Auftrag an die Stammgruppen

In diesem Gruppenpuzzle werdet ihr euch über das **Echelon-System, De-Mail, PGP** und **Kommunikationsfreiheit** Informieren. Am Ende der nächsten Stunde sollen *alle Schülerinnen und Schüler* in eurer Gruppe folgende Fragen beantworten können:

E 1 Was ist das Echelon-System?
E 2 Wie kann man sich und sein Unternehmen vor Informationsbeschaffung schützen?

D 1 Was ist De-Mail?
D 2 Was sind die Hauptkritikpunkte an dem geplanten „Bürgerportal“?

K 1 Wie und warum können Staaten E-Mail-Verkehr kontrollieren?
K 2 Was bringt Dir die Kommunikationsfreiheit?

P 1 Wie erschafft PGP Vertraulichkeit?
P 2 Wie erschafft PGP Authentizität und Integrität?

Nehmt Euch eine Minute Zeit, um zu sammeln: Was würdet ihr Euch unter den oben genannten Begriffen vorstellen? Betrachtet auch die Bilder im unteren Bereich dieses Arbeitsbogens!

Da ihr für die Beantwortung der Fragen viele Informationen braucht, sollt ihr Euch in vier Gruppen aufteilen, die jeweils zwei Fragen beantworten. Jede Gruppe erhält ein Arbeitsblatt mit wichtigen Informationen zum Thema, sowie Anhaltspunkte für eine weitergehende Recherche.

Am Ende der Stunde sollen alle auf ihrem Gebiet Expertinnen bzw. Experten sein. In der nächsten Stunde sollt ihr Euch dann gegenseitig informieren. Alle müssen sich also vorbereiten, einen kurzen, freien Vortrag zu „ihrem“ Thema zu halten und Nachfragen zu beantworten.

Arbeitsbogen *Echelon*

Aufgaben

1. Lest den Text auf dem Arbeitsbogen gründlich durch. Versucht, Unklarheiten miteinander zu klären. Natürlich könnt ihr auch den Lehrer fragen!
2. Überprüft Euer Wissen anhand der Kontrollfragen auf den nächsten Seiten.
3. Bereitet Euch darauf vor, einen kurzen Vortrag zu den unten aufgeführten Fragen E 1 und E 2 zu halten. Macht Euch Stichpunkte dazu!
4. Überlegt Euch, welche Nachfragen von Euren Klassenkameradinnen und -kameraden kommen könnten. Bereitet Euch darauf vor, diese zu beantworten. Fertigt Euch dazu Sprechkarten an!
5. Recherchiert nach weiteren Informationen zu den unten aufgeführten Fragen, um diese in Euren Vortrag einbauen zu können!

E 1 Was ist das Echelon-System?

Radom der US-Basis Bad Aiblingen (Bayern); [Quelle: en.wikipedia.org]

Der Name Echelon steht für ein globales Abhörsystem der Staaten des UKUSA-Abkommens. Da es sich hierbei um ein geheimdienstliches Projekt handelt, wurde die Existenz des Systems von öffentlicher Seite nie bestätigt. Im Jahr 2001 führte ein Ausschuss der EU jedoch einen Indizienbeweis für die – seitdem als gesichert geltende – Existenz von Echelon.
Echelon funktioniert hauptsächlich über das Abfangen von Satellitenkommunikation mittels Richtantennen (siehe Bild: Jede Kuppel verbirgt eine Richtantenne, so dass die Ausrichtung der Antenne geheim bleibt). Der Anteil des globalen Datenverkehrs über Satelliten beträgt nur etwa 5% - das Abhören von Kabeln ist wesentlich schwieriger, da hierfür eine physikalische Verbindung zum Kabel hergestellt werden muss. Die gewonnen Daten werden anschließend durch Computer nach bestimmten Stichwörtern durchsucht und verdächtige Nachrichten näher analysiert.
Das Abhören von Kommunikation ist per se nicht verboten: Nachrichtendienste dürfen lauschen, solang dies zum Zweck der Gefahrenabwehr, Bekämpfung von Kriminalität und Drogen-, bzw. Waffenhandel geschieht. Es wird jedoch befürchtet, dass Echelon auch zum Zweck der Wirtschaftsspionage eingesetzt wird – Beweise hierfür gibt es jedoch nicht. Grundsätzlich kann man annehmen, dass Wirtschaftsspionage eher auf „klassische“ Methoden zurückgreift: Einschleusung von Informanten, Anwerben von firmeninternen Mitarbeitern, Datenklau bei Geschäftsreisenden und gezieltes Abhören.
Nichtsdestotrotz hat die EU 2001 Empfehlungen an mittelständische und kleine Unternehmen, Behörden und Privatpersonen ausgesprochen, sensibel mit ihren Daten umzugehen. Einen guten Schutz bietet dabei der Einsatz von Verschlüsselung.

Gruppenpuzzle Echelon, DE-Mail, PGP und Kommunikationsfreiheit

E 2 Wie kann man sich und sein Unternehmen vor Informationsbeschaffung schützen?

In dem „Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), S. 17-22“ spricht die EU eine Reihe von Empfehlungen aus, unter anderem:
„ […] „in der Erwägung, dass Sicherheit für Unternehmen nur dann erzielt werden kann, wenn das gesamte Arbeitsumfeld abgesichert sowie alle Kommunikationswege geschützt sind, auf denen sensible Informationen übermittelt werden; dass es ausreichend sichere Verschlüsselungssysteme zu erschwinglichen Preisen auf dem europäischen Markt gibt; dass Privaten dringend zur Verschlüsselung von E-Mails geraten werden muss; dass eine unverschlüsselte Mail gleich einem Brief ohne Umschlag ist; dass sich im Internet relativ benutzerfreundliche Systeme finden, die sogar für den Privatgebrauch unentgeltlich zur Verfügung gestellt werden [...]
29. ersucht die Kommission und die Mitgliedstaaten, geeignete Maßnahmen für die Förderung, Entwicklung und Herstellung von europäischer Verschlüsselungstechnologie und -software auszuarbeiten und vor allem Projekte zu unterstützen, die darauf abzielen, benutzerfreundliche Kryptosoftware, deren Quelltext offen gelegt ist, zu entwickeln; [...]
32. appelliert an die europäischen Institutionen sowie an die öffentlichen Verwaltungen der Mitgliedstaaten, Verschlüsselung von E-Mails systematisch einzusetzen, um so langfristig Verschlüsselung zum Normalfall werden zu lassen;[...]“

Kontrollfragen zu Echelon

1. Wie funktioniert das Echelon-System?
2. Was besagt das UKUSA-Abkommen?
3. Zu welchem Zweck betreiben die UKUSA-Staaten eine globales Abhörsystem?
4. Warum soll „open-source“-Verschlüsselungssoftware besonders gefördert werden und wie hängt dies mit dem Kerckhoff'schen-Prinzip zusammen?
5. Überlege Dir, warum besonders kleine und mittelständische Unternehmen das Ziel von Wirtschaftsspionage sind.

Quellen (Links geprüft am 14.06.10)

Nichtständiger Ausschuss des Europäischen Parlaments, Bericht über die Existenz eines globen Abhörsystems für private und wirschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)): http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE
http://de.wikipedia.org/wiki/Echelon
Portfolio des Heise-Verlags über Echelon: http://www.heise.de/tp/r4/special/ech.html

Arbeitsbogen *De-Mail*

Aufgaben

1. Lest den Text auf dem Arbeitsbogen gründlich durch. Versucht, Unklarheiten miteinander zu klären. Natürlich könnt ihr auch den Lehrer fragen!
2. Überprüft Euer Wissen anhand der Kontrollfragen auf den nächsten Seiten.
3. Bereitet Euch darauf vor, einen kurzen Vortrag zu den unten aufgeführten Fragen D 1 und D 2 zu halten. Macht Euch Stichpunkte dazu!
4. Überlegt Euch, welche Nachfragen von Euren Klassenkameradinnen und -kameraden kommen könnten. Bereitet Euch darauf vor, diese zu beantworten. Fertigt Euch dazu Sprechkarten an!
5. Recherchiert nach weiteren Informationen zu den unten aufgeführten Fragen, um diese in Euren Vortrag einbauen zu können!

D 1 Was ist De-Mail?

Logo des E-Government Projekts "De-Mail"

2009 beschloss die Bundesregierung die Einrichtung eines so genannten elektronischen „Bürgerportals“. De-Mail ist ein Bestandteil dieses Portals. Zweck des Bürgerportals soll es sein, eine sichere Kommunikationsstruktur zwischen Bürgern, Behördern, Banken, Versicherungen und Firmen zur Verfügung zu stellen. Die Notwendigkeit eines solchen Portals beruht auf folgenden Überlegungen:
Eine offizielle Kommunikation mit Behördern, Versicherungen und Banken ist nur über Briefpost zulässig, da E-Mails bisher nicht die nötigen Anforderungen an eine sichere Kommunikation erfüllen. Da alle genannten Institutionen jedoch mit elektronischen Mitteln arbeiten, müssen schriftliche Eingänge in elektronische Daten und Ausgänge in Briefpost umgewandelt werden. Der dabei entstehende Arbeitsaufwand kostet natürlich Geld. Häufig müssen Briefe an Behörden per Einschreiben (dabei bestätigt der Adressat den Empfang der Post) gesendet werden – ein solches Prinzip gibt es zur Zeit bei der E-Mail-Kommunikation nicht. Firmen wie z.B. Mailprovider können sich beim Bürgerportal akkreditieren lassen und sind dann verpflichtet, die Sicherheitsstandards der Bundesregierung umzusetzen. Einer dieser Standards sieht vor, dass der E-Mail-Verkehr mittels asymmetrischer Verschlüsselungsverfahren chiffriert werden muss. Auch wenn die Einrichtung eines Online-Bürgerportals häufig begrüßt wird, gibt es erhebliche Bedenken von Seiten der Datenschützer über die konkrete Umsetzung des Projekts. Ein System, das sensible Daten von Bürgerinnen und Bürgern verwaltet, empfängt und versendet, muss vollständig gegenüber Missbrauch von außen – aber auch von innen – abgesichert sein. Das ursprüngliche Sicherheitskonzepts des Bürgerportals wurde auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2009 als unzureichend bezeichnet.

D 2 Was sind die Hauptkritikpunkte an dem geplanten „Bürgerportal“?

Am 29. April 2009 veröffentlichten die Datenschützer des Bundes und der Länder eine Stellungnahme zum geplanten Bürgerportal, in der sie Kritik an der Umsetzung äußerten (in Auszügen):

„Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. […]
Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Dienstanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt sein werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. […]
Die nach der Gesetzesbegründung […] mögliche unsichere Anmeldung mit Passwort wird abgelehnt.
Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. […] So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern […]. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen. [...]“

Quelle: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009 - Datenschutz beim vorgesehenen Bürgerportal unzureichend,
URL: http://www.datenschutz-berlin.de/attachments/580/Anlage.pdf?1239962678

Kontrollfragen

1. Aus welchen Gründen soll das Bürgerportal eingeführt werden?
2. Das Motto von De-Mail lautet „So einfach wie E-Mail, so sicher wie Briefpost – verschlüsselt, authentisch, nachweisbar“ Wie hängt dieses Motto mit den im Unterricht aufgestellten Anforderungen an sichere Kommunikation zusammen?
3. Für die oben geäußerten Kritikpunkte gibt es Lösungen! Welche fallen Dir ein?

Quellen (Links geprüft am 14.06.10)

http://de.wikipedia.org/wiki/De-Mail
Artikel des Heise-Verlags: http://www.heise.de/security/meldung/Bundeskabinett-verabschiedet-Buergerportalgesetz-205356.html
IT-Sicherheit-Blog: http://itsicherheit.wordpress.com/2009/04/18/datenschutzer-fordern-nachbesserungen-beim-burgerportal-gesetz/
Offizielle Website De-Mail: http://www.de-mail.de/
(dort findest Du auch weiterführende Links zu offiziellen Dokumenten Regierung!)

Arbeitsbogen *Kommunikationsfreiheit*

Aufgaben

1. Lest den Text auf dem Arbeitsbogen gründlich durch. Versucht, Unklarheiten miteinander zu klären. Natürlich könnt ihr auch den Lehrer fragen!
2. Überprüft Euer Wissen anhand der Kontrollfragen auf den nächsten Seiten.
3. Bereitet Euch darauf vor, einen kurzen Vortrag zu den unten aufgeführten Fragen K 1 und K 2 zu halten. Macht Euch Stichpunkte dazu!
4. Überlegt Euch, welche Nachfragen von Euren Klassenkameradinnen und -kameraden kommen könnten. Bereitet Euch darauf vor, diese zu beantworten. Fertigt Euch dazu Sprechkarten an!
5. Recherchiert nach weiteren Informationen zu den unten aufgeführten Fragen, um diese in Euren Vortrag einbauen zu können!

K 1 Wie und warum können Staaten E-Mail-Verkehr kontrollieren?

Karikatur: "Tweet-Hunting in Iran" vom User Rodrigo. [Quelle: toonpool.com]

Im Deutschen Grundgesetz (Art.5 Abs.1) wird jedem Bürger das Recht auf Kommunikationsfreiheit zugeschrieben. Dieses Recht ist die Grundlage der Meinungs-, Informations- und Medienfreiheit. Dieses Recht zu besitzen ist keine Selbstverständlichkeit – in einigen Ländern ist ein solches Recht nicht vorhanden. Wo ein Recht auf Kommunikationsfreiheit fehlt, ist es dem Staat nicht verboten, E-Mail-Verkehr zu kontrollieren.
Die Kontrolle funktioniert dabei wie folgt: Jeglicher E-Mail-Verkehr wird über einen (oder mehrere) Rechner, so genannte Proxies weitergeleitet. Wie Du bereits im Unterricht gesehen hast, kann man dort den Datenverkehr computergesteuert analysieren und somit auch den Inhalt von E-Mails lesen. Darüber hinaus kann man die E-Mails sogar verändern, wie es im Fall der chinesischen Falun-Gong-Sekte passierte: Dateianhänge von Falun Gong-E-Mails wurden mit Spionagesoftware versetzt, so dass die Empfänger der E-Mails beim Öffnen gleichzeitig die ungewollte Software installierten.
Die Verschlüsselung von Nachrichten ist in China keine Möglichkeit, um sichere Kommunikation zu betreiben: Bereits das Verwenden von nicht genehmigter Verschlüsselungssoftware oder -hardware ist verboten und kann bestraft werden. Weiterhin wollen viele Autoren, dass eine Nachricht möglichst viele Menschen erreicht, um die eigene Meinung zu verbreiten. So sind etwa die chinesischen Unterzeichner der Charta 08 bewusst das Risiko eingegangen, sich durch die Veröffentlichung des Dokuments im Internet einer Strafverfolgung auszusetzen. Eine der zentralen Forderungen der Charta 08 ist das Recht auf freie Meinungsäußerung. Bereits vor der Veröffentlichung des Dokuments wurden Unterzeichner, wie etwa der Dissident Liu Xiabo verhaftet.

K 2 Was bringt Dir die Kommunikationsfreiheit?

Folgende Zitate drehen sich rund um das Thema Kommunikationsfreiheit. Nutze die Zitate als Anregung, um mit Deinen Gruppenmitgliedern über den Nutzen von Kommunikationsfreiheit zu diskutieren! Überlegt dabei auch, warum ein Staat ein Interesse an der Kontrolle von Kommunikation haben kann.

"Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten [...] Eine Zensur findet nicht statt." (Art. 5 Abs. 1 GG)

„Freiheit. Ich verstehe das Wort nicht, weil ich sie nie entbehren musste.“ (Jonas T. Bengtsson, Die Hölle ist, mit sich allein zu sein, in: Wolfgang Klein (Hg.), Young Euro Connect 2006.“)

„China hat eine Mauer gebaut. Heutzutage baut man Mauern nicht mehr nur über Hügel und Felder, sondern auch im Internet. Die Menschen in China leben hinter einer Mauer, und nur was die chinesische Regierung erlaubt, darf durch diese Mauer hindurch ins Land kommen.“ (Statement auf der Webseite des Chaos-Computer-Club, URL: http://chinesewall.ccc.de/index-de.html)

Kontrollfragen

1. Wie kann ein Staat den gesamten E-Mail-Verkehr des eigenen Landes kontrollieren?
2. Was ist die Charta 08?
3. Warum dürfen Staaten den (elektronischen) Postverkehr kontrollieren, warum ist dies in Deutschland nicht der Fall? Kannst Du Dir vorstellen, wann auch der deutsche Staat E-Mails mitlesen darf?
4. Was will der Künstler „Rodrigo“ mit seiner Karikatur aussagen?
5. Warum ist das Verschlüsseln von Nachrichten keine Lösung um mangelnde Kommunikationsfreiheit auszugleichen?

Quellen (Links geprüft am 14.06.10)

http://de.wikipedia.org/wiki/Internetkontrolle_in_der_Volksrepublik_China
http://de.wikipedia.org/wiki/Charta_08
http://chinesewall.ccc.de/index-de.html
(Webseite des Chaos Computer Club über die Chinesische Internetkontrolle)
Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson, Ignoring the Great Firewall of China, URL: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf
(Ausführliche Informationen in englischer Sprache über die Technik der Chinesischen Internetkontrolle)
http://futurezone.orf.at/stories/255642/
(Blog des österreichischen Rundfunksenders ORF)

Arbeitsbogen *PGP* („Pretty Good Privacy“)

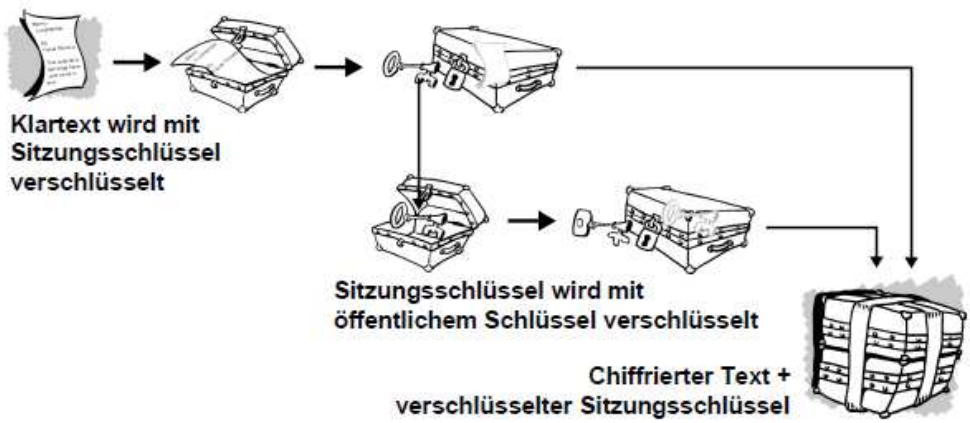
Aufgaben

1. Lest den Text auf dem Arbeitsbogen gründlich durch. Versucht, Unklarheiten miteinander zu klären. Natürlich könnt ihr auch den Lehrer fragen!
2. Überprüft Euer Wissen anhand der Kontrollfragen auf den nächsten Seiten.
3. Bereitet Euch darauf vor, einen kurzen Vortrag zu den unten aufgeführten Fragen P 1 und P 2 zu halten. Macht Euch Stichpunkte dazu!
4. Überlegt Euch, welche Nachfragen von Euren Klassenkameradinnen und -kameraden kommen könnten. Bereitet Euch darauf vor, diese zu beantworten. Fertigt Euch dazu Sprechkarten an!
5. Recherchiert nach weiteren Informationen zu den unten aufgeführten Fragen, um diese in Euren Vortrag einbauen zu können!

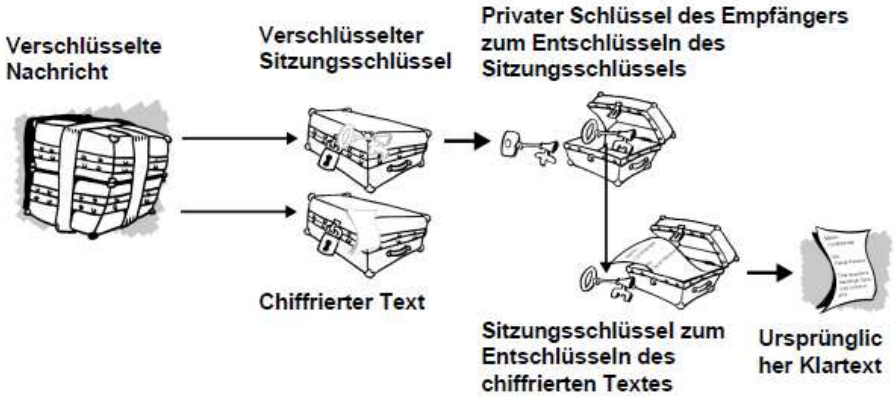
P 1 Wie erschafft PGP Vertraulichkeit?

Logo des des frei verfügbaren „Open-Source“- Projekts GnuPG [Quelle: gnupg.org]

PGP („Pretty Good Privacy“) ist ein hybrides Verschlüsselungssystem, das es ermöglicht, beim Versenden einer Nachricht Authentizität, Integrität und Vertraulichkeit zu gewährleisten. Es wurde 1991 vom US-Amerikaner Phil Zimmermann entwickelt und ist mittlerweile weit verbreitet. PGP ist nutzt ein asymmetrisches Verschlüsselungsverfahren, wie Du es bereits im Unterricht kennen gelernt hast: Jeder Teilnehmer besitzt einen öffentlichen und einen privaten Schlüssel. Möchte man jemanden eine Nachricht schicken, so verschlüsselt man diese mit dessen öffentlichen Schlüssel. Nur der Empfänger besitzt den privaten Schlüssel und somit ist nur er in der Lage, die Nachricht zu entschlüsseln. Auf diese Art und Weise entgeht man der Problematik, den geheimen Schlüssel austauschen zu müssen!
Genau genommen, wird bei PGP die Nachricht nicht mit einem asymmetrischen Verfahren verschlüsselt. Das Verfahren nutzt hier einen kleinen Trick: Der Klartext wird mit einem so genannten Sitzungsschlüssel symmetrisch verschlüsselt. Anschließend wird nur dieser Schlüssel mit einem asymmetrischen Verfahren verschlüsselt. Der Empfänger entschlüsselt anschließend zunächst den Schlüssel und damit dann die eigentliche Nachricht. Klingt kompliziert, ist aber einfach:



Verschlüsseln einer Nachricht mit PGP. [Quelle: Handbuch PGP- Eine Einführung in die Kryptographie, ftp://ftp.pgpi.org/pub/pgp/6.5/docs/german/IntroToCrypto.pdf], S8]

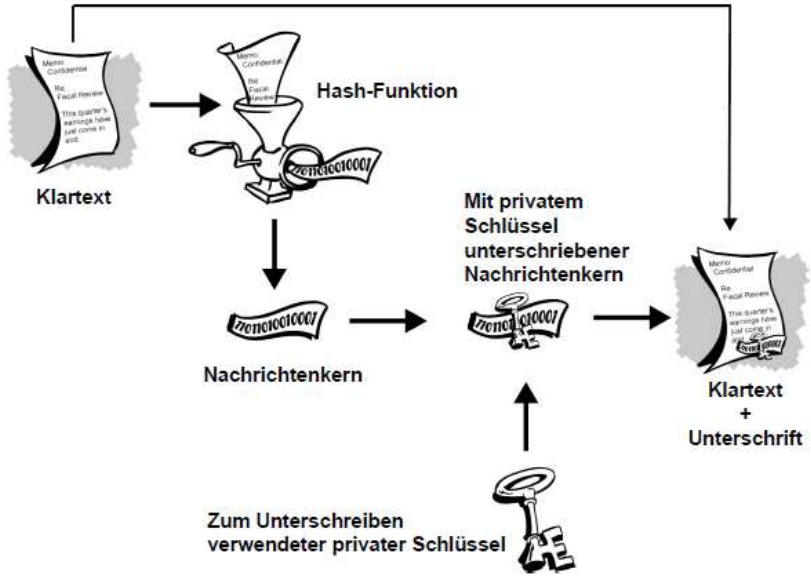


Entschlüsseln einer Nachricht mittels PGP. [Quelle: Handbuch PGP- Eine Einführung in die Kryptographie, ftp://ftp.pgpi.org/pub/pgp/6.5/docs/german/IntroToCrypto.pdf, S8]

Durch diese Methode erspart man sich die sehr zeitintensive Verschlüsselung des gesamten Nachrichtentextes durch ein asymmetrisches Verfahren. Nur den Sitzungsschlüssel asymmetrisch zu verschlüsseln geht hingegen sehr schnell!

P 2 Wie erschafft PGP Authentizität und Integrität?

Neben der Verschlüsselung besitzt PGP noch zwei weitere Verfahren: Die digitale Signatur und ein Hash-Verfahren. Diese dienen dazu, sicher zu stellen, dass 1. die Nachricht auch wirklich von demjenigen stammt, der als Absender genannt ist und 2. dass die Nachricht auf dem Transportweg nicht verändert wurde.Eine Hash-Funktion erzeugt aus einem großen Text einen so genannten Nachrichtenkern, der weitaus kleiner als der eigentliche Text. Dieser Nachrichtenkern wird anschließend mit dem privaten Schlüssel des Senders „unterschrieben“. Verändert man die ursprüngliche Nachricht auf dem Transportweg, so verändert sich auch der Nachrichtenkern. Beim Entschlüsseln fällt dies PGP auf und es meldet die Veränderung. Der unterschriebene Nachrichtenkern kann nur mit dem öffentlichen Schlüssel des Senders wieder entschlüsselt werden. Dadurch wird sichergestellt, dass die Nachricht auch wirklich von dem stammt, der sie gesendet hat.



[Quelle: Handbuch PGP- Eine Einführung in die Kryptographie, ftp://ftp.pgpi.org/pub/pgp/6.5/docs/german/IntroToCrypto.pdf, S12]

Gruppenpuzzle Echelon, DE-Mail, PGP und Kommunikationsfreiheit

Kontrollfragen

1. Warum braucht man bei der asymmetrischen Verschlüsselung einen privaten und einen öffentlichen Schlüssel?
2. Was ist ein hybrides Verschlüsselungsverfahren?
3. Was ist eine Hash-Funktion?
4. Warum heißt PGP „nur“ Pretty Good Privacy? Was ist GnuPG?
5. Warum entwickelte Phil Zimmermann PGP und warum war die US-Regierung damit zunächst nicht einverstanden? (Antwort dazu ist nicht im Text – du musst sie selbst recherchieren!)

Quellen (Links geprüft am 14.06.10)

Handbuch PGP – eine Einführung in die Kryptographie, URL:
ftp://ftp.pgpi.org/pub/pgp/6.5/docs/german/IntroToCrypto.pdf
http://de.wikipedia.org/wiki/Pretty_Good_Privacy
http://www.zdnet.de/news/wirtschaft_sicherheit_security_pgp_erfinder_philip_zimmermann_im_interview_story-39001024-2103010-1.htm
(Interview mit Phil Zimmermann)
Stefan Krempl, „Krieg um Krypto“, Spiegel Online 1998. URL:
http://www.spiegel.de/netzwelt/tech/0,1518,13719,00.html
„Sichere Mailverschlüsselung ohne Umtriebe“, Artikel in der FAZ 12.04.2005, URL:
http://www.faz.net/s/Rub4C34FD0B1A7E46B88B0653D6358499FF/Doc~E357B3B30B1E348128E2FB3B18070F685~ATpl~Ecommon~Scontent.html