secure-it in NRW. IT-Sicherheit macht Schule. Arbeitsmaterialien für den Unterricht. Sichere E-Mail-Kommunikation

secure IT®

Ministerium für Wirtschaft und Arbeit des Landes Nordrhein-Westfalen

NRW.

l Kontakt

Agentur »secure-it.nrw«
bei der IHK Bonn/Rhein-Sieg
Bonner Talweg 17
D-53113 Bonn
Telefon: +49 (0) 228/2284-184 und -185
Telefax: +49 (0) 228/2284-221
E-Mail: info@secure-it.nrw.de
Internet: www.secure-it.nrw.de

Ministerium für
Wirtschaft und Arbeit
des Landes Nordrhein-Westfalen
Referat Presse und Öffentlichkeitsarbeit
40190 Düsseldorf
www.mwa.nrw.de

Autor: Markus Asmuth
Redaktion: Manfred Kasper, Journalismus und PR
Gestaltung: Grafik-Atelier Seitz-Atlama

secure-it in NRW. IT-Sicherheit macht Schule. Arbeitsmaterialien für den Unterricht. Sichere E-Mail-Kommunikation

Vorbemerkungen für Lehrkräfte

Die im Folgenden aufgeführten Materialien stellen ein Angebot für Lehrkräfte aller Schulformen dar. Die verwendeten Links geben den Stand von Januar 2005 wieder.

Die Materialien eignen sich für den Unterricht aller Schulformen ab Klasse 8 in den Fächern bzw. Lernbereichen Ethik, Informatik, Medienbildung, ökonomische Bildung, Politik und Sozialwissenschaften.

Die vorliegenden Arbeitsmaterialien dienen als Kopiervorlage. Als Erläuterung zu Fachbegriffen bietet die Landesinitiative »secure-it.nrw« auf ihrer Internetpräsenz (www.secure-it.nrw.de) ein Glossar an. Hier befinden sich auch Verweise auf weitere Links zum Thema. Die Themen Verschlüsselung und Digitale Signatur werden im Jahr 2005 in Form weiterer Arbeitsmaterialien vertieft.

Das Thema: Sichere E-Mail-Kommunikation

E-Mails sind schnell geschrieben, schnell versendet und zudem kostengünstig. Der Empfänger entscheidet selbst, wann er eine Nachricht liest und bearbeitet.

Doch Vorsicht: Deine E-Mails könnten auf dem Weg über das Internet verloren gehen oder ein Spam-Filter könnte sie fälschlicherweise aussortieren. Daher kannst du dir nicht sicher sein, dass deine E-Mail ihr Ziel wirklich erreicht und vom Empfänger gelesen wird. Du solltest bei wichtigen Nachrichten den Empfänger bitten, eine kurze Bestätigungsmail zurückzusenden.

Die Kommunikation mit E-Mails hat drei weitere grundsätzliche Nachteile:

- Die Vertraulichkeit einer E-Mail ist nicht gewährleistet.
- Die Unverfälschtheit einer E-Mail ist nicht gewährleistet.
- Die Echtheit des Absenders ist nicht gewährleistet.

Die Vertraulichkeit einer E-Mail

Eine unverschlüsselte E-Mail wird im Klartext versendet. Sie durchläuft eine Vielzahl von Internetrechnern und Datenleitungen auf ihrem Weg zum Empfänger. Wenn du beispielsweise eine E-Mail zu einem Adressaten im Nachbargebäude schickst, wird diese viele Internetrechner im Inland und eventuell sogar im Ausland passieren. Spione, Hacker oder Geheimdienste können sich in die Rechner einklinken und Datenleitungen anzapfen. Dies ist keineswegs Phantasie: Von amerikanischen, englischen, kanadischen, australischen und neuseeländischen Geheimdiensten wird das Echelon-System betrieben. Echelon zapft E-Mail-, Telefon- und Faxverbindungen an. Neben dem militärischen Bereich sind Regierungen, Organisationen und die Industrie die Hauptziele von Spionage.

Das Thema Vertraulichkeit fängt jedoch schon im eigenen Umfeld an: Öffnet jemand unbefugt einen an dich persönlich adressierten Brief, so macht er sich strafbar. Anders sieht es aus, wenn er eine an dich adressierte E-Mail öffnet. Bedingung für die Gültigkeit des Briefgeheimnisses ist laut Strafgesetzbuch ein „verschlossenes Schriftstück“. Da eine E-Mail im Klartext vorliegt, greift das Briefgeheimnis für E-Mails nicht. Vermutlich wird man den „Spion“ auch nicht wegen Datenspionage zur Rechenschaft ziehen können.

Fazit: Willst du sicher gehen, dass deine elektronischen Nachrichten vertraulich bleiben, solltest du sie verschlüsseln. GnuPG (GNU Privacy Guard) und PGP (Pretty Good Privacy) sind zwei Verschlüsselungsprogramme, die sehr sicher und leicht zu bedienen sind. Sie laufen sowohl unter Windows- als auch unter Linux-Systemen. GnuPG ist eine mit Bundesmitteln geförderte, kostenlose Software. Auch das Programm PGP ist für den privaten Einsatz kostenlos.

Die Unverfälschtheit einer E-Mail

Wer geschäftliche E-Mails versendet, hat großes Interesse, dass die Nachrichten unverändert ankommen. Allein das Hinzufügen eines Wortes kann die Bedeutung eines Satzes entscheidend ändern. Ein Beispiel: „Wir geben das Angebot [nicht] in Auftrag.“

Gravierende Auswirkungen kann auch das Verändern von Zahlen haben: So macht es einen Riesenunterschied, ob man schreibt „Das Angebot beläuft sich auf 1.600.000 Euro“ anstatt „Das Angebot beläuft sich auf 1.400.000 Euro“. Den Zuschlag für den entsprechenden Auftrag wird sicherlich die Konkurrenz erhalten.

Die Echtheit des Absenders

Auch der Absender einer E-Mail lässt sich leicht verfälschen. Soll die Mail rechtsverbindlich dem Absender zugeordnet werden, muss er sie mit seiner Digitalen Signatur versehen. Diese stellt auf elektronischem Weg sicher, dass er wirklich der Absender der Mail ist. Beim Abschluss von Verträgen beispielsweise kann die Digitale Signatur als Sicherheitsmerkmal verlangt werden.

Mit den Verschlüsselungsprogrammen GnuPG und PGP kannst du E-Mails verschlüsseln und digital signieren. Die Digitale Signatur garantiert dabei ebenso die Unverfälschtheit deiner E-Mail. So kannst du dich leicht vor Schnüfflern, Fälschern und Betrügern schützen und dennoch die Vorteile der E-Mail-Kommunikation nutzen.

Sichere E-Mail-Kommunikation als Unterrichtsthema: Hinweise für Lehrerinnen und Lehrer

Einsatzmöglichkeiten im Unterricht

Die Schülerinnen und Schüler werden nach Abschluss ihrer Schulausbildung verantwortungsbewusst in Unternehmen mit elektronischen Daten umgehen müssen. Um sie erfolgreich zu sicherheitsbewussten Mitarbeitern und Bürgern auszubilden, sollte sich das Thema IT-Sicherheit kontinuierlich über die gesamte Schulzeit erstrecken. Die vorliegenden Materialien eignen sich für den Einsatz ab Klasse 8 (siehe Vorbemerkungen). Es empfiehlt sich, die Verschlüsselung von E-Mails ganzheitlich – das heißt fächerübergreifend – zu betrachten.

Technische Voraussetzungen

Voraussetzung für die Übung „Asymmetrische Verschlüsselungsverfahren“ ist die Installation von PGP oder GnuPG. Sie können eine grafische Version von PGP unter Windows einsetzen oder beispielsweise GnuPG als Konsolen-Programm unter Linux wählen.

Auch andere Varianten sind möglich: So kann PGP unter Windows oder Linux auch über die Konsole bedient werden, für GnuPG werden grafische Frontends angeboten. Voraussetzung für die Bedienung von GnuPG über die Kommandozeilen-Version ist allerdings, dass die Schülerinnen und Schüler die grundlegenden Linux-Konsolenbegriffe wie zum Beispiel ls, cat, cd, cp, mv, rm beherrschen. Wenn kein Linux auf dem Rechner installiert ist, kann die GNU/Linux-Software Knoppix von CD gestartet werden. Es ist keine Installation auf der Festplatte notwendig. Knoppix kann kostenlos aus dem Internet heruntergeladen und auf CD gebrannt werden (ca. 650 MB). GnuPG ist in dem entsprechenden Paket bereits enthalten.

Weiterführende Links

Es gibt eine Reihe von weiterführenden Links und Hinweisen zum Thema „Sichere E-Mail-Kommunikation“. Einige ausgewählte Materialien, die für die Beschäftigung mit dem Thema oder die Planung des eigenen Unterrichts relevant sein können, sind an dieser Stelle aufgelistet. Dabei handelt es sich sowohl um Querverweise zu ausgearbeiteten Unterrichtsreihen und Wettbewerben als auch um Angebote zur inhaltlichen und technischen Vertiefung des Themas.

www.lehrer-online.de/url/e-mail-verschluesseln
Die ausgearbeitete Unterrichtsreihe zum Verschlüsseln von E-Mails stellt die selbstständige Erarbeitung der Verschlüsselungsprogramme GnuPG und PGP unter Linux (Knoppix) und Windows in den Vordergrund.

www.ietf.org/rfc/rfc1855.txt
Die so genannte Netiquette beschreibt Kommunikationsregeln beim Austausch von E-Mails. Sie erleichtert allen Teilnehmern die Kommunikation. So wird zum Beispiel Wert auf einen detaillierten und aussagekräftigen Betreff gelegt. Hier soll der Leser bereits über den Inhalt der Nachricht informiert werden. Er kann dann schnell entscheiden, ob und wann er die E-Mail öffnet. Des Weiteren empfiehlt die Netiquette, dass beim Zitieren von E-Mails der Antworttext unterhalb des zitierten Textes zu platzieren ist. Nur der Text, auf den sich die Antwort bezieht, sollte jeweils zitiert werden.

Es bietet sich an, fächerübergreifend im Deutschunterricht die Kommunikation per E-Mail an praxisnahen Beispielen unter Berücksichtigung der Netiquette zu üben. Aus Gründen der Sicherheit sollten die E-Mails dabei verschlüsselt übertragen werden.

http://jya.com/echelon-dc.htm#echelon
Der erste in Europa veröffentlichte Bericht über Echelon von Duncan Campbell liefert Materialien für den Politikunterricht.

www.mystery-twister.de/
Der Mystery-Twister ist ein Wettbewerb für Schulklassen zum Thema Kryptographie. Starttermin ist der 1. Januar 2005. Erste Beispielaufgaben werden ab Oktober 2004 eingestellt.

www.lfd.nrw.de/fachbereich/download/e_mail_sicher.pdf
Eine verständliche Einführung in das Thema „Sichere E-Mail-Kommunikation“ und eine anschauliche Bedienungsanleitung zur grafischen Version von PGP unter Windows bietet die Broschüre „E-Mails, aber sicher“ der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Diese eignet sich gut, um die Übungen zum Einsatz von PGP vorzubereiten.

www.bsi-fuer-buerger.de/schuetzen/07_0301.htm
Die PGP und GnuPG zugrunde liegenden Verschlüsselungsverfahren werden auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik allgemeinverständlich erklärt. Die Seite richtet sich an sicherheitsbewusste Bürgerinnen und Bürger. Sie setzt nur wenig technische Vorkenntnisse voraus.

www.gnupg.org/
Die offizielle Homepage von GnuPG bietet Bedienungsanleitungen in kompakter und ausführlicher Form. Hier ist es zudem möglich, GnuPG downzuloaden.

www.pgpi.org/
Auf der Homepage von PGP-International können die Freeware-Versionen von PGP heruntergeladen werden. Im fächerübergreifenden Unterricht mit Englisch bietet sich ein Download der englischen Version an.

www.knopper.net/knoppix
Wenn Sie GnuPG unter Linux einsetzen wollen und das System nicht auf ihrem Rechner installiert ist, kann die GNU/Linux-Software Knoppix auch von CD gestartet werden. Dazu ist keine Installation auf der Festplatte notwendig. Knoppix kann kostenlos aus dem Internet heruntergeladen und auf CD gebrannt werden (ca. 650 MB) – GnuPG ist in dem entsprechenden Paket bereits enthalten (siehe Technische Voraussetzungen).

Abschließend noch eine Anmerkung zu den Übungen zum Einsatz von GnuPG und PGP: Beim Unterricht in der Sekundarstufe I werden die Schülerinnen und Schüler die Übungen nicht ohne die Hilfe des Lehrers durchführen können. Der Lehrer könnte hier exemplarisch einzelne Arbeitsschritte am Beamer vorführen.

Eine sinnvolle Ergänzung zum Thema „Sichere E-Mail-Kommunikation“ stellen die ebenfalls von der Initiative »secure-it.nrw« entwickelten Unterrichtsmaterialien zum Thema „Viren, Würmer und Trojaner“ dar.

Arbeitsmaterialien für den Unterricht
Fragen zur sicheren E-Mail-Kommunikation

1. Was sind Spam-Mails und was ist ein Spam-Filter?

2. Welche Sicherheitslücken bestehen beim Austausch von E-Mails?

3. Überlege dir zu jeder Sicherheitslücke ein eigenes Beispiel.

4. Was ist das Echelon-System? Wer betreibt es? Zu welchem Zweck wird Echelon eingesetzt?

5. Wer könnte Interesse am Mitlesen von E-Mails haben?

6. Wie können Firmen und Privatpersonen vertrauliche E-Mails vor Schnüfflern, Fälschern und Betrügern schützen?

7. Du schreibst aus dem Urlaub einen privaten Brief an eine Freundin, eine Postkarte an deine Eltern und eine E-Mail an einen Freund. Welche der drei Nachrichten fallen unter das Briefgeheimnis?

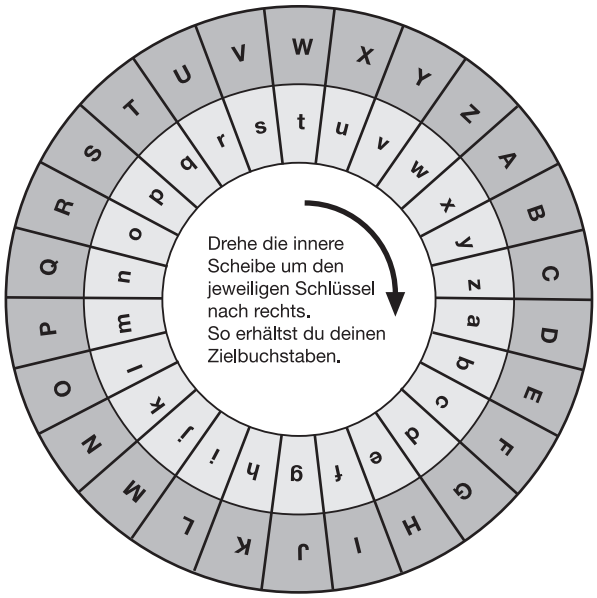
Arbeitsmaterialien für den Unterricht
Übungen zur Caesar-Verschlüsselung

Das „Internet“ des römischen Kaisers Julius Caesar beruhte auf Boten. Hin und wieder kreuzten sich deren Wege mit Galliern, die auf Wildschweinjagd waren. Oder einige Boten verplapperten sich bei einem Krug Wein in einer Taverne. Dann war der Schlachtplan bekannt und die Gallier konnten nach einem kräftigen Schluck Zaubertrank viele Römerhelme sammeln. Ein Grund dafür, warum Caesar seinen Boten immer mehr misstraute. Er ging dazu über, seinen Kurieren Meldungen in verschlüsselter Form mit auf den Weg zu geben.

Er entwickelte die Caesar-Verschlüsselung, die folgendermaßen funktioniert: Ersetze jeden Buchstaben des Klartextes durch den Buchstaben, der im Alphabet um eine bestimmte Zahl von Zeichen weiter hinten steht. Diese Zahl wird Schlüssel genannt. Gelangst du bei der Suche ans Ende des Alphabets, so setze sie einfach am Alphabetanfang fort. Lasse Wortzwischenräume und Satzzeichen weg und benutze nur Großbuchstaben.

Beispiel

Schlüssel: 3
Klartext: Angriff um acht
Geheimtext: DQJULIIXPDFKW



Es kam, wie es kommen musste: Die Geheimtexte gerieten in die Hände der Gallier. Diese konnten jedoch nichts mit den Zeichenfolgen anfangen. Seitdem aber ist man sich in Gallien sicher: „Die spinnen, die Römer!“

Arbeitsauftrag

1. Verschlüssele den Klartext „Angriff ueber Nordflanke“ mit dem Schlüsselwert 5.

2. Entschlüssele den Geheimtext „XGTUVCGTMWPIPCJV“. Der Schlüssel hat den Wert 2.

3. Schreibe eine geheime Nachricht mit mindestens 30 und maximal 50 Zeichen. Denke dir einen Schlüssel aus (mit einem Wert kleiner oder gleich 5) und verschlüssele die Nachricht auf einem separaten Zettel.

4. Tausche den Geheimtext mit deinem Tischnachbarn und versuche, den Text zu entschlüsseln. Welchen Schlüssel hat er gewählt?

Arbeitsmaterialien für den Unterricht
Übungen zur Vigenère-Verschlüsselung

Im Mittelalter verbesserte der französische Diplomat Blaise de Vigenère (1523-1596) die überalterte Caesar-Verschlüsselung. Die Verbesserung bestand darin, das Alphabet nicht immer um die gleiche Anzahl von Stellen zu verschieben, sondern die Anzahl der Stellen zu variieren.

Beispiel

Schlüssel:	3, 5, 1
Klartext:	Jenny ist eine Hexe
Anpassen:	JENNYISTEINEHEXE
Weiterzählen um:	3513513513513513
Geheimtext:	MJOQDJVYFLSFKJYH

Arbeitsauftrag

1. Verschlüssele den Klartext „Angriff ueber Nordflanke“ mit dem Schlüsselwert 4, 1, 3.

2. Entschlüssele den Geheimtext „ZJUSXFFLHODC“. Der Schlüssel hat den Wert 3,1.

3. Schreibe eine geheime Nachricht mit mindestens 30 und maximal 50 Zeichen. Denke dir einen Schlüssel aus, der aus genau zwei Zahlen besteht, um die der Klartext abwechselnd verschoben wird (mit jeweils einem Wert kleiner oder gleich 2). Verschlüssele die Nachricht auf einem separaten Zettel.

4. Tausche den Geheimtext mit deinem Tischnachbarn und versuche, den Text zu entschlüsseln. Welchen Schlüssel hat er gewählt?

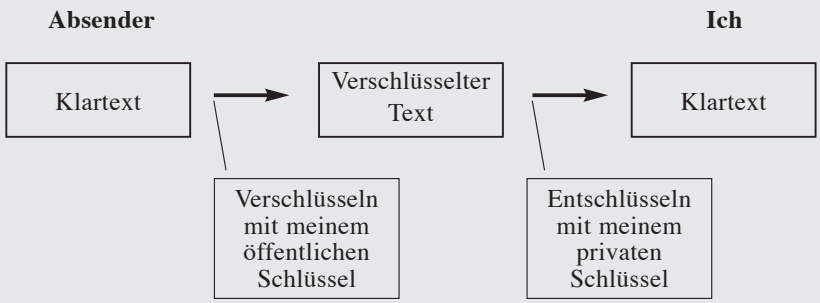
Arbeitsmaterialien für den Unterricht
Übungen zum Asymmetrischen Verschlüsselungsverfahren

Sowohl die Caesar-Verschlüsselung als auch die Vigenère-Verschlüsselung sind mit moderner Rechnertechnik leicht und schnell zu knacken. Daher gibt es mittlerweile ausgetüftelte rechnergestützte Verschlüsselungsverfahren. Viele dieser Verfahren haben jedoch noch heute den gleichen Nachteil wie einst die Caesar- und Vigenère-Verschlüsselung: Es ist sehr aufwändig, den geheimen Schlüssel vorab dem Empfänger mitzuteilen.

So scheint der Schlüsseltausch mit einem Geschäftspartner in der gleichen Stadt noch machbar. Im weltweiten Internet mit einem Kommunikationspartner in New York allerdings wird der sichere Austausch schon schwieriger. Den geheimen Schlüssel über das Internet zu versenden und darauf zu hoffen, dass niemand ihn abfängt, wäre wohl etwas blauäugig. Die Amerikaner Whitfield Diffie und Martin Hellman behoben diesen Nachteil 1975 mit der Entwicklung des asymmetrischen Verschlüsselungsverfahrens.

Dabei hat jeder Kommunikationspartner ein eigenes Schlüsselpaar. Dieses besteht aus einem öffentlichen Schlüssel, den du in die weite Welt hinausposaunen kannst und einem privaten Schlüssel, den du unter allen Umständen geheim halten solltest. Will dir jemand eine E-Mail zusenden, verschlüsselt er diese mit **deinem** öffentlichen Schlüssel. Nur du kannst diese E-Mail wieder entschlüsseln, da nur du in Besitz des zugehörigen privaten Schlüssels bist: E-Mails, die mit dem öffentlichen Schlüssel deines Schlüsselpaares verschlüsselt wurden, können nur mit deinem privaten Schlüssel wieder entschlüsselt werden. Fängt ein Datendieb deine E-Mail ab, sieht er nur Hieroglyphen. Es nutzt ihm auch nichts, wenn er über deinen öffentlichen Schlüssel verfügt, denn den darf eh jeder besitzen.

Beispiel



Arbeitsauftrag

Anna wohnt in den USA und Bert in Berlin. Beide legen sich ein Schlüsselpaar an und tauschen verschlüsselte E-Mails aus.

1. Welche Schlüssel tauschen Anna und Bert aus? Können Sie sich gefahrlos diese Schlüssel über das Internet zusenden?

2. Skizziere und beschreibe das Verschlüsseln, Übertragen und Entschlüsseln einer E-Mail von Anna zu Bert.

3. Skizziere und beschreibe das Verschlüsseln, Übertragen und Entschlüsseln der Antwortmail von Bert zu Anna.

Arbeitsmaterialien für den Unterricht
Übungen zum Einsatz von GnuPG oder PGP

1. Erstelle ein Schlüsselpaar.

2. Tausche deinen öffentlichen Schlüssel – zum Beispiel per E-Mail – mit deinen Mitschülern.

3. Binde die öffentlichen Schlüssel deiner Mitschüler in dein Verschlüsselungsprogramm ein.

4. Schreibe eine E-Mail an einen Mitschüler und verschlüssele diese mit seinem öffentlichen Schlüssel. Sende ihm die verschlüsselte E-Mail zu.

5. Entschlüssele empfangene E-Mails mit deinem privaten Schlüssel.

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden.

Dies gilt für Landtags-, Bundestags- und Kommunalwahlen sowie auch für die Wahl der Mitglieder des Europäischen Parlaments.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken und Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt. Unabhängig davon, wann, auf welchem Wege und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zu Gunsten einzelner politischer Gruppen verstanden werden könnte.

www.secure-it.nrw.de
www.mwa.nrw.de

Ministerium für Wirtschaft und Arbeit des Landes Nordrhein-Westfalen
NRW.
secure IT®