich ergebende Vorschrift zur Entschlüsselung: „Nehme den Buchstaben des Alphabets, der k Stellen vor dem Buchstaben dieses Geheimtextes steht."

In eine mathematische Formel gefasst, lauten die Vorschriften zur Chiffrierung und zur Dechiffrierung:

$$\text{encrypt}_k(P) = (p+k) \bmod 26$$

und

$$\text{decrypt}_k(C) = (c-k) \bmod 26,$$

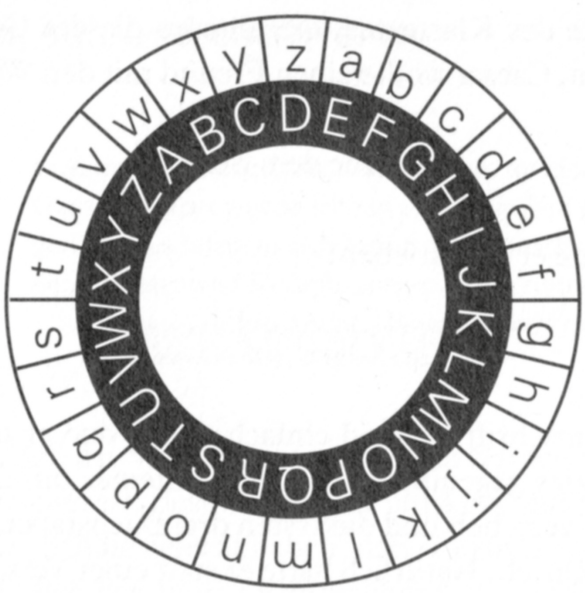
wobei beispielhaft c und p die Nummern der Buchstaben „C" und „P" im Alphabet sind und k der Schlüssel, eine Zahl zwischen 1 und 25. Die Anzahl der Buchstaben des Alphabets wird hier mit 26 angenommen. Allen Buchstaben wird eine Nummer zugewiesen, beginnend mit der 0 für das „A", und endet mit der 25 für das „Z". Die mathematische Operation „Modulo", angewendet auf diese Nummern, bedeutet, dass, wenn z. B. die Addition zweier Zahlen die Anzahl der möglichen Zahlen (hier 26) überschreitet, die Zahl 26 so oft abgezogen werden muss, dass das Ergebnis kleiner ist als 26.

Man nennt die Caesar-Verschlüsselung das Verschlüsselungsverfahren und die Zahl, um die verschoben werden soll, den Schlüssel. Während üblicherweise ein Verschlüsselungsverfahren über einen längeren Zeitraum hin gleichbleibend verwendet wird, sollte der Schlüssel häufiger gewechselt werden, möglicht von Nachricht zu Nachricht. Beispiel für die Caesar-Verschlüsselung des Buchstaben „W" mit dem Schlüssel 14: W + 14 = 22 + 14 = 36 ≡ 10 mod 26, die Geheimzahl ergibt sich zu 10, der daraus folgende Geheimbuchstabe ist „K".

Wenn also der Text der Botschaft lautete „Wir treffen uns morgen um sechs im Capitol" und die Verschlüsselungsvorschrift beinhaltete den Wert 3 für die Buchstabenverschiebung, so lautete der Geheimtext „Zlu wuhiiq xqv prujhq ..." .

Um leicht solche Verschlüsselungen durchführen zu können, fertigte man sich ein Hilfsmittel aus zwei gegeneinander verschieblichen Kreisen mit jeweils den Buchstaben des Alphabets an. Sie wurden dann um den Wert k gegeneinander verschoben und man konnte zu jedem Klartextbuchstaben den entsprechendenn Buchstaben des Geheimtextes ablesen – und umgekehrt.

Ein solches Hilfsmittel in Form einer runden Scheibe mit zwei gegeneinander verschiebbaren Ringen in Abb. 1 dargestellt:



1 *Chiffrierscheibe für die Caesar-Verschiebung*

Das Verschlüsselungsverfahren könnte man bei Verwendung eines solchen Hilfsmittels auf verschiedene Weise verändern: Man könnte z. B. auf dem inneren Kreis der Chiffrierscheibe die Geheimbuchstaben gegen den Uhrzeigersinn aufgetragen oder die Geheimbuchstaben in einer unregelmäßigen Reihenfolge (man nennt das „verwürfelt") anordnen.

Solche Verschlüsselungen sind besonders leicht zu knacken, wenn man erstmal auf die Idee mit den gegeneinander verschobenen Buchstaben des Alphabets kommt, denn bei 26 Buchstaben (wie in Abb. 1) braucht man nur 26 Versuche, um den Klartext angezeigt zu bekommen.

Textverschlüsselung mit Schlüsselwort

Statt einer Buchstabenfolge als Geheimtext versendet man auch gern eine Ziffernfolge. Dazu wird jeder

Buchstabe des Alphabets durch seine laufende Nummer ersetzt: A=1, B=2 usw.

Man kann die Sache aber auch verfeinern und den am häufigsten vorkommenden Buchstaben zunächst einmal die einstelligen Zahlen zuordnen. Das sind (im Englischen) die Buchstaben a, s, i, n, t, o, e und r, die dann die Ziffern von 0 bis 7 erhalten.

Die zweistelligen Zahlen für die anderen Buchstaben lässt man mit 8 und 9 beginnen. Zusätzlich kann man ein Schlüsselwort einbauen, mit dem man einzelne Buchstaben aus der vorgegebenen Reihenfolge des Alphabets herauslöst und an den Anfang stellt. Man nennt dies „Verwürfelung" des Alphabets und erreicht damit, dass je nach Länge des Schlüsselwortes weniger Buchstaben in der normalen Reihenfolge stehen. Das ist in Abb. 2, 3 und 4 gezeigt, wobei im Beispiel das Schlüsselwort „Democrats" lautet.

d	e	m	o	c	r	a	t	s	
b	f	g	h	i	j	k	l	n	
p	q	u	v	w	x	y	w	/	.

2 *Reihenfolge der Buchstaben des Alphabets mit dem Schlüsselwort „Democrats", dessen Buchstaben an den Anfang gestellt sind; als Satztrennzeichen sind der Schrägstrich und der Punkt hinzugefügt.*

Wenn man jetzt bei der Zuteilung von Nummern zu den Buchstaben beachtet, dass die Buchstaben a, s, i, n, t, o, e und r einstellig verschlüsselt werden sollen, ergibt sich die Zuordnung von Nummern zu den Buchstaben des Alphabets wie in Abb. 3 dargestellt. Vorangestellt ist das Schlüsselwort:

d	e	m	o	c	r	a	t	s	
	0		1		2	3	4	5	
b	f	g	h	i	j	k	l	n	
				6				7	
p	q	u	v	w	x	y	w	/	.

3 *Die am häufigsten vorkommenden Buchstaben (a, s, i, n, t, o und r) haben die Ziffern 0 bis 7 erhalten.*

Nun bekommen die restlichen Buchstaben mit den Ziffern 8 und 9 beginnende Zahlen zugewiesen.

Verwendet man nun die Verschlüsselungstabelle aus Abb. 4, so lautet der verschlüsselte Text, den der amerikanische Präsident abschickt („We meet tomorrow six o clock on capitol hill.") in Geheimschrift:

„97098810049841811221949856959819882891828898179882390641899886689899 9"

D	e	m	o	c	r	a	t	s	
80	0	81	1	82	2	3	4	5	
B	f	g	h	i	j	k	l	n	
83	84	85	86	6	87	88	89	7	
P	q	u	v	w	x	y	w	/	.
90	91	92	93	94	95	96	97	98	99

4 *Die am häufigsten vorkommenden Buchstaben haben die Ziffern 0 bis 7 erhalten; die weiteren Buchstaben erhalten die Nummern ab 80.*

Man nennt eine Verschlüsselung, in der einem bestimmten Klartext-Buchstaben des Alphabets immer wieder der gleiche Geheimbuchstabe zugeordnet wird, eine „monoalphabetische Verschlüsselung". Bei einer solchen Geheimschrift, in der einem Buchstaben genau immer wieder eine bestimmte Nummer zugeordnet ist, beginnt man – wenn man den Schlüssel nicht kennt – die Entschlüsselung mit einer Häufigkeitsanalyse. Von der am häufigsten vorkommenden Zahl nimmt man an, dass sie den Buchstaben „E" verschlüsselt usw. (s. Abb. 6).

0: 3 (e)	86: 1
1: 7 (o)	87: 0
2: 2	88: 1
3: 1	89: 4 (w)
4: 3 (t)	90: 1
5: 1	91: 0
6: 3 (i)	92: 0
7: 1	93: 0
80: 0	94: 1
81: 2	95: 1
82: 3	96: 0
83: 0	97: 1
84: 0	98: 8 (_)
85: 0	99: 1

5 *Häufigkeitsanalyse über den vorläufig verschlüsselten Text „We meet tomorrow six o clock on capitol hill."*

Man erreicht hier mit der Häufigkeitsanalyse allerdings noch nichts, denn der Text ist nicht lang genug, um ein statistisch auswertbares Ergebnis zu bekommen.

Da man also bei einem solcherart verschlüsselten Text, wenn er genügend lang ist und wenn man zu-

dem in Rechnung stellt, dass mit den Ziffern 8 und 9 jeweils ein Ziffernpaar beginnt, bei der Entschlüsselung recht leichtes Spiel hat, wird noch eine zusätzliche Verschüsselung vorgenommen, was im nächsten Abschnitt dargestellt wird.

Die einzelnen Buchstaben des Alphabets einer Sprache treten in jeder Sprache mit einer für diese charakteristischen Häufigkeit auf. In der Tabelle in Abb. 6 ist die prozentuale Häufigkeit der Buchstaben des Alphabets in einem deutschen Text angegeben. Dabei sind die Umlaute ä, ö und ü durch ae, oe und ue und das ß durch ss ersetzt. [3]

1.	e	17,40
2.	n	9,78
3.	i	7,55
4.	s	7,27
5.	r	7,00
6.	a	6,51
7.	t	6,15
8.	d	5,08
9.	h	4,76
10.	u	4,35
11.	l	3,44
12.	c	3,06
13.	g	3,01
14.	m	2,53
15.	o	2,51
16.	b	1,89
17.	w	1,89
18.	f	1,66
19.	k	1,21
20.	z	1,13
21.	p	0,79
22.	v	0,67
23.	j	0,27
24.	y	0,04
25.	x	0,03
26.	q	0,02

6 *Häufigkeit der Buchstaben in einem durchschnittlichen deutschen Text*

Wer nun im Geheimtext für das Zeichen mit der größten Häufigkeit den Klartextbuchstaben „e“ einsetzt, hat einen Anfang zur Entschlüsselung des Textes gemacht und kann sich nun mit Hilfe der Tabelle weiter vorantasten. Weitere Häufigkeiten in der deutschen Sprache können einfließen:

1. Die häufigsten Buchstabenpaare: en, er, ch, te, de, nd, ei, ie, in, es,...

2. Die auf den Buchstaben e am häufigsten folgenden Buchstaben: n, r, i, s

3. Die häufigsten kurzen Wörter: die, der, zu, in, ein, an, den, auf, das,...

Um dem unbefugten Entschlüsseler die Arbeit zu erschweren, könnte man nun dafür sorgen, dass die häufigsten Buchstaben abwechselnd durch mehrere Geheimbuchstaben ersetzt werden. Das ist dann gut möglich, wenn an Stelle der Buchstaben im Geheimcode Zahlen gesetzt werden.

Je länger das Schlüsselwort, desto mehr werden die Häufigkeiten der Buchstaben in einem Text aneinander angeglichen. Bei polyalphabetischen Verschlüsselungen wiederholen sich die Schlüsselbuchstaben periodisch, wobei die Periode die Länge des Schlüsselwortes ist. Je länger der Schlüssel, desto schwieriger die Entschlüsselung.

Man könnte auch ein Schlüsselwort dafür verwenden, dass man den Klartext nicht mit einem gegen das Klartextalphabet verschobenen (Caesar) oder verwürfelten Alphabet verschlüsselt, sondern mit mehreren unterschiedlich verschobenen oder verwürfelten Alphabeten, gesteuert durch ein Schlüsselwort. Dann ergibt sich eine polyalphabetische Verschlüsselung und mit einer Häufigkeitsanalyse ist nichts mehr zu erreichen beim Entschlüsseln.

Vor der Übermittlung des Geheimtextes muss der Sender also dem Empfänger neben dem verschlüsselten Text das Verschlüsselungsverfahren und den Schlüssel mitteilen. Das Verfahren kann abgesprochen sein und über einen längeren Zeitraum gleich bleiben – muss auch kein Geheimnis sein –, der Schlüssel dagegen sollte von Nachricht zu Nachricht wechseln und dem Empfänger möglichst nicht mit der gleichen Post mitgeteilt werden wie die Nachricht.

Textverschlüsselung mit sehr langem Schlüssel

Während das Verschlüsselungsverfahren abgesprochen wird und auf längere Zeit gleich bleiben kann,

muss neben dem verschlüsselten Text der Absender dem Empfänger natürlich den Schlüssel mitteilen. Dies kann zum einen eine mündliche Verabredung sein, die für viele verschlüsselte Sendungen gelten soll, wie hier im Beispiel das Wort „Democrats". Für eine deutlich bessere Verschlüsselung gehört zu dieser Verabredung zum Beispiel, dass man neben der Verwürfelung des Alphabets einen möglicht langen Schlüssel wählt, z. B. einen Text aus einem bestimmten Roman, den auch der Empfänger in seinem Bücherregal stehen hat – etwa „Das Glasperlenspiel" von Hermann Hesse.

Man vereinbart, dem Roman einen Text zu entnehmen, beginnend auf einer bestimmten Seite und genau so lang, wir der zu verschlüsselnde Text. Die Seitenzahl wird dem fertigen Geheimtext schließlich vorangestellt, z. B. 069, d. h., zum Verschlüsseln wird der Text ab Seite 69 aus „Das Glasperlenspiel" genommen: „Im Übrigen war für Knecht das Internatsleben nichts Neues; er ordnete sich ohne Mühe ein. ..." Man sieht, dass auch für die Behandlung der deutschen Umlaute eine Verabredung getroffen werden muss, ebenso auch für die Satzzeichen. Diese Verabredung soll hier lauten: Umlaute mit zwei Buchstaben ausschreiben, also Ä = AE, und Satzzeichen bis auf den Wortzwischenraum und den Punkt ignorieren. Die Ziffernfolge des Schlüsseltextes ergibt nun bei Verwendung der Verschlüsselungstabelle aus Abb. 4:

„68198 9208326850798 973298 84920298 88708286498 803598 674025345890830798 76...".

Nach der 96. Ziffer wird abgebrochen. Zur Übersichtlichkeit sind hier noch Leerzeichen hinter den verschlüsselten Wörtern gesetzt.

Der vorläufig verschlüsselte Text (zum Klartext „We meet tomorrow six o clock on capitol hill", siehe Abschnitt „Textverschlüsselung mit Schlüsselwort") wird nun mit seiner Folge aus 69 Ziffern hingeschrieben und darunter die Ziffernfolge des Schlüsseltextes. Dann werden die jeweils übereinanderstehenden Ziffern miteinander addiert. Gibt es einen Übertrag in die Zehnerstelle, wird dieser einfach weggelassen (Für jeder Ziffer wird also eine Addition „modulo 10" durchgeführt.). Es ergibt sich folgendes Bild (s. Abb. 7).

Die Seitenzahl, von der der Schlüsseltext stammt, wird dem Geheimtext vorangestellt. Sie wird verschlüsselt, indem die ersten drei Ziffern des Geheimtextes hinzuaddiert werden, wieder jede Ziffer für sich und modulo 10. So wird aus der Seitennummer in verschlüsselter Form: 069 plus 551 ergibt 510.

```
Erste 23 Ziffern:
 97098810049841811221949
+68198920832685079897329
=55186730871426880018268
;
folgende 23 Ziffern:
 85695981988289182889817
+88492029888708286498803
=63087900766987368277610
;
letzte 23 Ziffern
..98823906418998866898999
+59867402534589083079876
=47680308942477849867765
```

7 *Die Erzeugung des veschlüsselten Textes durch ziffernweise Addition eines Schlüsseltextes modulo 10.*

Folgende verschlüsselte Nachricht wird nun vom Sender an den Empfänger geschickt (69 Ziffern Text und vorangestellt 3 Ziffern der Seitenzahl):

„510551867308714268800182686308790076698736827761047680308942477849867765"

Die Häufigkeitsanalyse ergibt:

0: 8 (e)	86: 2
1: 5 (o)	87: 2
2: 2	88: 1
3: 4	89: 1
4: 4	90: 1
5: 4	91: 0
6: 9 (i)	92: 0
7: 10 (n)	93: 0
80: 1	94: 0
81: 0	95: 0
82: 2	96: 0
83: 0	97: 1
84: 1	98: 2 (_)
85: 0	99: 0

8 *Häufigkeitsanalyse über den fertig verschlüsselten Text „We meet tomorrow six o clock on capitol hill."*

Eine Häufigkeitsanalyse kann nun nicht mehr bei der Entschlüsselung des Textes helfen. Obwohl die Ziffern ohne vorangestellte 8 oder 9 hier auch am häufigsten vorkommen, entsprechen sie nicht den Klartextbuchstaben aus Abb. 4.

Der vorgesehene Empfänger weiß, wie er aus den ersten drei Ziffern die Seitenzahl im Buch „Das Glasperlenspiel" ermittelt: Er zieht von der verschlüsselten Seitenzahl (510) die Ziffern 5, 5 und 1 ab, jeweils modulo 10. Er erhält 5 – 5 = 0, 1 – 5 ≡ 6 (mod 10) und 0 – 1 ≡ 9 (mod 10), also 69. Auf dieser Seite links oben findet er im Roman „Das Glasperlenspiel" den Schlüsseltext. Dann nimmt er seine Verschlüsselungstabelle mit dem Schlüsselwort „Democrats" zur Hand (Tabelle in Abb. 4) und erzeugt damit die Ziffernfolge für den Schlüssel „68198 9208326850798 973298 84920298 88708286498 803598 674025345890830798 7", wie es auch der Absender getan hat. Diese Ziffernfolge wird nun Ziffer für Ziffer modulo 10 vom empfangenen Geheimtext abgezogen: 5 – 6 ≡ 9 (mod 10), 5 – 8 ≡ 7 (mod 10), 1 – 1 = 0, 8 – 9 ≡ 9 (mod 10), 6 – 8 ≡ 8 (mod 10), 7 – 9 ≡ 8 (mod 10), 3 – 2 = 1, 0 – 0 = 0, 8 – 8 = 0, 7 – 3 =4, 1 – 2 ≡ 9 (mod 10), 4 – 6 ≡ 8 (mod 10), 2 – 8 ≡ 4 (mod 10), usw.. Aus der nun erzeugten Ziffernfolge „970988100498418112..." wird wieder der Klartext, wenn man die Tabelle in Abb. 4 zur Hilfe nimmt: „we/meet/tomor...".

Dies ist also ein brauchbares, kaum zu knackendes Verschlüsselungsverfahren, zu dem keine besonderen Hilfsmittel benötigt werden.

Wenn man nun als Schlüssel nicht einen in Ziffern übersetzten Text nimmt, sondern von vornherein eine Ziffernfolge, eröffnet sich eine Reihe von Möglichkeiten für möglichst lange Schlüssel, deren Ziffern keinerlei Muster aufweisen. Nimmt man den Bruch 1/7, so erhält man zwar eine unendlich lange Ziffernfolge, aber – was der Nachteil ist – mit einer recht kurzen Periode:

1/7 = 0,142857142857142857...

Ein Schlüssel mit einer so kurzen Periode – 142857 – ist recht unbrauchbar. Der Bruch 1/499 liefert dagegen eine Folge von 498 nichtperiodischen Ziffern, die sich erst nach der 499. Ziffer wiederholen. Gut könnte man auch eine unendlich sich nichtperiodisch fortsetzende Ziffernfolge wie die Zahl „Pi" [4] oder die Zahl „e" [5] verwenden. Hier muss man aber, um von Nachricht zu Nachricht einen anderen Schlüssel zu haben, z. B. mitteilen, von welcher Nachkommastelle an der Schlüssel beginnen soll – oder man vereinbart eine Rechenoperation mit dieser transzendenten Zahl, z. B. 7 x Pi oder 3/e.

Eine gute Idee für eine lange Folge zufälliger Ziffern ist es auch, das Telefonbuch einer großen Stadt zur Hand zu nehmen. Allerdings darf man nur die zwei oder drei niedrigstwertigen Ziffern jeder Nummer nehmen, da die höherwertigen sich vielfach wiederholen, weil sie für größere Stadtgebiete jeweils gleich sind. Wenn man nun ein bestimmtes Telefonbuch vereinbart hat, muss man dann als Schlüssel nur noch den Namen angeben, bei dem begonnen werden soll.

Prüfung auf Echtheit von Nummern

An vielen Stellen will man sicher gehen, dass eine bestimmte Zahl korrekt ist und nicht durch einen Übermittlungsfehler oder eine bewusste Verfälschung verändert wurde. Solche Zahlen sind zum Beispiel Kontonummern, die Fahrzeug-Nummern bei der Eisenbahn oder die ISBN-Nummern (ISBN = International Standard Book Number) zur Bestellung eines Buches. Man nennt solche Nummern „kodierte Nummern". Eine empfangene Nummer kann mit einer bestimmten Vorschrift überprüft werden. Zeigt sich ein bestimmtes Ergebnis, dann kann man sehr sicher sein, dass keine Ziffern vertauscht oder verändert wurden.

Beispielhaft sei das für die Nummer einer VISA-Karte gezeigt: Die Nummer lautet:

8259 4280 4533 1182

Die Prüfvorschrift lautet: Man schreibe von rechts nach links die Ziffern in eine zweite Zeile unter die Zahl, indem man nach der ersten jeweils eine Ziffer überspringt:

8259 4280 4533 1182
_2_9 _2_0 _5_3 _1_2

Dann fülle man die Lücken mit der verdoppelten oben stehenden Ziffer auf. Ergibt sich eine Zahl größer als 9, ziehe man 9 davon ab (Addition modulo 9):

8259 4280 4533 1182
7219 8270 8563 2172

Wenn man nun die Ziffern der unteren Zeile alle zusammenaddiert, muss sich eine durch 10 teilbare Zahl ergeben. Das ist hier der Fall:

7 + 2 + 1 + 9 + 8 + 2 + 7 + 0 + 8 + 5 + 6 + 3 + 2 + 1 + 7 + 2 = 70

Ein Schwachpunkt dieser Prüfung: Werden Zahlen paarweise vertauscht, funktioniert die Kontrolle nicht.

Die Prüfung der ISBN 3-499-60807-3 sieht wie folgt aus:

Erste Ziffer mit 10 multiplzieren, die zweite mit 9, die dritte mit 8,... und die vorletzte mit 2. Werden die Ergebnisse aufsummiert und zur letzten Ziffer addiert, muss eine durch 11 teilbare Zahl herauskommen, sonst stimmt irgendetwas nicht.

Hier ergibt sich: 30 + 36 + 72 + 63 + 36 + 0 + 32 + 0 +1 + 3 = 286

Das Ergebnis 286 ist durch 11 teilbar, ohne dass ein Rest bleibt. Man erhält also bei Angabe der ISBN-Nummer 3-499-60807-3 mit Sicherheit das Buch „Verschlüsselte Botschaften" von Rudolf Kippenhahn.

Prüfung auf Echtheit von Texten

Wenn man eine wichtige Entdeckung gemacht hat, wie z. B. „die Erde dreht sich um die Sonne", und will erreichen, dass man eines Tages nachweisen kann, als erster dies erkannt zu haben, bildet man aus dieser Aussage ein Anagramm. Dies geschieht in der Weise, dass man alle Buchstaben dieser Aussage in alphabetische Reihenfolge bringt: „cddddeeeeeehhiiikmonnrrsstu". Der Übergang zum Anagramm ist eine Einwegfunktion, d. h., man kommt vom Anagramm nicht zurück zum Ausgangstext. Verwahrt der Entdecker das Anagramm und jemand behauptet irgendwann, er hätte entdeckt, dass sich die Erde um die Sonne dreht, so kann er anhand des Anagramms beweisen, dass diese Feststellung schon von ihm vor einiger Zeit gemacht wurde.

Das Anagramm ist nun ein sehr einfaches Verfahren. Zur Realisierung von Einwegfunktionen gibt es Verfahren, Hash-Funktionen genannt, die einen langen Text extrem verkürzen. Sie erzeugen eine Zeichenkette bestimmter Länge, die einzigartig ist und die Wahrscheinlichkeit ist extem gering, dass irgendein anderer Text zur gleichen Zeichenfolge führt, wenn man die gleiche Hash-Funktion auf ihn anwendet. Man nennt eine solche, durch eine Hash-Funktion entstandene Zeichenkette „Fingerprint", also „Fingerabdruck". Schon ein Vertauschen zweier Buchstaben im Text führt zu einem anderen „Fingerprint". Ein solches Verfahren dient dazu, zu erkennen, ob ein Text von Sender zum Empfänger gelangt ist, ohne dass er unterwegs irgendwie verändert wurde.

Solche Fingerprints werden z. B. in Banken verwendet, wo die PIN einer Bankkarte nicht gespeichert wird – auch nicht verschlüsselt –, sondern als Hash-Wert.

Speichern von Passwörtern

Die zur Zugangskontrolle dienenden Passwörter werden in Rechnersystemen nicht abgespeichert – weder im Klartext, noch in verschlüsselter Form. Stattdessen wird mit einem bestimmten Verfahren ein Hash-Wert gebildet und dieser abgespeichert. Der Hash-Wert hat eine bestimmte Länge und ist – unabhängig von dessen Länge – meist länger als das Passwort. Wenn nun bei einer Anmeldung das Passwort eingegeben wird, wird der Hash-Wert gebildet und mit dem abgespeicherten Hash-Wert verglichen. Stimmt beides überein, ist das Passwort mit äußerster Sicherheit das richtige gewesen.

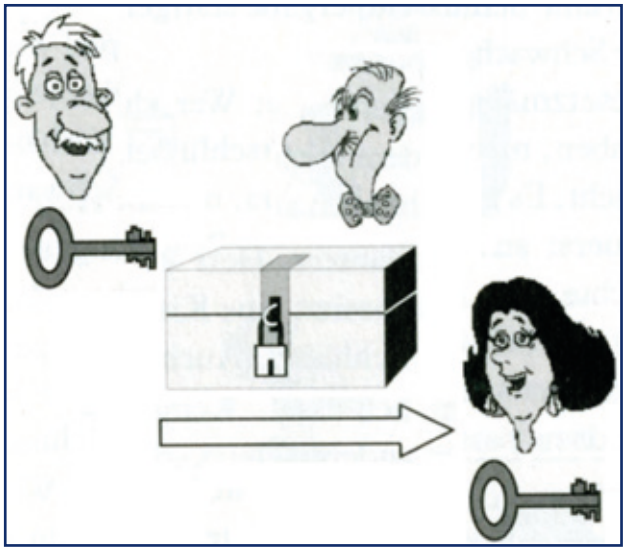
Besondere Schlüssel

Wenn sich zwei Personen geheime Botschaften zusenden wollen, ist klar, dass sie vorher ein Verfahren zur Verschlüsselung vereinbaren. Darüber hinaus ist es notwendig, dass sie beide den gleichen Schlüssel verwenden, und zwar möglichst für jede Nachricht einen neuen Schlüssel. Wenn es nämlich einem unerwünschten Mitleser der verschlüsselt übertragenen Nachricht gelingt, die Nachricht zu entschlüsseln, erfährt er dabei normalerweise auch den Schlüssel. Wenn jede Nachricht mit einem neuen Schlüssel kodiert wird, hat der unbefugte Mitleser immer wieder den gleichen Aufwand für die Entschlüsselung. Das Problem ist die Übersendung des Schlüssels. Der unbefugte Eindringling könnte in Erfahrung bringen, wie er jedes Mal wieder in den Besitz des Schlüssels kommt.

Im Folgenden soll auf einfache Weise gezeigt werden, wie man zu einem sicheren Schlüsselsystem kommt.

Symmetrische Verschlüsselung mit einem Schlüssel

In den bisher beschriebenen Verfahren ist jeweils die symmetrische Verschlüsselung verwendet worden. Das bedeutet, dass sowohl der Absender einer Nachricht als auch der Empfänger den gleichen Schlüssel besitzen und benutzen. Mit ihm können sie geheime Nachrichten austauschen, die niemand anderes lesen kann, es sei denn, er hätte den Schlüssel einmal in seine Hand bekommen und sich ein drittes Exemplar in Kopie hergestellt. In Abb. 9 ist diese einfachste Form der Versendung einer geheimen Nachricht dargestellt. Verwendet man das Bild einer Kassette mit einem dazugehörigen Schlüssel, in dem die geheime Nachricht verschickt wird, dann erscheint es unwahrscheinlich, dass ein Dritter in den Besitz eines dritten Schlüssels kommt. Übertragt man allerdings dieses Bild auf eine Nachrichtenübertragung mit modernen Medien, so kann es ganz leicht sein, den geheimen Schlüssel zu kopieren, denn, wenn er als Bitmuster über ein Übertragungsmedium versendet wird, kann derjenige, der das Übertragungsmedium in irgend einer Weise anzapft, leicht eine Kopie dieses Bitmusters machen.



9 *Herr Weiß verschließt die Truhe mit der geheimen Nachricht mit seinem Schlüssel, Frau Schwarz kann mit ihrem Schlüssel öffnen. Herr Grau kann die Nachricht nicht lesen.*

Da hier eine verschließbare Kassette mit dem Klartext darin verschickt wird, können sowohl Frau Schwarz als auch Herr Weiß, die beide den passenden (gleichen) Schlüssel besitzen, die Kassette aufschließen, einen Brief hineinlegen oder entnehmen. Herr Grau, der den passenden Schlüssel nicht besitzt, kann den Brief nicht lesen, auch wenn er die Kassette in die Hände bekommt.

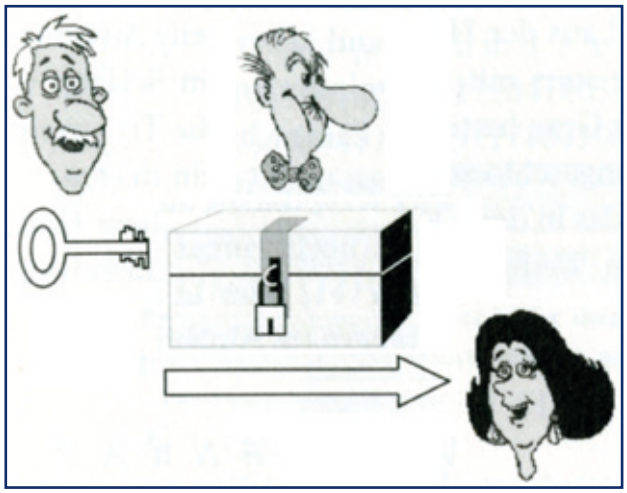
Nachteil dieses Verfahrens ist, dass der Schlüssel auf irgendeine sichere Weise übergeben werden muss.

Dieser Nachteil wird beseitigt, wenn das Verfahren etwas aufwändiger gestaltet wird. Es sind jetzt nicht mehr zwei gleiche Schlüssel bei beiden Partnern.

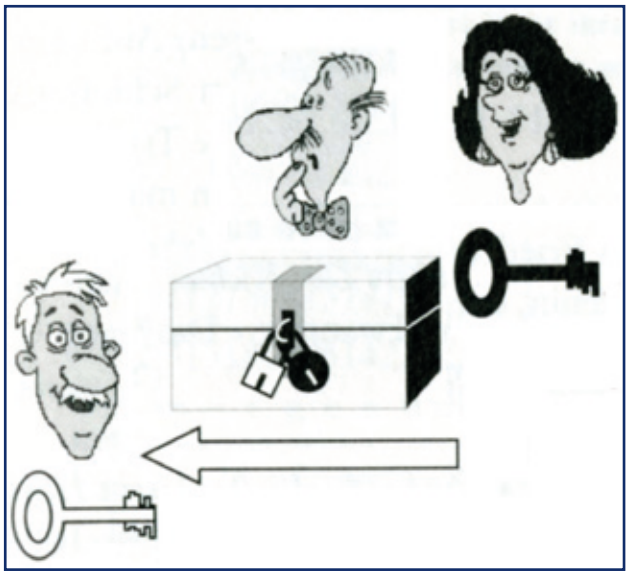
Symmetrische Verschlüsselung mit zwei Schlüsseln

Auch dieses Verfahren soll wieder mit dem Brief in der verschlossenen Kassette veranschaulicht werden. Angenommen, Herr Weiß will an Frau Schwarz eine geheime Botschaft versenden. Er verschließt das Schloss mit seinem Schlüssel und schickt die Kassette an Frau Schwarz. Frau Schwarz kann die Kassette nicht öffnen, denn sie hat keinen passenden Schlüssel. Sie hängt aber ein weiteres Schloss an die Kassette, welches sie mit ihrem dazu passenden Schlüssel verschließt. Nun schickt sie die Sendung an Herrn Weiß zurück. Dieser entfernt sein Schloss und schickt die Kassette, die nun nur noch das Schloss von Frau Schwarz aufweist, ein zweites Mal zu Frau Schwarz. Diese kann das Schloss (ihr Schloss) mit ihrem Schlüssel öffnen und den Brief lesen: „Treffen morgen um drei". Schade, das war vorgestern. Das Hin- und Hersenden hat zu lange gedauert. Eine umständliche Prozedur, aber keiner der Beteiligten hat seinen Schlüssel aus der Hand geben müssen.

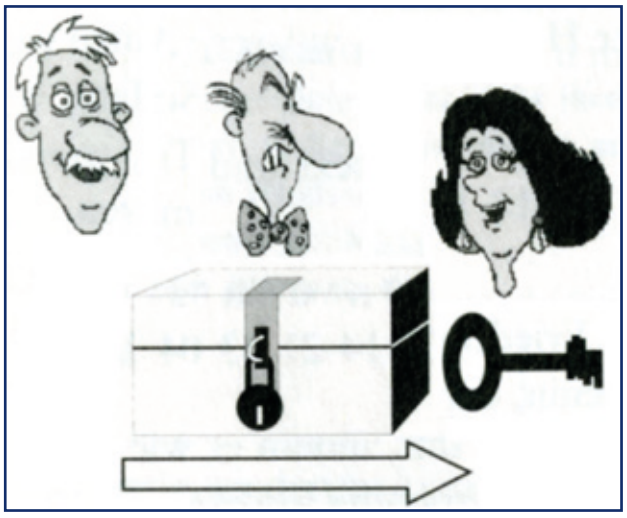
Mittels moderner Übertragungstechnik läuft dieses Verfahren natürlich schneller ab.



10 *Herr Weiß verschließt die Truhe mit der geheimen Nachricht mit seinem Schlüssel, Frau Schwarz empfängt die verschlossene Kassette und holt ihr Schloss und ihren Schlüssel. Herr Grau hat keine Chance.*



11 *Frau Schwarz verschließt die Truhe mit ihrem Schloss und ihrem Schlüssel, Herr Weiß empfängt die doppelt verschlossene Kassette, öffnet sein Schloss, nimmt es ab und schickt die Kassette an Frau Schwarz. Herr Grau wundert sich.*



12 *Frau Schwarz empfängt die Kassette, die nur noch mit ihrem eigenen Schloss gesichert ist. Sie öffnet die Kassette mit ihrem Schlüssel und liest die Nachricht von Herrn Weiß. Herr Grau hatte keine Chance, die Kassette zu öffnen.*

Herr Weiß kodiert seine Mitteilung „Treffen morgen um drei." mit der Tabelle aus Abb. 4. Es ergibt sich als vorläufige Verschlüsselung die Ziffernfolge:

42084840798811285079892819880206 99

Diese wird nun noch (auf gleiche Weise wie in Abschnitt „Textverschlüsselung mit sehr langem Schlüssel" beschrieben) mit dem Text von Seite 69 des Romans „Das Glasperlenspiel" („Im Übrigen war für Knecht das Internatsleben nichts Neues; er ordnete sich ohne Mühe ein. ...") verschlüsselt, und zwar durch ziffernweise Addition modulo 10:

42084840798811285079892819880206 99
+68198920832685079897329884920298 88
=00172760520496254866111693700494 77

So versendet nun Herr Weiß die verschlüsselte Nachricht. Der heimliche Mitleser Herr Grau kann sie nicht lesen, weil er den Schlüssel nicht kennt, aber auch nicht Frau Schwarz, denn sie hat den Schlüssel ebenfalls nicht.

Sie verschlüsselt nun den Text ein weiteres Mal mit einem Schlüssel, den nur sie kennt und niemandem mitteilen wird. Sie nimmt für diese kurze Nachricht den Spruch „Morgenstund ist aller Laster Anfang." (36 Buchstaben), den sie mit der Tabelle in Abb. 4 verschlüsselt:

M	o	r	g	e	n	s	t	u	n	d	/
81	1	2	85	0	7	5	4	92	7	80	98
l	s	t	/	a	l	l	e	r	/		
6	5	4	98	3	89	89	0	2	98		
L	a	s	t	e	r	/	A	n	f	a	n
89	3	5	4	0	2	98	3	7	84	3	7

Die sich ergebende Ziffernfolge „8112850…" addiert Frau Schwarz zum Geheimtext, den sie von Herrn Weiß erhalten hat (wieder ohne Zehnerübertragung):

00172760520496254866111693700494 77
+81128507549278098654983898902988 93
=81290267069664242410094481602372 60

Das Ergebnis, die Ziffernfolge „8129026…" sendet sie Herrn Weiß zurück. Dieser entfernt nun seinen Schlüssel, indem er die Ziffernfolge „681989..." modulo 10 abzieht:

81290267069664242410094481602372 60
-68198920832685079897329884920298 88
=23102347237089273623775607782184 82

Der nun entstandene Geheimtext, der nur noch den Schlüssel von Frau Schwarz enthält und nicht mehr den von Herrn Weiß, wird nun wieder an Frau Schwarz übermittelt. Die zieht ihren Schlüssel „Morgenstund…" wieder ab:

23102347237089273623775607782184 82
-81128507549278098654983898902988 93
=42084840798811285079892819880206 99

Die entstandene Ziffernfolge muss nun unter Zuhilfenahme von der Tabelle in Abb. 4 wieder in einen Klartext übersetzt werden:

4	2	0	4	84	0	7	98	81	1
t	r	e	t	f	e	n	/	m	o
2	85	0	7	98	92	81	98	80	2
r	g	e	n	/	u	m	/	d	r
0	6	99							
e	i	.							

Also: „Treffen morgen um drei."

Dieses zweimalige Hin- und Herschicken der Nachricht fällt sicher bei elektronischer Übertragung nicht als Nachteil ins Gewicht. Aber es gibt einen gewichtigen Schwachpunkt. Wenn Herr Grau die erste Nachricht von Herrn Weiß an Frau Schwarz abfängt und auch die zurückkommende Nachricht, kann er aus der Subtraktion beider verschlüsselten Nachrichten den Schlüssel von Frau Schwarz bestimmen. Fängt er dann auch noch die von Herrn Weiß an Frau Schwarz zurückgehende Nachricht auf, die nur noch ihren Schlüssel enthält, bekommt er den Klartext, weil er ja ihren Schlüssel ermittelt hat.

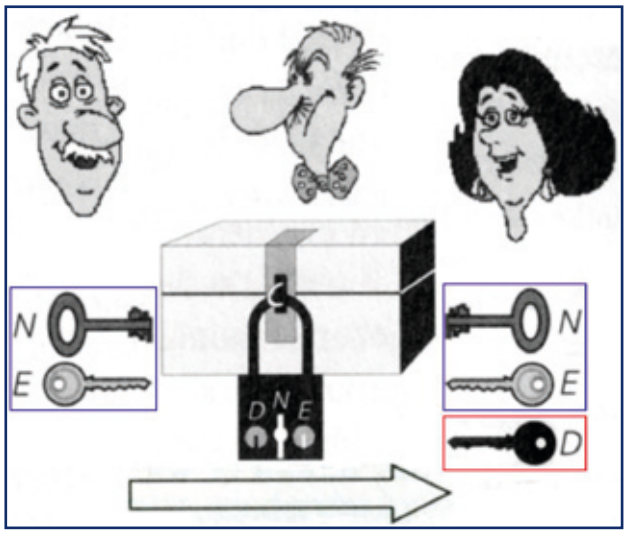
Asymmetrische Verschlüsselung mit drei Schlüsseln

Ein wiederum besseres Verschlüsselungsverfahren, bei dem der Schlüssel nicht ausgetauscht werden muss, erfordert ein besonderes Schloss an der Kassette, nämlich eines mit drei Schlüssellöchern für drei verschiedene Schlüssel.

13 *Das Wunderschloss mit seinen drei Schlüsseln D, E und N*

Wir bekommen dazu einen großen Schlüssel, mit N bezeichnet, und zwei kleinere Schlüssel, die Schlüssel D und E. Die Besonderheit des Schlosses: Wer das Schloss verschließen will, muss das mit dem großen Schlüssel N und einem der beiden kleineren Schlüssel D oder E tun. Nun lässt es sich aber nicht mit den gleichen Schlüsseln wieder öffnen. Wurde es mit D und N verschlossen, kann es nur mit E und N wieder geöffnet werden. Wurde es dagegen mit N und E verschlossen, so kann es nur mit N und D wieder geöffnet werden.

Angenommen, Frau Schwarz hat sich, um geheime Sendungen verschicken zu können, eine Kassette mit einem solchen Wunderschloss gekauft. Dazu wurden ihr die drei Schlüssel D, E und N geliefert. Die Bedienungsanleitung empfiehlt ihr, den Schlüssel D als ihren geheimen Schlüssel anzusehen und gut zu verwahren. Von den beiden Schlüsseln E und N lässt sie viele Duplikate herstellen, von denen sie jeweils ein Paar an ihre Freunde und Geschäftspartner schickt.



14 *Herr Weiß verschließt die Kassette mit dem Wunderschloss und den öffentlichen Schlüsseln von Frau Schwarz; Frau Schwarz benötigt zum Öffnen ihren geheimen Schlüssel D.*

Herr Weiß kann ihr nun also die Kassette zusenden, nachdem er das Schloss mit den öffentlichen Schlüsseln N und E von Frau Schwarz verschlossen hat. Er kann das Schloss anschließend selbst nicht mehr öffnen, denn das geht nur mit dem geheimen Schlüssel D von Frau Schwarz. Nachdem die Kassette bei Frau Schwarz eingetroffen ist, öffnet sie diese mit den Schlüsseln N und D und liest die geheime Botschaft. Wäre Herr Grau in den Besitz der verschlossenen Kassette gekommen, hätte er sie nicht öffnen können, denn dies geht nicht mit dem öffentlichen Schlüssel, mit dem sie verschlossen wurde.

Jetzt wollen wir von dem Bild mit der verschlossenen Kassette Abschied nehmen und uns einen Brief vorstellen, in dem ein geheimer Text einfach nur als Zahlenfolge versendet wird.

Für die drei Schlüssel werden drei „magische" Zahlen verwendet. Es sind große Zahlen und „magisch" deswegen, weil Sie in besonderer Beziehung zueinander stehen; sie sind nämlich nach einem besonderen Verfahren aus zwei Primzahlen berechnet worden. Das Verfahren kann man im Buch „Verschlüsselte Botschaften" von Rudolf Kippenhahn im Anhang C nachlesen. Magische Zahlen sind z. B. N=49048499, E=61 und D=2409781 [6]. Tatsächlich werden heute zur Verschlüsselung enorm große Zahlen verwendet, derzeit stehen 2.048 Bits zur Verfügung, um die Zahl N zu bilden.

Im folgenden Beispiel sollen, damit es leicht nachvollziehbar ist, sehr kleine Schlüsselzahlen verwendet werden, die aber auch magische Zahlen sind: N=85, D=13, E=5. Der öffentliche Schlüssel von Frau Schwarz sei also N=85 und E=5. Diese beiden Zahlen kann sie an alle Bekannten und Geschäftspartner senden, die dann mit Hilfe dieses – ihres öffentlichen Schlüssels – an Frau Schwarz verschlüsselte Botschaften senden können.

Wir wollen im Beispiel nur einen einzelnen Buchstaben verschlüsseln, um das Prinzip zu zeigen. Nehmen wir den Buchstaben „C". Herr Weiß verschlüsselt also ein „C" mit dem öffentlichen Schlüssel von Frau Schwarz:

Legen wir zur Umwandlung der Buchstaben des Alphabets wieder die Tabelle in Abb. 4 zu Grunde, ergibt sich für C die Zahl 82. Die Vorschrift verlangt, dass Herr Weiß diese Zahl zur E-ten (also 5-ten) Potenz nimmt, es ergibt sich 82 x 82 x 82 x 82 x 82 = 3707398432. Die verschlüsselte Form des Buchstaben C soll nun der Rest sein, der bei der Teilung des Ergebnisses 82^5 durch die Schlüsselzahl N (= 85) übrig bleibt, also $C' \equiv 82^5 \pmod{85} = 12$.

Statt, wie in diesem Beispiel, nur einen Buchstaben wird man natürlich in der Praxis einen längeren Text verschlüsseln wollen. Diesen sollte man nun nicht Buchstabe für Buchstabe verschlüsseln, denn dann hätten wir eine monoalphabetische Verschlüsselung, die man mit einer Häufigkeitsanalyse leicht knacken kann. Man sollte vereinbaren, Gruppen von vier oder fünf Buchstaben zusammenzufassen. Dabei muss dann die Schlüsselzahl N nicht nur mindestens genau so viele Ziffern haben, wie die aus dem Klartext erzeugte Zahl, sondern sie muss für jede Buchstabengruppe auch größer sein. (Bei der hier verwendeten Alphabetsverschlüsselung ist N kleiner als die höchste vorkommende Schlüsselzahl, nämlich 99. Das Tripel D, E und N ist also hier gar nicht geeignet!) Beim Berechnen der Geheimzahl und beim Entschlüsseln erhält man sehr große Zahlen. Damit die Zahlen nicht zu groß werden, sollte man immer wieder die Schüsselzahl N abziehen (mit dem Taschenrechner), da es bei dieser modulo-N-Rechnung nur auf die Reste ankommt (wissenschaftliche Taschenrechner, auch der im Windows-Zubehör, verfügen über die Modulo-Funktion). Sowohl die Geheimzahl als auch die aus der Geheimzahl zurückgewonnene Klartextzahl ist ja jeweils der Rest aus einer Modulo-N-Rechnung.

Zur Entschlüsselung muss Frau Schwarz: die Geheimzahl bzw. den Vierer- oder Fünfer-Block zur D-ten Potenz nehmen und modulo 85 bilden, um zum Klartext zu gelangen:

$12 \times 12 \times \ldots = 12^{13} = 106993205379072 \equiv 82 \pmod{85}$

Frau Schwarz erhält also mit Hilfe der Tabelle in Abb. 4 als Klartextbuchstaben das „C" (kodiert als 82).

Sobald man tatsächlich einen größeren Text verschlüsseln will, merkt man, dass dies auch bei Zuhilfenahme eines Taschenrechners zu mühsam ist. Man benutzt also besser seinen Computer.

Das beschriebene Verschlüsselungsverfahren ist bei der Verwendung großer Schlüsselzahlen nicht zu knacken. Das liegt an der Verwendung von großen Primzahlen bei der Erzeugung der Schlüsselzahlen. Während es zwar leicht ist, große Primzahlen zu multiplizieren, so ist es fast unmöglich, durch Berechnung mit einem Computer aus einer solch großen Zahl die beiden Ausgangszahlen (Primfaktoren) wieder zurück zu gewinnen. Dies wäre aber notwendig, wenn man aus den beiden Zahlen N und E des öffentlichen Schlüssels den geheimen Schlüssel D bestimmen wollte: „Wenn Herr Grau die Zahl N, die ja öffentlich ist, in zwei Primzahlen zerlegen kann, hat er die Chiffrierung geknackt." [7]

Verschlüsseln mit dem Rechner

In der Kryptologie werden beim Verschlüsseln auf Rechnern symmetrische und asymmetrische Verfahren verwendet, wobei bei letzterem auch mit geheimen und öffentlichen Schlüsseln gearbeitet wird, d. h. es müssen keine geheimen Schlüssel ausgetauscht werden.

Das amerikanische Standardsystem DES

Das von der Computerfirma IBM und dem Geheimdienst NSA (NSA = National Security Agency) entwickelte Verschlüsselungssystem wurde 1977 von den USA als Standardsystem eingeführt.

Im DES-System (DES = Data Encryption) wird der Klartext in Dualzahlen geschrieben, in 64 Bits lange Blöcke aufgeteilt und auf vielfache Weise verschlüsselt. Das komplizierte Verfahren, das hier nicht beschrieben werden kann [8], führt zu einer sehr sicheren Verschlüsselung.

Asymmetrische Verschlüsselung

Das im Folgenden kurz beschriebene Verfahren wurde 1978 von den Mathematikern Ronald L. Riverst, Adi Shamir und Leonard Adleman entwickelt. Mit diesem – nach den Anfangsbuchstaben der Nachnamen der Entwickler „RSA" benannten Verschlüsselungsverfahrens – sollten zwei Ziele erreicht werden:

Erstens sollte eine Möglichkeit geschaffen werden, per Datenübertragung versandte Texte so unterschreiben zu können, dass die Unterschrift als authentisch erkannt werden kann, dass der Empfänger also sicher sein kann, dass das Schreiben tatsächlich von dem Absender stammt, der es unterschrieben hat.

Zweitens sollte das Verfahren die Möglichkeit bieten, den Text der Nachricht zu verschlüsseln, ohne dass der geheime Schlüssel aus der Hand gegeben werden muss.

Wie bei der asymmetrischen Verschlüsselung, bei der Frau Schwarz und Herr Weiß ein Schloss mit drei Schlüsseln verwenden, wird auch bei der Verschlüsselung im Computer mit den drei Schlüsseln N, D und E gearbeitet. Wir wollen weiterhin so verfahren, dass wir die Schlüssel E und N als die öffentlichen Schlüssel bezeichnen, während D der geheime Schlüssel sein soll.

Das RSA-Verfahren ist in aller Einfachheit nun bereits im Abschnitt „Asymmetrische Verschlüsselung mit drei Schlüsseln" beschrieben worden, die längliche Beschreibung, wie die Schlüsselzahlen aus einem Primzahlpaar gewonnen werden können, kann im Anhang C von Rudolf Kippenhahns Buch „Verschlüsselte Botschaften" nachgelesen werden.

Das RSA-Verfahren wurde in der Praxis im Chiffrierprogramm „PGP" (Pretty Good Privacy), das Phil Zimmermann 1991 der Allgemeinheit zur Verfügung gestellt hat, verwendet. Dabei wurde allerdings jeweils nur der Schüssel mit dem asymmetrischen RSA-Verschlüsselungsverfahren übertragen, der Text wurde – mit diesem Schlüssel – mit einem symmetrischen Verfahren verschlüsselt. Die Berechnungen hätten seinerzeit auf den Computern eine allzu lange Zeit gebraucht, wenn man alles mit dem asymmetrischen Verfahren verschlüsselt hätte.

PGP beinhaltete auch die sichere Authentifizierung des Absenders, denn: „Was mit dem öffentlichen Schlüssel E (und dem N) der Frau Schwarz dechiffriert werden kann, muss mit ihrem geheimen D chiffriert worden sein. Da nur sie das geheime D kennt, muss der Geheimtext, der mit E entschlüsselt werden kann, von ihr stammen. Das ist so sicher, wie wenn sie eigenhändig unterschrieben hätte." [9]

Fußnoten

[1] Empfohlen wird das Buch „Verschlüsselte Botschaften" von Rudolf Kippenhahn.

[2] Gaius Suetonius Tranquillus (um 70 n. Chr. bis 130 140 n. Chr.), Sueton genannt, römischer Schriftsteller, der vor allem für seine Kaiserbiograhpien bekannt wurde.

[3] Die Werte der Tabelle stammen aus Albrecht Beutelsbachers Buch „Kryptologie".

[4] Kreiszahl Pi = π = 3,14159265358979323846264338327 95...

[5] Eulersche Zahl e = 2,71828182845904523536028 74713526...

[6] Mit Erlaubnis des Verfassers Rudolf Kippenhahn werden in diesem Beispiel die gleichen Zahlen,

die er in seinem Buch „Verschlüsselte Botschaften“ verwendet und berechnet hat, genannt.

[7] Zitat aus Rudolf Kippenhahn: „Verschlüsselte Botschaften“.

[8] Wird z. B. auf *http://www.kuno-kohn.de/crypto/crypto/des.htm* beschrieben.

[9] Zitat aus Rudolf Kippenhahn: „Verschlüsselte Botschaften“.

Literatur

Albrecht Beutelspacher: „Kryptologie“, Friedr. Vieweg Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1993 (3. Auflage), ISBN 3-528-28990-2

Friedrich L. Bauer: „Entzifferte Geheimnisse“, Springer Verlag, Heidelberg/Berlin, 2000 (3. Auflage), ISBN 3-540-67931-6

Rudolf Kippenhahn: „Verschlüsselte Botschaften“, Rowohlt Taschenbuch, Reinbek bei Hamburg, 2011 (5. Auflage), ISBN 3-499-60807-3

Eyßell

Kontakt:
Manfred Eyßell
meyssel@gwdg.de
0551 201-1539

IT-Grundschutz-Überblickspapier „Smartphones“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das erste IT-Grundschutz-Überblickspapier veröffentlicht. Das „Überblickspapier Smartphones“ befasst sich mit typischen Gefährdungen der Informationssicherheit bei Smartphones sowie möglichen Gegenmaßnahmen.

Mit den Überblickspapieren bietet das BSI ab sofort in loser Folge Lösungsansätze zu aktuellen Themen der Informationssicherheit, die zu einem späteren Zeitpunkt auch in den IT-Grundschutz eingearbeitet werden.Zur Ermittlung der derzeit in der Wirtschaft relevanten Themen hat das BSI im April 2011 eine Umfrage unter den IT-Grundschutz-Anwendern durchgeführt. Das mit Abstand wichtigste IT-Sicherheitsthema war der Umfrage zufolge der sichere Umgang mit Smartphones.

Smartphones erfreuen sich zunehmender Beliebtheit sowohl bei Privatnutzern als auch bei Anwendern im geschäftlichen Umfeld. Die Geräte bieten neben Telefonie und SMS-Kommunikation einen breiten Funktionsumfang (Kamera, E-Mail, Internet und GPS) sowie die einfache Möglichkeit, neue Anwenderprogramme (Apps) zu installieren.

Die zunehmende Nutzung macht Smartphones allerdings auch für Angreifer attraktiv und für das Informationssicherheitsmanagement zu einer Herausforderung. Das neue Überblickspapier enthält Informationen zu diesen Herausforderungen und bietet konkrete Hilfestellungen für die sichere Nutzung von Smartphones im geschäftlichen und privaten Umfeld an. Das Überblickspapier sowie weitere Informationen sind auf den Webseiten des BSI unter folgendem URL abrufbar:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html

Die nächsten IT-Grundschutz-Überblickspapiere werden sich voraussichtlich mit den Themen Netzzugangskontrolle, Skype sowie der Nutzung privater IT-Geräte im dienstlichen Umfeld („Bring your own Device“) beschäftigen.

Reimann

Kontakt:
Michael Reimann
michael.reimann@gwdg.de
0551 201-1826

Kurse von Oktober bis Dezember 2011

Allgemeine Informationen zum Kursangebot der GWDG

Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Kursanmeldung, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@gwdg.de* mit dem Betreff „Kursanmeldung" erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/index.php?id=799* ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager – eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu autorisierte Person – oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils sieben Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit der Service-Hotline bzw. Information (Tel.: 0551 201-1523, E-Mail: *support@gwdg.de*) möglich.

Kosten bzw. Gebühren

Die Kurse sind – wie die meisten anderen Leistungen der GWDG – in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu acht Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

Kursorte

Alle Kurse finden in Räumen der GWDG statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 5 bzw. 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Faßberg 11, 37077 Göttingen. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL *http://www.gwdg.de/index.php?id=13* zu finden.

Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL *http://www.gwdg.de/index.php?id=57* zu finden. Anfragen zu den Kursen können an die Service-Hotline bzw. Information per Telefon unter der Nummer 0551 201-1523 oder per E-Mail an die Adresse *support@gwdg.de* gerichtet werden.

Kurs	Vortragende/r	Termin	Anmeldeschluss	AE
Administration von PCs im Active Directory der GWDG	Buck, Eyßell, Hast, Quentin	05.10.2011 09:00 - 12:30 Uhr und 13:30 - 15:30 Uhr	28.09.2011	4
Outlook – E-Mail und Groupware	Helmvoigt	06.10.2011 09:15 - 12:00 Uhr und 13:00 - 16:00 Uhr	29.09.2011	4
Einrichten von Windows-PCs im GÖNET	Eyßell, Quentin	10.10.2011 09:30 - 12:30 Uhr	03.10.2011	2
Photoshop für Fortgeschrittene	Töpfer	11.10.2011 - 12.10.2011 09:30 - 16:00 Uhr	04.10.2011	8
Mobile Dienste bei der GWDG	Reimann	13.10.2011 09:15 - 12:00 Uhr	06.10.2011	2
Führung durch das Rechnermuseum	Eyßell	14.10.2011 10:00 - 12:30 Uhr	07.10.2011	0
UNIX für Fortgeschrittene	Dr. Sippel	17.10.2011 - 19.10.2011 09:15 - 12:00 Uhr und 13:15 - 15:30 Uhr	10.10.2011	12
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	01.11.2011 - 02.11.2011, 09.11.2011 - 10.11.2011 13:00 - 16:30 Uhr	25.10.2011	8
Einführung in die Statistische Datenanlyse mit SPSS	Cordes	03.11.2011 - 04.11.2011 09:00 - 12:00 Uhr und 13:00 - 15:30 Uhr	27.10.2011	8
Programmierung von Parallelrechnern	Dr. Boehme, Dr. Schwardmann	15.11.2011 - 17.11.2011 09:15 - 12:15 Uhr und 13:30 - 16:30 Uhr	08.11.2011	12
Einführung in die Programme zur Sequenzanalyse	Dr. Bohrer	22.11.2011 - 23.11.2011, 29.11.2011 - 30.11.2011 13:00 - 16:30 Uhr	15.11.2011	8
Angewandte Statistik mit SPSS für Nutzer mit Vorkenntnissen	Cordes	01.12.2011 - 02.12.2011 09:00 - 12:00 Uhr und 13:00 - 15:30 Uhr	24.11.2011	8
UNIX/Linux-Arbeitsplatzrechner – Installation und Administration	Dr. Heuer, Dr. Sippel	05.12.2011 - 06.12.2011 09:15 - 12:00 Uhr und 13:30 - 16:00 Uhr	28.11.2011	8
UNIX/Linux-Server – Grundlagen der Administration	Dr. Heuer, Dr. Sippel	07.12.2011 - 08.12.2011 09:15 - 12:00 Uhr und 13:30 - 16:00 Uhr	30.11.2011	8
UNIX/Linux-Systemsicherheit für Administratoren	Dr. Heuer, Dr. Sippel	09.12.2011 09:15 - 12:00 Uhr und 13:30 - 15:00 Uhr	02.12.2011	4