

JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schwickert, Axel; Schick; Lukas; Schramm, Laura;
Hein, Melanie

Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails – Reader zur WBT-Serie

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 01/2019
ISSN 1613-6667

Arbeitspapiere WI Nr. 1 / 2019

Autoren: Schwickert, Axel; Schick, Lukas; Schramm, Laura; Hein, Melanie

Titel: Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails – Reader zur WBT-Serie

Zitation: Schwickert, Axel; Schick, Lukas; Schramm, Laura; Hein, Melanie: Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 1/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019, 54 Seiten, ISSN 1613-6667.

Kurzfassung: Das vorliegende Arbeitspapier dient als Reader zur WBT-Serie „Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails“, die im E-Campus Wirtschaftsinformatik online zur Verfügung steht.

Grundlagen der Verschlüsselung, sowie das Vorgehen zur Verschlüsselung, Entschlüsselung und das Signieren von Dateien und E-Mails werden erläutert. Dazu werden die symmetrischen und asymmetrischen Verschlüsselungsverfahren eingeführt und näher beschrieben. Die Bedeutung von Schlüsselpaaren, bestehend aus einem öffentlichen und einem privaten Schlüssel, ist diesbezüglich essentiell. Im zweiten Abschnitt wird gezeigt, wie Dateien mithilfe von Verschlüsselungssoftware auf den Plattformen Windows und macOS Schritt für Schritt gesichert werden können. Im dritten und letzten Abschnitt erfolgt das Verschlüsseln, Entschlüsseln und Signieren von E-Mails mithilfe von Verschlüsselungssoftware auf den Plattformen Windows und macOS.

Schlüsselwörter: Grundlagen der Verschlüsselung, Verschlüsseln, Entschlüsseln, Signieren

A Zur Einordnung der WBT-Serie

Die WBT-Serie richtet sich an Interessenten des Themenbereiches „Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails“.

Für Ihr Selbststudium per WBT müssen Sie einen Internet-Zugang haben – entweder auf Ihren eigenen PCs, auf den PCs im JLU-Hochschulrechenzentrum, in den JLU-Bibliotheken oder dem PC-Pool des Fachbereichs.

B Die Web-Based Trainings

Der Stoff zu diesem Thema ist in Lerneinheiten zerlegt worden und wird durch eine Serie von Web-Based-Trainings (WBT) vermittelt. Mit Hilfe der WBT kann der Stoff im Eigenstudium erarbeitet werden. Die WBT bauen inhaltlich aufeinander auf und sollten in der angegebenen Reihenfolge absolviert werden.

WBT-Nr.	WBT-Bezeichnung	Bearbeitungs-dauer
1	Grundlagen der Verschlüsselung	45 Min.
2	Verschlüsseln, Entschlüsseln und Signieren von Dateien	45 Min.
3	Verschlüsseln, Entschlüsseln und Signieren von E-Mails	45 Min.

Tab. 1: Übersicht WBT-Serie

Die Inhalte der einzelnen WBT werden nachfolgend in diesem Dokument gezeigt. Alle WBT stehen Ihnen rund um die Uhr online zur Verfügung. Sie können jedes WBT beliebig oft durcharbeiten. In jedem WBT sind enthalten:

- Vermittlung des Lernstoffes
- interaktive Übungen zum Lernstoff
- abschließende Tests zum Lernstoff

Inhaltsverzeichnis

Seite

A Zur Einordnung der WBT-Serie I

B Die Web-Based Trainings II

Inhaltsverzeichnis III

Abbildungsverzeichnis VI

Tabellenverzeichnis VII

Abkürzungsverzeichnis VIII

1 Die WBT-Serie „Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails“ 1

2 Grundlagen der Verschlüsselung 2

2.1 Praktikum in der Securenet Consulting GmbH 2

2.1.1 Ein Student stellt sich vor 2

2.1.2 Die Vorbereitung auf das Praktikum 2

2.1.3 Was bedeutet Verschlüsselung? 3

2.2 Symmetrische und asymmetrische Verschlüsselungsverfahren 3

2.2.1 Das Netzwerk der Universität Gießen 3

2.2.2 Die Geschichte der Verschlüsselung 4

2.2.3 Beispiel symmetrischer Verschlüsselungsverfahren 5

2.2.4 Die symmetrische Verschlüsselung 6

2.2.5 Die Entwicklung der Verschlüsselung 7

2.2.6 Der private und öffentliche Schlüssel 8

2.2.7 Die Handhabung des privaten und öffentlichen Schlüssels 9

2.2.8 Die asymmetrische Verschlüsselung 10

2.2.9 Die praktische Anwendung 11

2.3 Abschlusstest - WBT 01 11

2.3.1 Abschlusstest 11

2.3.2 Drag-and-Drop-Test - Teil 1 13

2.3.3 Drag-and-Drop-Test - Teil 2 14

3 Verschlüsseln, Entschlüsseln und Signieren von Dateien 15

3.1 Verschlüsselung von Dateien 15

3.1.1 Der erste Praktikumstag 15

3.1.2 Den Arbeitsplatz einrichten 15

3.2 Anwendung der Verschlüsselungs-Software Gpg4win (Windows) 16

3.2.1 Die Installation der Software Gpg4win 16

3.2.2 Die Werkstudentin Anna stellt sich vor 16
3.2.3 Das Verschlüsseln einer Datei mit Gpg4win 17
3.2.4 Das Entschlüsseln einer Datei mit Gpg4win 18
3.2.5 Das Signieren einer Datei mit Gpg4win 18
3.2.6 Die Gültigkeit und der Bezug von öffentlichen Schlüsseln 19
3.2.7 Der Fingerabdruck-Vergleich 20
3.2.8 Einen neuen Schlüssel aufnehmen 21
3.2.9 Das Abschlussgespräch 21
3.3 Anwendung der Verschlüsselungs-Software GPG Suite (macOS) 22
3.3.1 Installation der Software GPG Suite 22
3.3.2 Die Werkstudentin Anna stellt sich vor 22
3.3.3 Das Verschlüsseln einer Datei mit GPG Suite 23
3.3.4 Das Entschlüsseln einer Datei mit GPG Suite 24
3.3.5 Das Signieren einer Datei mit GPG Suite 24
3.3.6 Die Gültigkeit und der Bezug von öffentliche Schlüsseln 25
3.3.7 Der Fingerabdruck-Vergleich 26
3.3.8 Einen neuen Schlüssel aufnehmen 27
3.3.9 Das Abschlussgespräch 27
3.4 Abschlusstest – WBT 02 28
3.4.1 Abschlusstest 28

4 Verschlüsseln, Entschlüsseln und Signieren von E-Mails 30
4.1 Der zweite Praktikumstag 30
4.1.1 Früh am Morgen 30
4.1.2 Team-Besprechung in der Securenet Consulting GmbH 30
4.1.3 Hintergrund zur E-Mail-Verschlüsselung 31
4.1.4 Das Prinzip der asymmetrischen E-Mail-Verschlüsselung 31
4.1.5 Auswahl Deines Betriebssystems 32
4.2 Verschlüsseln, Entschlüsseln und Signieren von E-Mails mit Windows 32
4.2.1 Die Vorbereitung 32
4.2.2 Überprüfung des Outlook-Plugins 34
4.2.3 Das Verschlüsseln und Signieren einer E-Mail mit Gpg4win 35
4.2.4 Das Entschlüsseln einer E-Mail mit Gpg4win 35
4.2.5 Das Abschlussgespräch 35
4.3 Verschlüsseln, Entschlüsseln und Signieren von E-Mails mit macOS 36
4.3.1 Die Vorbereitung 36
4.3.2 Überprüfung des Apple Mail-Plugins 37
4.3.3 Das Verschlüsseln und Signieren einer E-Mail mit GPG Suite 38
4.3.4 Das Entschlüsseln einer E-Mail mit GPG Suite 38
4.3.5 Das Abschlussgespräch 39
4.4 Abschlusstest – WBT 03 39
4.4.1 Abschlusstest 39
4.4.2 Drag-and-Drop-Test 41

5 Anhang..... VIII

Abbildungsverzeichnis

Seite

Abb. 1: Unternehmenslogo der Securenet Consulting GmbH 2
Abb. 2: Netzwerk der Justus-Liebig-Universität 3
Abb. 3: Verschiebung des Alphabets um drei Buchstaben nach Caesar 4
Abb. 4: Caesar-Verschlüsselung als Klartext 4
Abb. 5: Caesar-Verschlüsselung als verschlüsselter Text 4
Abb. 6: Polybius Matrix 5
Abb. 7: Polybius Matrix - Verschlüsselter Text „22“ 5
Abb. 8: Polybius Matrix - Verschlüsselter Text „15“ 5
Abb. 9: Polybius Matrix - Verschlüsselter Text „23“ 6
Abb. 10: Polybius Matrix - Verschlüsselter Text „15“ 6
Abb. 11: Polybius Matrix - Verschlüsselter Text „24“ 6
Abb. 12: Polybius Matrix - Verschlüsselter Text „32“ 6
Abb. 13: Die symmetrische Verschlüsselung 7
Abb. 14: Der private und öffentliche Schlüssel 8
Abb. 15: Der private und öffentliche Schlüssel als eigenständige Dateien 9
Abb. 16: Bekanntmachung des öffentlichen Schlüssels 9
Abb. 17: Geheimhaltung des privaten Schlüssels 10
Abb. 18: Die asymmetrische Verschlüsselung 10
Abb. 19: Drag-and-Drop-Test - WBT 01 – Teil 1 13
Abb. 20: Drag-and-Drop-Test - WBT 01 – Teil 2 14
Abb. 23: Unternehmenslogo der Securenet Consulting GmbH 15
Abb. 24: Beliebige E-Mail-Adressen von Robin 19
Abb. 25: Beliebige E-Mail-Adressen von Robin 25
Abb. 26: Die asymmetrische E-Mail-Verschlüsselung 31
Abb. 27: Das Logo von GpgOL 34
Abb. 28: Überprüfung des Outlook-Plugins GpgOL 34
Abb. 29: Das Logo von GPGMail 37
Abb. 30: Überprüfung des Apple Mail-Plugins GPGMail 38
Abb. 31: Drag-and-Drop-Test - WBT 03 41
Abb. 21: Lösung Drag-and-Drop-Test - WBT 01 – Teil 1 IX
Abb. 22: Lösung Drag-and-Drop-Test - WBT 01 – Teil 2 X
Abb. 32: Lösung Drag-and-Drop-Test - WBT 03 XII

Tabellenverzeichnis

Seite

Tab. 1: Übersicht WBT-Serie II
Tab. 2: Abschlusstest - WBT 01 13
Tab. 4: Abschlusstest - WBT 02 29
Tab. 6: Abschlusstest - WBT 03 40
Tab. 3: Lösungen Abschlusstests - WBT 01 IX
Tab. 5: Lösungen Abschlusstest - WBT 02 XI
Tab. 7: Lösungen Abschlusstest - WBT 03 XII

Abkürzungsverzeichnis

BWL ……..……Betriebswirtschaftslehre
bzw. ……..…… beziehungsweise
E-Mail ……..……. electronic mail
GmbH ……... Gesellschaft mit beschränkter Haftung
WBT …….…….Web-Based-Training
z. B. ……...……... zum Beispiel

1 Die WBT-Serie „Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails“

Die WBT-Serie „Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails“ hat zum Ziel, einen kurzen Überblick über die Grundlagen der Verschlüsselung und die Anwendungsmöglichkeiten von zwei verschiedenen Verschlüsselungs-Software-Tools zu geben. Die allgemeinen Grundlagen zur Verschlüsselung sowie die Funktionsweise der Software-Tools „Gpg4win“ und „GPG Suite“ werden dabei anhand eines Modellunternehmens und des dortigen Aufgabengebietes demonstriert. So werden unter anderem zunächst die wesentlichen Unterschiede zwischen symmetrischer und asymmetrischer Verschlüsselung sowie zwischen geheimen, öffentlichen und privaten Schlüsseln anhand einfacher Beispiele aufgezeigt. Nachdem auf die einzelnen Verschlüsselungsverfahren und ihre Bestandteile näher eingegangen wurde, werden die Ziele, Funktionen und Anwendungsmöglichkeiten der Software-Tools „Gpg4win“ und „GPG Suite“ zur Verschlüsselung, Entschlüsselung und dem Signieren von Dateien und E-Mails veranschaulicht.

2 Grundlagen der Verschlüsselung

2.1 Praktikum in der Securenet Consulting GmbH

2.1.1 Ein Student stellt sich vor

Robin Schmidt (Praktikant):

„Hallo! Ich bin Robin, BWL-Student der Justus-Liebig-Universität in Gießen. Im Rahmen meines Studiums beginne ich morgen ein dreimonatiges Praktikum im Bereich IT-Security in der Securenet Consulting GmbH (Abb. 1). Leider habe ich gerade wenig Zeit, um Euch mehr darüber zu erzählen. Denn ich muss mich noch ein bisschen auf meinen ersten Tag vorbereiten. Als Erstes checke ich meine E-Mails!“

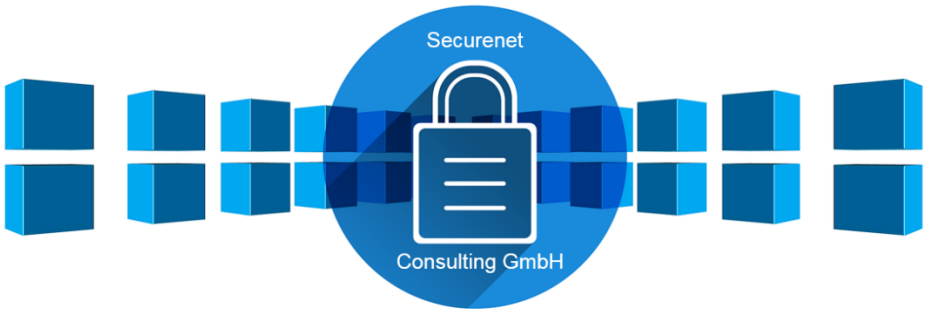


Abb. 1: Unternehmenslogo der Securenet Consulting GmbH

2.1.2 Die Vorbereitung auf das Praktikum

Robin Schmidt (Praktikant):

„Oh! Ich habe eine neue Nachricht.“

E-Mail von Frau Jung (Senior Consultant):

„Hallo Robin,

im Name der Securenet Consulting GmbH heiße ich Dich als neuen Praktikanten in unserem Unternehmen herzlich willkommen.

Wie Du sicher weißt, betreut die Securenet Consulting GmbH als mittelständische Unternehmensberatung Kunden zum Thema Datensicherheit. Dabei unterstützt unsere Beratung Unternehmen aus den unterschiedlichsten Branchen. Denn Datensicherheit spielt heutzutage in allen Unternehmen eine wichtige Rolle.

Mein verantwortlicher Aufgabenbereich liegt in der Kryptografie, unter anderem in der Verschlüsselung und Entschlüsselung von vertraulichen Dateien. Dies wird

auch Dein Aufgabenbereich ab morgen sein. Ich freue mich schon, Dich persönlich kennen zu lernen.

Freundliche Grüße,
Deine Betreuerin
Frau Jung“

2.1.3 Was bedeutet Verschlüsselung?

Robin Schmidt (Praktikant):

„Ach herrje!

Ich habe das Thema Verschlüsselung bereits vor einiger Zeit im Modul Wirtschaftsinformatik behandelt. Leider kann ich mich an die Einzelheiten nicht mehr so genau erinnern. Ich sollte mich auf jeden Fall nochmal in das Thema einlesen, damit ich für morgen gut vorbereitet bin. Am besten suche ich meine Unterlagen aus dem entsprechendem Semester nochmal heraus.“

2.2 Symmetrische und asymmetrische Verschlüsselungsverfahren

2.2.1 Das Netzwerk der Universität Gießen

Robin Schmidt (Praktikant):

„Zum Glück kann ich meine Unterlagen ganz einfach im Netzwerk der Justus-Liebig-Universität (Abb. 2) suchen. Ich versuche es mal mit dem Begriff ‚Verschlüsselung‘.“



Abb. 2: Netzwerk der Justus-Liebig-Universität

2.2.2 Die Geschichte der Verschlüsselung

Der Überlieferung nach verschlüsselte der römische Feldherr Caesar seine militärischen Nachrichten für die geheime Kommunikation mit seinen Soldaten. Caesar nutzte dafür eine Verschiebung des Alphabets um drei Buchstaben (Abb. 3).

klar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
geheim	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Abb. 3: Verschiebung des Alphabets um drei Buchstaben nach Caesar

Aus dem Klartext „caesar“ (Abb. 4) wird der verschlüsselte Text „FDHVDU“ (Abb. 5). Dies ist ein Beispiel für eine sog. „symmetrische“ Verschlüsselung. Zur Verschlüsselung und zur Entschlüsselung nutzen Sender und Empfänger der Nachricht den gleichen Schlüssel („Schlüssel-Symmetrie“).

klar	**a**	b	**c**	d	**e**	f	g	h	i	j	k	l	m	n	o	p	q	**r**	**s**	t	u	v	w	x	y	z
geheim	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Abb. 4: Caesar-Verschlüsselung als Klartext

klar	**a**	b	**c**	d	**e**	f	g	h	i	j	k	l	m	n	o	p	q	**r**	**s**	t	u	v	w	x	y	z
geheim	**D**	E	**F**	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	**U**	**V**	W	X	Y	Z	A	B	C

Abb. 5: Caesar-Verschlüsselung als verschlüsselter Text

Der Schlüssel im Caesar-Beispiel lautet „Verschiebe um 3 Buchstaben“. Dieser Schlüssel musste natürlich vor den Feinden geheim gehalten werden.

Damit nur Caesars Offiziere seine Nachrichten von Geheimtext in Klartext umwandeln konnten, musste Caesar den Offizieren vorher den geheimen Schlüssel mitgeteilt haben.

Caesar konnte das noch recht einfach bewerkstelligen. Bevor er mit seinem Heer in den Krieg zog, teilte er seinen Offizieren in Rom den geheimen Schlüssel im persönlichen Gespräch mit.

2.2.3 Beispiel symmetrischer Verschlüsselungsverfahren

Der griechische Geschichtsschreiber Polybius (etwa 200 v. Chr.) verwendete ein anderes Verfahren zur Verschlüsselung seiner Nachrichten.

Dabei ersetzte er die Buchstaben des Alphabets durch zweistellige Zahlen. Die Buchstaben des Alphabetes werden dazu in eine Matrix aus 5 Zeilen und 5 Spalten eingetragen (Abb. 6). Bei diesem Verfahren besetzen die Buchstaben „I“ und „J“ denselben Platz.

Beim Verschlüsseln wird jeder Buchstabe durch ein Zahlenpaar ersetzt, das sich aus seiner Position der Zeilen- und Spaltennummer ergibt. Der Buchstabe „D“ wird beispielsweise durch die Zahl 14, der Buchstabe „R“ durch 42 ersetzt. Aus dem Klartext „Geheim“ wird der verschlüsselte Text „22 15 23 15 24 32“ (Abb. 7-12).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 6: Polybius Matrix

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 7: Polybius Matrix - Verschlüsselter Text „22“

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 8: Polybius Matrix - Verschlüsselter Text „15“

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 9: Polybius Matrix - Verschlüsselter Text „23“

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 10: Polybius Matrix - Verschlüsselter Text „15“

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 11: Polybius Matrix - Verschlüsselter Text „24“

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abb. 12: Polybius Matrix - Verschlüsselter Text „32“

2.2.4 Die symmetrische Verschlüsselung

In der Vergangenheit nutzten Caesar und Polybius geheime Verfahren zur Verschlüsselung und Entschlüsselung von Nachrichten. Im heutigen E-Business wird auf geheime Passwörter (auch „Passphrases“ genannt) zur symmetrischen Verschlüsselung und Entschlüsselung zurückgegriffen.

Die symmetrische Verschlüsselung wird auch als „Secret-Key-Verfahren“ bezeichnet und basiert auf einer Schlüssel-Symmetrie. Das heißt sowohl zum Verschlüsseln als auch zum Entschlüsseln wird der gleiche geheime Schlüssel verwendet (Abb. 13).

Das Secret-Key-Verfahren basiert auf einer speziellen mathematischen Funktion, die einen Klartext in Abhängigkeit eines Schlüssels (digitaler Code) in einen Geheimtext umwandelt.

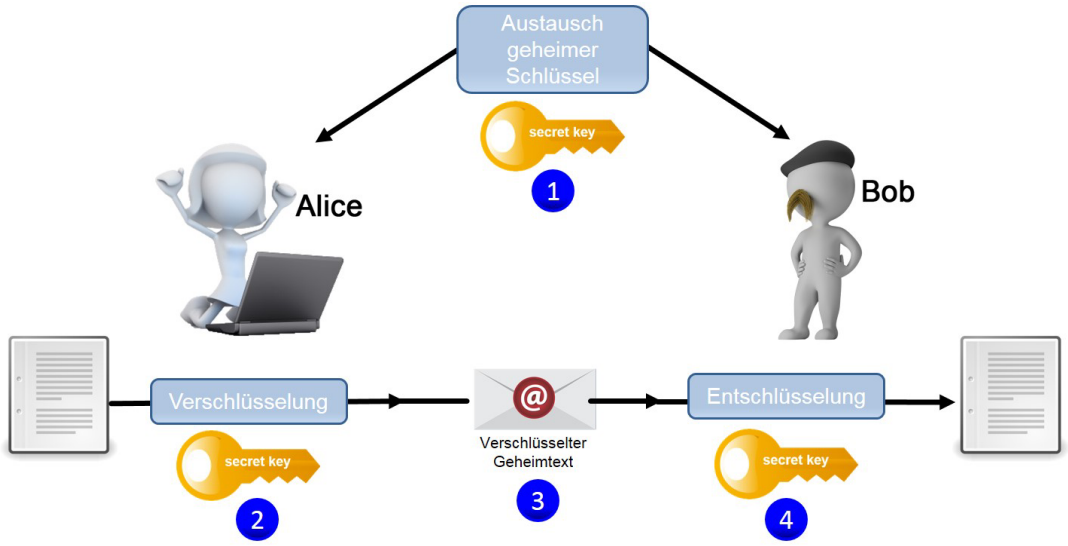


Abb. 13: Die symmetrische Verschlüsselung

(1) Alice und Bob tauschen untereinander einen geheimen Schlüssel aus.

(2) Alice schreibt den Klartext ihrer Nachricht „Klartext“ und verschlüsselt ihn mit dem geheimen Schlüssel, den Bob und Alice untereinander ausgetauscht haben. Es entsteht eine Nachricht mit dem Geheimtext.

(3) Alice schickt die Datei mit dem Geheimtext per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

(4) Bob kann die Geheimtext-Datei mit dem geheimen Schlüssel, den Alice und Bob untereinander ausgetauscht haben in Klartext umwandeln.

2.2.5 Die Entwicklung der Verschlüsselung

Robin Schmidt (Praktikant):

„Eins verstehe ich nicht...

Wie hilft ein symmetrisches Verschlüsselungsverfahren, wenn im heutigen Internet zwei Personen miteinander geheim kommunizieren wollen?

Die Personen kennen sich doch nicht und haben auch keine Gelegenheit, vor ihrer Kommunikation einen gemeinsamen („symmetrischen“) geheimen Schlüssel auszutauschen.

Also spielen im Internet zur Verschlüsselung von Nachrichten zwischen anonymen Kommunikationspartnern andere Verschlüsselungsverfahren eine zentrale Rolle. Ich erinnere mich, dass es auch ‚asymmetrische‘ Verschlüsselungsverfahren mit zwei unterschiedlichen Schlüssel gibt. Dabei herrscht sogenannte ‚Schlüssel-Asymmetrie‘.“

2.2.6 Der private und öffentliche Schlüssel

Bei den asymmetrischen Verfahren besitzt jeder Kommunikationsteilnehmer ein eigenes Schlüsselpaar. Das Schlüsselpaar besteht aus einem öffentlichen Schlüssel (public key) und einem privaten Schlüssel (private key) (Abb. 14).

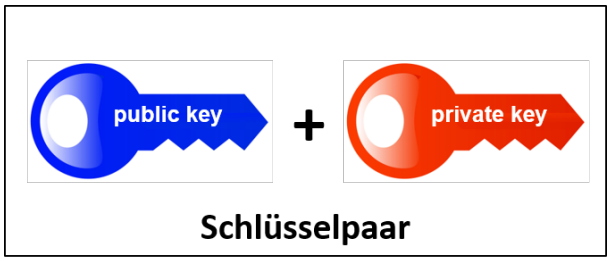


Abb. 14: Der private und öffentliche Schlüssel

Jedes Schlüsselpaar wird absolut individuell für eine bestimmte einzelne Person erstellt. Aus technischer Sicht besteht jeder einzelne Schlüssel aus einer langen Zeichenabfolge, die als eine eigenständige Datei auf dem Rechner abgespeichert wird (Abb. 15).

Der öffentliche und der private Schlüssel sind über ein kompliziertes mathematisches Verfahren eindeutig miteinander verbunden.

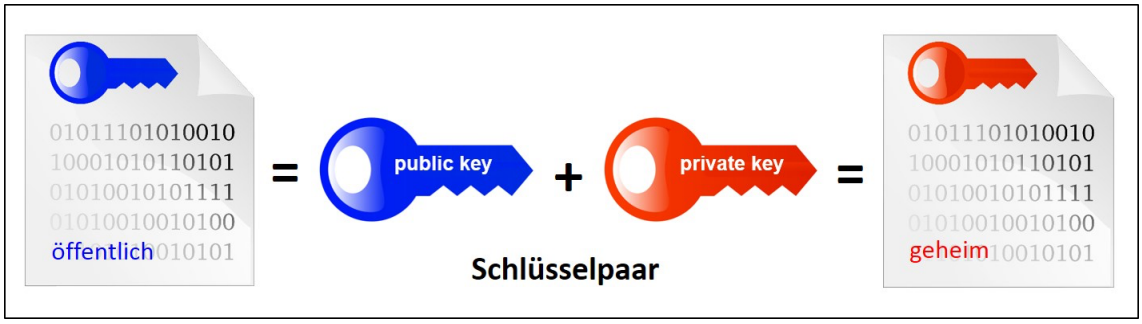


Abb. 15: Der private und öffentliche Schlüssel als eigenständige Dateien

2.2.7 Die Handhabung des privaten und öffentlichen Schlüssels

Um eine geheime Nachricht zu schicken, muss der Absender der Nachricht den öffentlichen Schlüssel des Empfängers kennen (Abb. 16). Seinen privaten Schlüssel hält der Empfänger jedoch geheim (Abb. 17).



Abb. 16: Bekanntmachung des öffentlichen Schlüssels

Jeder Kommunikationsteilnehmer gibt seinen eigenen öffentlichen Schlüssel bekannt. Dies erfolgt häufig durch das Einstellen seiner Datei mit dem öffentlichen Schlüssel in sogenannte „Schlüssel-Listen“. Diese Listen kann jeder im Internet offen einsehen. Jeder kann auch die Datei mit seinem öffentlichen Schlüssel an seine E-Mails anhängen.

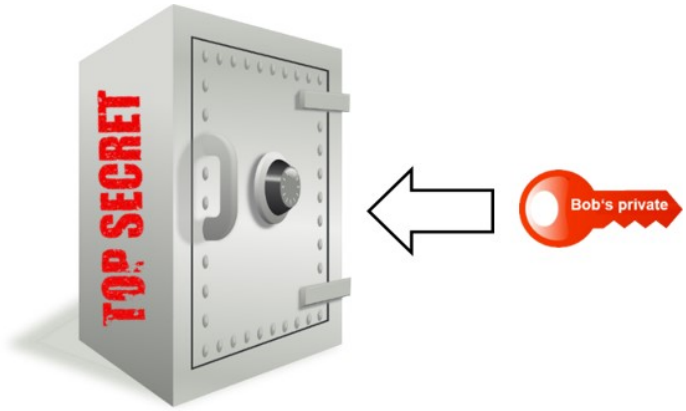


Abb. 17: Geheimhaltung des privaten Schlüssels

Nur Sie kennen den privaten Schlüssel aus Ihrem persönlichen Schlüsselpaar. Die Datei Ihres privaten Schlüssels ist auf Ihrem persönlichen Rechner gespeichert. Daher sollten Sie auf den Rechner und die Datei gut aufpassen.

2.2.8 Die asymmetrische Verschlüsselung

Die asymmetrische Verschlüsselung wird auch als „Public-Key-Verfahren“ bezeichnet. Der wesentliche Unterschied zur symmetrischen Verschlüsselung ist, dass die asymmetrische Verschlüsselung mit zwei unterschiedlichen Schlüsseln arbeitet (Abb. 18).

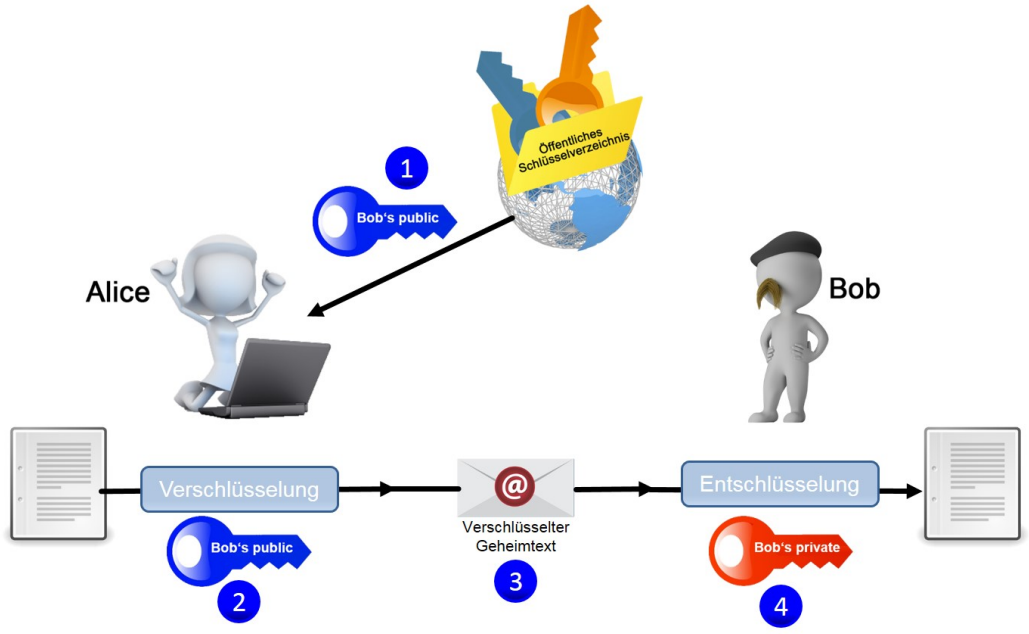


Abb. 18: Die asymmetrische Verschlüsselung

(1) Alice holt sich den öffentlichen Schlüssel von Bob aus der öffentlichen Schlüssel-Liste.

(2) Alice schreibt den Klartext ihrer Nachricht „Klartext“ und verschlüsselt ihn mit dem öffentlichen Schlüssel von Bob. Es entsteht eine Nachricht mit dem Geheimtext.

(3) Alice schickt die Datei mit dem Geheimtext per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

(4) Nur Bob kann die Geheimtext-Datei mit seinem privaten Schlüssel in Klartext umwandeln.

2.2.9 Die praktische Anwendung

Robin Schmidt (Praktikant):

„Jetzt erinnere ich mich wieder!

Die asymmetrische Verschlüsselung und Entschlüsselung von Dateien wird heute vollständig durch Software-Tools automatisiert. Bestimmt werde ich ein solches Software-Tool im Laufe meines Praktikums in der Securenet Consulting GmbH in der praktischen Anwendung kennenlernen. Ich bin schon ganz gespannt auf morgen!“

2.3 Abschlusstest - WBT 01

2.3.1 Abschlusstest

Bitte beantworten Sie die folgenden Fragen durch Ankreuzen der korrekten Antworten (Tab. 2). Bei einigen Fragen können auch mehrere Antworten richtig sein.

Nr.	Frage	Richtig	Falsch
1	Welche Verschlüsselungsverfahren werden unterschieden?		
	Vertikale Verschlüsselung		
	Asymmetrische Verschlüsselung		
	Symmetrische Verschlüsselung		
	Horizontale Verschlüsselung		

2	Verschlüsselung ist die Umwandlung von Informationen mit Hilfe bestimmter Verschlüsselungsverfahren, so dass unberechtigte Personen sie nicht lesen können.		
	Richtig		
	Falsch		
3	Die symmetrische Verschlüsselung wird auch als „Public-Key-Verfahren“ bezeichnet.		
	Richtig		
	Falsch		
4	Welche Schlüssel bilden bei asymmetrischen Verschlüsselungsverfahren ein Schlüsselpaar?		
	Öffentlicher Schlüssel		
	Geheimer Schlüssel		
	Privater Schlüssel		
5	Bei der Verschlüsselung einer Datei mit dem asymmetrischen Verschlüsselungsverfahren erfolgt das Verschlüsseln mit dem privaten Schlüssel des Absenders und das Entschlüsseln mit dem öffentlichen Schlüssel des Empfängers.		
	Richtig		
	Falsch		
6	Wozu dient der geheime Schlüssel in symmetrischen Verschlüsselungsverfahren?		
	zum Verschlüsseln		
	zum Entschlüsseln		
	nichts von beidem		
7	Jeder, der Ihren öffentlichen Schlüssel kennt, kann für Sie Dateien verschlüsseln, die nur Sie mit Ihrem privaten Schlüssel entschlüsseln können.		
	Richtig		
	Falsch		

8	Aus technischer Sicht besteht ein Schlüsselpaar in asymmetrischen Verschlüsselungsverfahren aus einer langen Zeichenabfolge, die als eigenständige Datei auf dem Rechner gespeichert wird.		
	Richtig		
	Falsch		

Tab. 2: Abschlusstest - WBT 01

2.3.2 Drag-and-Drop-Test - Teil 1

Bitte ordnen Sie die Objekte für eine asymmetrische Verschlüsselung richtig zu (Abb. 19).

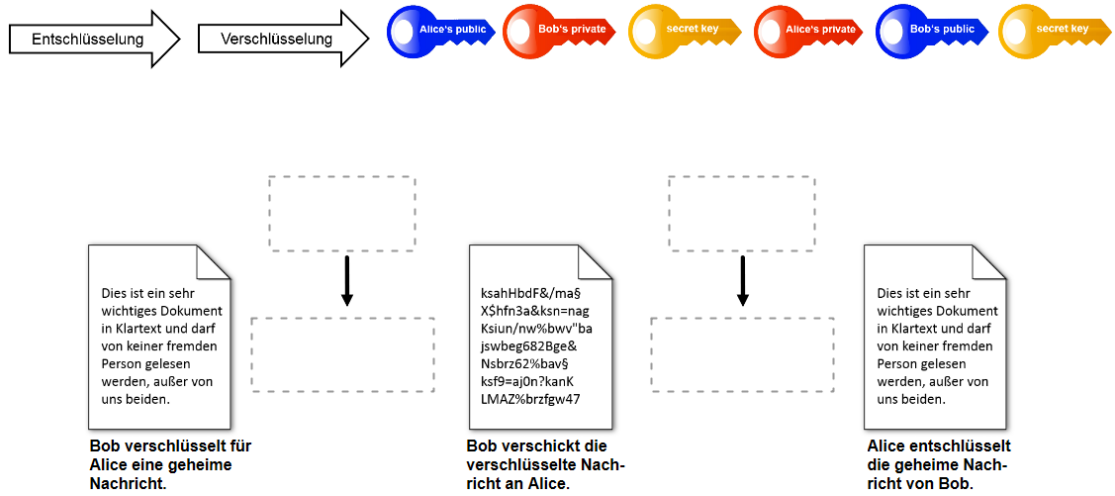


Abb. 19: Drag-and-Drop-Test - WBT 01 – Teil 1

2.3.3 Drag-and-Drop-Test - Teil 2

Bitte ordnen Sie die Objekte für eine symmetrische Verschlüsselung richtig zu (Abb. 20).

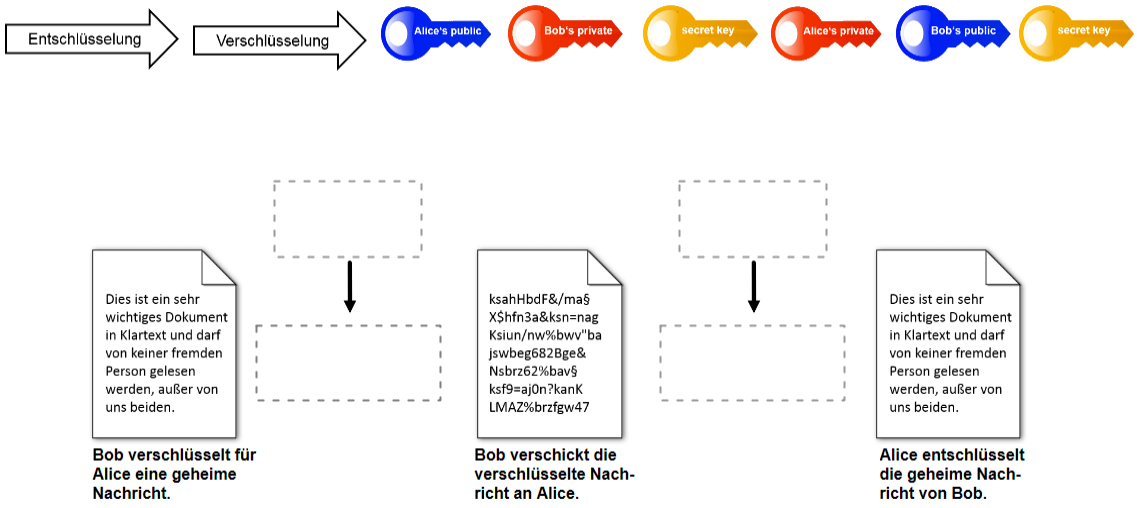


Abb. 20: Drag-and-Drop-Test - WBT 01 – Teil 2

3 Verschlüsseln, Entschlüsseln und Signieren von Dateien

3.1 Verschlüsselung von Dateien

3.1.1 Der erste Praktikumstag

Frau Jung (Senior Consultant):

„Hallo Robin! Willkommen bei der Securenet Consulting GmbH (Abb. 21)!
Ich bin Frau Jung, Senior Consultant im Bereich IT-Security.

Ich werde Dich in Deiner Praktikumszeit betreuen. Das heißt wenn Du Fragen hast, kannst Du gerne jederzeit zu mir kommen.

Da Du nun einige Wochen bei uns bleiben wirst, müssen wir zunächst Deinen Laptop entsprechend einrichten. Wie bereits in meiner E-Mail erwähnt, drehen sich unsere Projekte um die Verschlüsselung, die Entschlüsselung und das Signieren von Dateien. Hierfür benötigst Du als Erstes eine Verschlüsselungs-Software. Aber bevor wir loslegen, zeige ich Dir erstmal Deinen Arbeitsplatz.“

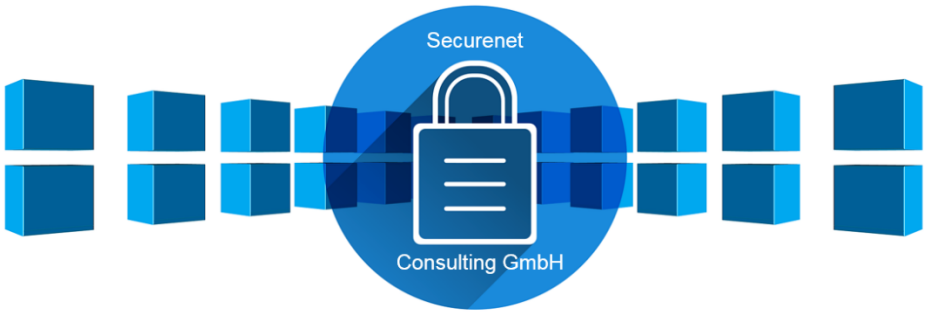


Abb. 21: Unternehmenslogo der Securenet Consulting GmbH

3.1.2 Den Arbeitsplatz einrichten

Frau Jung (Senior Consultant):

„Super, Du hast Deinen Laptop mitgebracht! Ich sehe Du hast Dich vorbereitet. Für die Installation der Verschlüsselungs-Software müssen wir erstmal nachsehen, welches Betriebssystem Du auf Deinem Rechner verwendest.

Denn wir verwenden für das Windows Betriebssystem die Verschlüsselungs-Software Gpg4win und für das Betriebssystem macOS die Software GPG Suite. Darf ich fragen, welches Betriebssystem auf Deinem Laptop installiert ist?“

Robin Schmidt (Praktikant):

„Auf meinem Laptop ist die neuste Version des Betriebssystems von Windows bzw. macOS installiert."

Hinweis: An dieser Stelle können Sie entscheiden, welches Betriebssystem Sie auf ihrem Rechner verwenden. Je nach Betriebssystem kommt für Sie folgendes Kapitel als nächstes in Frage: 3.2 Anwendung der Verschlüsselungs-Software Gpg4win (Windows) oder 3.3 Anwendung der Verschlüsselungs-Software GPG Suite (macOS).

3.2 Anwendung der Verschlüsselungs-Software Gpg4win (Windows)

3.2.1 Die Installation der Software Gpg4win

1. Lade auf der Web Site https://www.gpg4win.de die neuste Version von Gpg4win herunter.
2. Starte die Installation, indem Du die heruntergeladene .exe-Datei doppelklickst. Folge dann der Installationsanweisung.
3. Nach erfolgter Installation kannst Du die .exe-Installationsdatei in den Papierkorb legen. Durch diese Installation wurde auf Deinem Rechner das Programm „Kleopatra" installiert.

Gpg4win enthält neben dem Programm Kleopatra noch weitere Programme, die bei der Installation automatisch mitinstalliert werden:

- GnuPG (für mathematische Verschlüsselungsoperationen)
- GpgOL (Funktionserweiterung für Microsoft Outlook)
- GpgEX (Plugin, welches Gpg4win-Funktionalitäten in andere Anwendungen integriert)

Die Funktionsweise und der genaue Nutzen richtet sich jedoch an fortgeschrittene Nutzer und wird in diesem WBT nicht weiter erläutert.

3.2.2 Die Werkstudentin Anna stellt sich vor

Frau Jung (Senior Consultant):

„So Robin, dann lass uns beide zu Deinem Arbeitsplatz gehen!

Oh halt, mein Chef ruft an!

Tut mir leid Robin, ich muss dringend los. Ich habe noch einen Termin mit dem Vorstand. Soweit haben wir alles Notwendige zum Verschlüsseln, zum Entschlüsseln und zum Signieren von Dateien auf Deinem Laptop installiert. Da Du Dir dein Büro mit Anna unserer Werkstudentin teilen wirst, kannst Du Dir von ihr die Software erklären lassen. Bis später!“

Anna Fröhlich (Werkstudentin):

„Hallo Robin! Ich bin Anna, ebenfalls Studentin an der Justus-Liebig-Universität in Gießen. Ich erinnere mich an Dich. Wir haben zusammen das Modul Wirtschaftsinformatik besucht.

Vielleicht erinnerst Du Dich noch an das Verschlüsseln, Entschlüsseln und Signieren von Dateien mit asymmetrischen Verschlüsselungsverfahren. Dies übernimmt hier die installierte Software Gpg4win.

Bevor wir mit der Verschlüsselung starten, möchte ich Dir vorher noch kurz zeigen, wie Du ein Schlüsselpaar in Kleopatra erstellst. Denn das ist die Voraussetzung, um eine asymmetrische Verschlüsselung durchführen zu können. Könntest Du die Software starten?“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.2.3 Das Verschlüsseln einer Datei mit Gpg4win

Anna Fröhlich (Werkstudentin):

„So Robin, wir haben im ersten Schritt Dein persönliches Schlüsselpaar erstellt. Deinen öffentlichen Schlüssel kannst Du nun beliebig vielen Personen im Internet über Schlüssel-Listen mitteilen. Du kannst Deinen öffentlichen Schlüssel auch per E-Mail bestimmten Personen zukommen lassen.

Als Nächstes kannst Du Deinen öffentlichen Schlüssel nutzen, um eine beliebige Datei von Dir zu verschlüsseln. Natürlich kannst Du auch für jeden anderen Empfänger Dateien verschlüsseln, soweit Du deren öffentlichen Schlüssel besitzt.

Ich zeige Dir jetzt, wie ich eine Datei mit Deinem öffentlichen Schlüssel verschlüssele. Schau genau zu.“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.2.4 Das Entschlüsseln einer Datei mit Gpg4win

Anna Fröhlich (Werkstudentin):

„Robin, wir haben nun eine Datei mit Deinem öffentlichen Schlüssel erfolgreich verschlüsselt.

Im nächsten Schritt kannst nur Du mit Deinem, im ersten Schritt, erstellten privaten Schlüssel die verschlüsselte Datei wieder entschlüsseln.

Und so könnte auch jede weitere beliebige Person Dir eine Datei zusenden, die mit Deinem öffentlichen Schlüssel verschlüsselt wurde. Diese kannst nur Du mit Deinem privaten Schlüssel wieder entschlüsseln.

Die Entschlüsselung funktioniert ähnlich wie die Verschlüsselung nur unter zusätzlicher Eingabe deines Passworts für den privaten Schlüssel. Dieses Passwort hast Du bei der Erstellung des Schlüsselpaars selbst festgelegt, um deinen privaten Schlüssel zu schützen. Also bist Du jetzt an der Reihe.

Lass uns die Plätze tauschen!“

Robin Schmidt (Praktikant):

„Okay, los geht’s!“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.2.5 Das Signieren einer Datei mit Gpg4win

Robin Schmidt (Praktikant):

„Hm...jetzt habe ich aber doch eine Frage.

Wie kann ich sicherstellen, dass eine bestimmte Datei von Dir und niemand anderen stammt und nicht manipuliert wurde?“

Anna Fröhlich (Werkstudentin):

„Damit sichergestellt werden kann, dass eine bestimmte Datei von Dir und niemand anderem stammt und nicht manipuliert wurde, solltest Du diese signieren.

Soll ich es Dir zeigen?“

Signaturen werden mit privaten Schlüsseln erstellt und beziehen sich z. B. auf Dateien. Du kannst jede Art von Dateien signieren, es muss nicht zwingend eine verschlüsselte Datei sein. So könntest Du Word-, PowerPoint-, PDF-, ZIP-, TXT-Dateien oder jede andere beliebige Datei signieren.

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.2.6 Die Gültigkeit und der Bezug von öffentlichen Schlüsseln

Robin Schmidt (Praktikant):

„Super, vielen Dank Anna!
Das hat mir sehr weitergeholfen. Nun habe ich ein eigenes Schlüsselpaar. Aber das Verschlüsseln von Dateien mit dem eigenen öffentlichen Schlüssel ist nicht der Regelfall oder?

Wie ich sehe, ist es grundsätzlich jedem Nutzer möglich, Schlüsselpaare auf beliebige E-Mail-Adressen zu erstellen (Abb. 22). Es wird nicht sichergestellt, dass der Ersteller des Schlüsselpaares auch der Eigentümer der zugehörigen E-Mail-Adresse ist.“



Abb. 22: Beliebige E-Mail-Adressen von Robin

Anna Fröhlich (Werkstudentin):

„Genau! Daher ist es wichtig, dass Du im nächsten Schritt, nach Erstellung deines Schlüsselpaares, die ‚richtigen‘ öffentlichen Schlüssel Deiner Empfänger in Kleopatra importierst und verwendest.

Importierst Du den falschen öffentlichen Schlüssel und verschlüsselst damit eine Datei, kann der Empfänger diese nicht entschlüsseln. Zur Sicherstellung der Echtheit von Schlüsseln gibt es zwei Möglichkeiten in Kleopatra:

1. Die flüchtige, nicht sichere Kontrolle: Schlüssel ID-Vergleich
2. Die sichere Kontrolle: Fingerabdruck-Vergleich“

Die Schlüssel-ID ist ein 32-Bit-Wert, welcher in hexadezimaler Darstellung bereitgestellt wird. Diese Schlüssel-ID sollte für jedes Schlüsselpaar eindeutig sein.

Im Jahr 2014 wurde jedoch das Gegenteil bewiesen. Eine Kontrolle ausschließlich auf Basis der Schlüssel-ID reicht daher nicht aus. Vielmehr muss auf die Kontrolle über Fingerabdrücke zurückgegriffen werden.

Hier siehst Du eine Beispiel-Schlüssel-ID: 99FE4EB7

3.2.7 Der Fingerabdruck-Vergleich

Der Fingerabdruck ist einzigartig und stellt eine Art Quersumme dar, welche aus dem Schlüsselpaar errechnet wurde. Dieser Fingerabdruck hat eine entsprechende Länge und passt weltweit nur auf ein einziges Schlüsselpaar.

A767 1A57 5F87 B31E 2C26 2265 857F C948 99FE 4EB7

In Kleopatra können Sie sich per Doppelklick auf den entsprechenden Schlüssel oder über Rechtsklick auf den Schlüssel und dem Eintrag „Details“ die Details eines Schlüssels anzeigen lassen.

Im unteren Bereich des Fensters siehst Du die Zertifikatsdetails des Schlüssels vom jeweils angeklickten Schlüssel. In diesem Bereich siehst Du ebenfalls den zugehörigen Fingerabdruck.

Über den Button „Beglaubigungen“ kannst Du sehen, wer diesem Schlüssel bereits sein Vertrauen zugesichert hat. Dein Vertrauen gegenüber einem Schlüssel kannst Du in der Schlüsselübersicht von Kleopatra festlegen: Klicke dazu per Rechtsklick auf einen Schlüssel und wähle den Eintrag „Beglaubigen...“.

Eigens erstellte Schlüssel haben standardmäßig ein „ultimatives“ Vertrauen. Importierte Schlüssel müssen dieses Vertrauen durch Dich erst erlangen. Wenn Du einen neuen Schlüssel in Kleopatra aufnehmen willst, solltest Du zuerst den Fingerabdruck des Schlüssels überprüfen. Erst nach Überprüfung legst Du Dein Vertrauen gegenüber dem Schüssel fest.

3.2.8 Einen neuen Schlüssel aufnehmen

Anna Fröhlich (Werkstudentin):

> „So Robin, wir haben im ersten Schritt Dein persönliches Schlüsselpaar erstellt. Wenn Du mir nun ein geheimes Dokument schicken willst, dann brauchst Du meinen öffentlichen Schlüssel. Ich zeige Dir mal, wie Du einen neuen öffentlichen Schlüssel aufnehmen kannst."

„Auf Server suchen"-Button in der Menüleiste

Um nun einen öffentlichen Schlüssel zu importieren, klicke in Kleopatra auf den „Auf Server suchen"-Button in der Menüleiste. Gebe im vorgesehenen Feld entweder den Namen, die E-Mail oder den Fingerabdruck Deines Kommunikationspartners ein.

Je präziser Deine Anfrage, desto weniger Schlüssel werden Dir zum Import angeboten. Wenn Du den Fingerabdruck Deines Gesprächspartners in das Suchfeld eingibst, solltest Du nur einen einzigen Schlüssel finden. Klicke diesen Schlüssel an und bestätige den Import mit „Importieren".

Versand der Datei

Wahlweise kann Dein Kommunikationspartner Dir den öffentlichen Schlüssel seines Schlüsselpaars auch als Datei zukommen lassen (z. B. per E-Mail), die Du dann über den „Importieren"-Button in der Menüleiste von Kleopatra importieren kannst.

Fortgeschrittene Nutzer können den öffentlichen Schlüssel des Kommunikationspartners auch über die Kommandozeile importieren.

3.2.9 Das Abschlussgespräch

Anna Fröhlich (Werkstudentin):

> „Toll Robin, wir haben es geschafft! Ich hoffe Du hast einiges dazu gelernt und hattest Spaß dabei. Morgen wird wieder ein aufregender Tag für Dich. Denn die Verschlüsselung ist nicht nur auf Dateien beschränkt.
>
> Aber für heute reicht es erstmal!"

Robin Schmidt (Praktikant):

> „Vielen Dank, Anna!

Mir hat der erste Praktikumstag richtig viel Spaß gemacht! Ich glaube ich kann bei der Securenet Consulting GmbH noch richtig viel lernen. Ich bin schon ganz gespannt auf morgen.

Oh, hallo Frau Jung!“

Frau Jung (Senior Consultant):

„Hallo ihr beiden! Wie ich sehe, versteht ihr zwei Euch. Ich habe bereits von Anna per E-Mail erfahren, dass sie Dir die Anwendung der Software Gpg4win nähergebracht hat. Hättest Du Lust auf einen kleinen Abschlusstest für heute? Ich würde gerne Deinen Lernerfolg sehen.“

3.3 Anwendung der Verschlüsselungs-Software GPG Suite (macOS)

3.3.1 Installation der Software GPG Suite

1. Lade auf der Web Site https://gpgtools.org die neuste Version von GPG Suite herunter.
2. Starte die Installation, indem Du die heruntergeladene .dmg-Datei doppelklickst. Folge dann der Installationsanweisung.
3. Nach erfolgter Installation kannst Du die .dmg-Installationsdatei in den Papierkorb legen. Durch diese Installation wurde auf Deinem Rechner das Programm GPG Keychain installiert.

Die GPG Suite enthält neben dem Programm GPG Keychain noch weitere Programme, die bei der Installation automatisch mitinstalliert werden:

- GPGMail ist eine Funktionserweiterung für Apple Mail
- MacGPG ist eine Anwendung für die Kommandozeile
- GPG Services ist ein Plugin, welches GPG Suite-Funktionalitäten in andere Anwendungen integriert

Die Funktionsweise und der genaue Nutzen richtet sich jedoch an fortgeschrittene Nutzer und wird in diesem WBT nicht weiter erläutert.

3.3.2 Die Werkstudentin Anna stellt sich vor

Frau Jung (Senior Consultant):

„So Robin, dann lass uns beide zu Deinem Arbeitsplatz gehen.

Oh halt, mein Chef ruft an!

Tut mir leid Robin, ich muss dringend los. Ich habe noch einen Termin mit dem Vorstand. Soweit haben wir alles Notwendige zum Verschlüsseln, zum Entschlüsseln und zum Signieren von Dateien auf Deinem Laptop installiert.

Da Du Dir dein Büro mit Anna unserer Werkstudentin teilen wirst, kannst Du Dir von ihr die Software erklären lassen. Bis später!“

Anna Fröhlich (Werkstudentin):

„Hallo Robin! Ich bin Anna, ebenfalls Studentin an der Justus-Liebig- Universität in Gießen. Ich erinnere mich an Dich. Wir haben zusammen das Modul Wirtschaftsinformatik besucht.

Vielleicht erinnerst Du Dich noch an das Verschlüsseln, Entschlüsseln und Signieren von Dateien mit asymmetrischen Verschlüsselungsverfahren. Dies übernimmt hier die installierte Software GPG Suite.

Bevor wir mit der Verschlüsselung starten, möchte ich Dir vorher noch kurz zeigen, wie Du ein Schlüsselpaar mit GPG Keychain erstellst. Denn das ist die Voraussetzung, um eine asymmetrische Verschlüsselung durchführen zu können. Könntest Du die Software starten?“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.3.3 Das Verschlüsseln einer Datei mit GPG Suite

Anna Fröhlich (Werkstudentin):

„So Robin, wir haben im ersten Schritt Dein persönliches Schlüsselpaar erstellt. Deinen öffentlichen Schlüssel kannst Du nun beliebig vielen Personen im Internet über Schlüssel-Listen mitteilen. Du kannst Deinen öffentlichen Schlüssel auch per E-Mail bestimmten Personen zukommen lassen.

Als Nächstes kannst Du Deinen öffentlichen Schlüssel nutzen, um eine beliebige Datei von Dir zu verschlüsseln. Natürlich kannst Du auch für jeden anderen Empfänger Dateien verschlüsseln, soweit Du deren öffentlichen Schlüssel besitzt.

Ich zeige Dir jetzt, wie ich eine Datei mit Deinem öffentlichen Schlüssel verschlüssele.

Schau genau zu!“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.3.4 Das Entschlüsseln einer Datei mit GPG Suite

Anna Fröhlich (Werkstudentin):

„Robin, wir haben nun eine Datei mit Deinem öffentlichen Schlüssel erfolgreich verschlüsselt.

Im nächsten Schritt kannst nur Du mit Deinem, im ersten Schritt, erstellten privaten Schlüssel die verschlüsselte Datei wieder entschlüsseln.

Und so könnte auch jede weitere beliebige Person Dir eine Datei zusenden, die mit Deinem öffentlichen Schlüssel verschlüsselt wurde. Diese kannst nur Du mit Deinem privaten Schlüssel wieder entschlüsseln.

Die Entschlüsselung funktioniert ähnlich wie die Verschlüsselung nur unter zusätzlicher Eingabe deines Passworts für den privaten Schlüssel. Dieses Passwort hast Du bei der Erstellung des Schlüsselpaars selbst festgelegt, um deinen privaten Schlüssel zu schützen. Also bist Du jetzt an der Reihe.

Lass und die Plätze tauschen!“

Robin Schmidt (Praktikant):

„Okay, los geht’s!“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.3.5 Das Signieren einer Datei mit GPG Suite

Robin Schmidt (Praktikant):

„Hm...jetzt habe ich aber doch eine Frage.

Wie kann ich sicherstellen, dass eine bestimmte Datei von Dir und niemand anderen stammt und nicht manipuliert wurde?“

Anna Fröhlich (Werkstudentin):

„Damit sichergestellt werden kann, dass eine bestimmte Datei von Dir und

niemand anderem stammt und nicht manipuliert wurde, solltest Du diese signieren.

Soll ich es Dir zeigen?“

Signaturen werden mit privaten Schlüsseln erstellt und beziehen sich z. B. auf Dateien. Du kannst jede Art von Dateien signieren, es muss nicht zwingend eine verschlüsselte Datei sein. So könntest Du Word-, PowerPoint-, PDF-, ZIP-, TXT-Dateien oder jede andere beliebige Datei signieren.

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

3.3.6 Die Gültigkeit und der Bezug von öffentliche Schlüsseln

Robin Schmidt (Praktikant):

„Super, vielen Dank Anna!

Das hat mir sehr weitergeholfen. Nun habe ich ein eigenes Schlüsselpaar. Aber das Verschlüsseln von Dateien mit dem eigenen öffentlichen Schlüssel ist nicht der Regelfall oder?

Wie ich sehe, ist es grundsätzlich jedem Nutzer möglich, Schlüsselpaare auf beliebige E-Mail-Adressen zu erstellen (Abb. 23). Es wird nicht sichergestellt, dass der Ersteller des Schlüsselpaares auch der Eigentümer der zugehörigen E-Mail-Adresse ist.“



Abb. 23: Beliebige E-Mail-Adressen von Robin

Anna Fröhlich (Werkstudentin):

„Genau! Daher ist es wichtig, dass Du im nächsten Schritt, nach Erstellung Deines Schlüsselpaares, die ‚richtigen‘ öffentlichen Schlüssel Deiner Empfänger in GPG Keychain importierst und verwendest.

Importierst Du den falschen öffentlichen Schlüssel und verschlüsselst damit eine Datei, kann der Empfänger diese nicht entschlüsseln. Zur Sicherstellung der Echtheit von Schlüsseln gibt es zwei Möglichkeiten in GPG Keychain:

1. Die flüchtige, nicht sichere Kontrolle: Schlüssel ID-Vergleich
2. Die sichere Kontrolle: Fingerabdruck-Vergleich“

Die Schlüssel-ID ist ein 32-Bit-Wert, welcher in hexadezimaler Darstellung bereitgestellt wird. Diese Schlüssel-ID sollte für jedes Schlüsselpaar eindeutig sein.

Im Jahr 2014 wurde jedoch das Gegenteil bewiesen. Eine Kontrolle ausschließlich auf Basis der Schlüssel-ID reicht daher nicht aus. Vielmehr muss auf die Kontrolle über Fingerabdrücke zurückgegriffen werden.

Hier siehst Du eine Beispiel-Schlüssel-ID: 99FE4EB7

3.3.7 Der Fingerabdruck-Vergleich

Der Fingerabdruck ist einzigartig und stellt eine Art Quersumme dar, welche aus dem Schlüsselpaar errechnet wurde. Dieser Fingerabdruck hat eine entsprechende Länge und passt weltweit nur auf ein einziges Schlüsselpaar.

A767 1A57 5F87 B31E 2C26 2265 857F C948 99FE 4EB7

In GPG Keychain können Sie sich per Doppelklick auf den entsprechenden Schlüssel oder über Rechtsklick auf den Schlüssel und dem Eintrag „Details“ die Details eines Schlüssels anzeigen lassen.

Auf der rechten Seite siehst Du das Detail-Fenster des Schlüssels. In diesem Bereich siehst Du ebenfalls die zugehörige Schlüssel-ID und den Fingerabdruck.

Im Dropdown-Feld „Vertrauen“ könntest Du Dein Vertrauen gegenüber diesem Schlüssel festlegen.

Eigens erstellte Schlüssel haben standardmäßig ein „absolutes“ Vertrauen. Importierte Schlüssel müssen dieses Vertrauen durch Dich erst erlangen. Wenn Du einen neuen Schlüssel in GPG Keychain aufnehmen willst, solltest Du daher zuerst den Fingerabdruck des Schlüssels überprüfen. Erst nach Überprüfung legest Du Dein Vertrauen gegenüber dem Schüssel fest.

3.3.8 Einen neuen Schlüssel aufnehmen

Anna Fröhlich (Werkstudentin):

> „So Robin, wir haben im ersten Schritt Dein persönliches Schlüsselpaar erstellt. Wenn Du mir nun ein geheimes Dokument schicken willst, dann brauchst Du meinen öffentlichen Schlüssel. Ich zeige Dir mal, wie Du einen neuen öffentlichen Schlüssel aufnehmen kannst."

„Schlüssel suchen"-Button in der Menüleiste

Um nun einen öffentlichen Schlüssel zu importieren, klicke in GPG Keychain auf den „Schlüssel suchen"-Button in der Menüleiste. Gebe im vorgesehenen Feld entweder den Namen, die E-Mail oder den Fingerabdruck Deines Kommunikationspartners ein. Je präziser Deine Anfrage, desto weniger Schlüssel werden Dir zum Import angeboten.

Wenn Du den Fingerabdruck Deines Kommunikationspartners in das Suchfeld eingibst, solltest Du nur einen einzigen Schlüssel finden. Markiere diesen Schlüssel per Checkbox am Anfang der Ergebniszeile und bestätige den Import mit „Schlüssel holen". Der importierte Schlüssel sollte nun in GPG Keychain auftauchen. Per Doppelklick auf diesen Schlüssel erhältst Du alle weiteren Details und könntest so noch einmal den Fingerabdruck überprüfen und anschließend Dein Vertrauen gegenüber dem Schlüssel anpassen.

Versand der Datei

Wahlweise kann Dein Kommunikationspartner Dir den öffentlichen Schlüssel seines Schlüsselpaars auch als Datei zukommen lassen (z. B. per E-Mail), die Du dann über den „Importieren"-Button in der Menüleiste von GPG Keychain importieren kannst.

Fortgeschrittene Nutzer können den öffentlichen Schlüssel des Kommunikationspartners auch über die Kommandozeile importieren.

3.3.9 Das Abschlussgespräch

Anna Fröhlich (Werkstudentin):

> „Toll Robin, wir haben es geschafft! Ich hoffe Du hast Einiges dazu gelernt und hattest Spaß dabei. Morgen wird wieder ein aufregender Tag für Dich. Denn die Verschlüsselung ist nicht nur auf Dateien beschränkt.

Aber für heute reicht es erstmal!“

Robin Schmidt (Praktikant):

„Vielen Dank, Anna!

Mir hat der erste Praktikumstag richtig viel Spaß gemacht! Ich glaube ich kann bei der Securenet Consulting GmbH noch richtig viel lernen. Ich bin schon ganz gespannt auf morgen.

Oh, hallo Frau Jung!“

Frau Jung (Senior Consultant):

„Hallo ihr beiden!

Wie ich sehe, versteht ihr zwei Euch. Ich habe bereits von Anna per E-Mail erfahren, dass sie Dir die Anwendung der Software GPG Suite nähergebracht hat. Hättest Du Lust auf einen kleinen Abschlusstest für heute?“

3.4 Abschlusstest – WBT 02

3.4.1 Abschlusstest

Bitte beantworten Sie die folgenden Fragen durch Ankreuzen der korrekten Antworten (Tab. 3). Bei einigen Fragen können auch mehrere Antworten richtig sein.

Nr.	Frage	Richtig	Falsch
1	Jeder, der Ihren öffentlichen Schlüssel kennt, kann für Sie Dateien verschlüsseln, die nur Sie entschlüsseln können.		
	Richtig		
	Falsch		
2	Signaturen werden mit privaten Schlüsseln erstellt.		
	Richtig		
	Falsch		
3	Zur Sicherstellung der Echtheit von Schlüsseln, stellt der Schlüssel-ID-Vergleich eine sichere Kontrolle dar.		
	Richtig		
	Falsch		

4	Der Fingerabdruck stellt eine Art Quersumme dar, welche aus dem Schlüsselpaar errechnet wird. Dieser Fingerabdruck hat eine entsprechende Länge und passt weltweit auf		
	nur einen einzigen öffentlichen Schlüssel.		
	nur einen einzigen privaten Schlüssel.		
	nur ein einziges Schlüsselpaar.		
5	Importieren Sie den falschen öffentlichen Schlüssel des Empfängers und verschlüsseln damit eine Datei, kann er diese trotzdem entschlüsseln.		
	Richtig		
	Falsch		

Tab. 3: Abschlusstest - WBT 02

4 Verschlüsseln, Entschlüsseln und Signieren von E-Mails

4.1 Der zweite Praktikumstag

4.1.1 Früh am Morgen

Frau Jung (Senior Consultant):

„Guten Morgen Robin, Du bist aber früh im Büro.
Ich würde sagen, wir holen uns erstmal einen Kaffee."

Robin Schmidt (Praktikant):

„Guten Morgen Frau Jung, schön Sie wieder zu sehen.
Oh ja, Kaffee klingt super!"

Frau Jung (Senior Consultant):

„Anna hat Dir gestern bereits die Installation und Anwendung der Verschlüsselungs-Software zur Verschlüsselung, Entschlüsselung und zum Signieren von Dateien gezeigt. Der Abschlusstest hat gezeigt, dass du das Thema verstanden hast.

Und das freut mich! Denn das ist unser Hauptgeschäft hier in der Securenet Consulting GmbH. Du solltest jedoch wissen, dass wir nicht nur Dateien schützen. Auch unser E-Mail-Verkehr erfolgt verschlüsselt und wird durch Signaturen geschützt. Wie die Verschlüsselung, Entschlüsselung und das Signieren von E-Mails funktioniert, erklärt Dir Anna später."

4.1.2 Team-Besprechung in der Securenet Consulting GmbH

Anna Fröhlich (Werkstudentin):

„Guten Morgen Frau Jung!
Guten Morgen Robin!"

Robin Schmidt (Praktikant):

„Guten Morgen Anna!"

Frau Jung (Senior Consultant):

„Guten Morgen Anna!
Ich habe Dir Deine Aufgaben heute früh schon gemailt."

Anna Fröhlich (Werkstudentin):

„Ah! Sehr schön, vielen Dank! Wie ich hier lese, arbeiten Robin und ich heute wieder zusammen. Ich werde schon mal in unser Büro gehen, ein paar Vorkehrungen treffen und dort auf Dich warten."

4.1.3 Hintergrund zur E-Mail-Verschlüsselung

Robin Schmidt (Praktikant):

„So, hier bin ich."

Anna Fröhlich (Werkstudentin):

„Sehr schön! Schau mal, ich möchte Dir etwas zeigen.

Wir schauen uns heute an, wie man E-Mails schützen kann. Ich werde Dir zeigen, wie wir E-Mails verschlüsseln, entschlüsseln und signieren. Das zugrundeliegende Prinzip, die asymmetrische Verschlüsselung, hast Du bereits am Beispiel von Dateien kennengelernt.

Genauso wie Dateien enthalten auch E-Mails vertrauliche Daten, die geschützt werden müssen. Daher schauen wir uns zunächst an, wie das Konzept der asymmetrischen E-Mail-Verschlüsselung funktioniert (Abb. 24). Alice und Bob kennst Du sicher noch aus unseren Anleitungen."

4.1.4 Das Prinzip der asymmetrischen E-Mail-Verschlüsselung

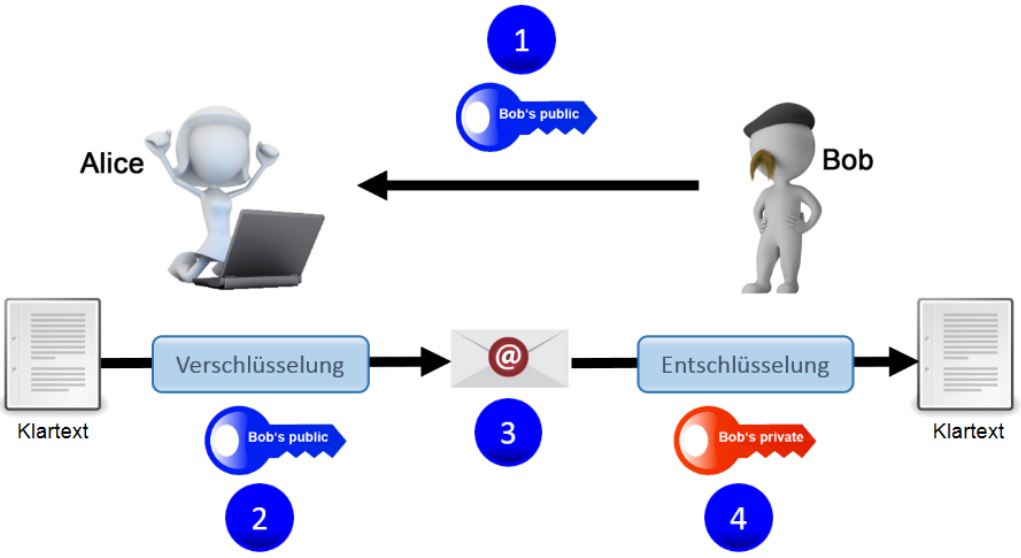


Abb. 24: Die asymmetrische E-Mail-Verschlüsselung

(1) Alice erhält den öffentlichen Schlüssel von Bob.

(2) Alice schreibt den Klartext ihrer E-Mail „Klartext“ und verschlüsselt sie mit dem öffentlichen Schlüssel von Bob.

(3) Alice schickt die E-Mail als Geheimtext an Bob. Wenn jemand unterwegs die E-Mail abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

(4) Nur Bob kann die E-Mail mit Geheimtext mit seinem privaten Schlüssel in Klartext umwandeln.

4.1.5 Auswahl Deines Betriebssystems

Anna Fröhlich (Werkstudentin):

„Wie Du Dich sicher erinnern kannst, ist die eingesetzte Verschlüsselungs-Software zum Schützen von Dateien abhängig vom verwendeten Betriebssystem. Auf Windows setzen wir Gpg4win und auf macOS die GPG Suite ein. Das gilt auch für die Verschlüsselung, Entschlüsselung und das Signieren von E-Mails.

Darf ich fragen, welches Betriebssystem Du auf Deinem Rechner verwendest?“

Robin Schmidt (Praktikant):

„Windows bzw. macOS.“

Hinweis: An dieser Stelle können Sie entscheiden, welches Betriebssystem Sie auf ihrem Rechner verwenden. Je nach Betriebssystem kommt für Sie folgendes Kapitel als nächstes in Frage: 4.2 Verschlüsseln, Entschlüsseln und Signieren von E-Mails mit Windows oder 4.3 Verschlüsseln, Entschlüsseln und Signieren von E-Mails mit macOS.

4.2 Verschlüsseln, Entschlüsseln und Signieren von E-Mails mit Windows

4.2.1 Die Vorbereitung

Anna Fröhlich (Werkstudentin):

„Bevor wir loslegen, hast Du noch Fragen?“

Robin Schmidt (Praktikant):

„Ja, ich habe mir eben bereits ein paar Fragen aufgeschrieben, bei welchen ich mir unsicher bin.“

1. Brauche ich ein Schlüsselpaar zur Verschlüsselung von E-Mails?

Anna Fröhlich (Werkstudentin):

„Du benötigst natürlich auch zum Verschlüsseln, Entschlüsseln und Signieren von E-Mails ein Schlüsselpaar, welches aus einem öffentlichen und privaten Schlüssel besteht. Dieses Schlüsselpaar haben wir bereits in ‚WBT 02 - Verschlüsseln, Entschlüsseln und Signieren von Dateien' mit Kleopatra erstellt."

2. Welche Schlüssel benötige ich?

Anna Fröhlich (Werkstudentin):

„Bevor wir mit der Verschlüsselung, Entschlüsselung und dem Signieren von E-Mails starten, ist es wichtig, dass Du alle notwendigen Schlüssel besitzt.

Zum Verschlüsseln einer E-Mail benötigst Du den öffentlichen Schlüssel des Empfängers. Das heißt, Du kannst Deinen öffentlichen Schlüssel beliebig vielen Personen mitteilen, damit diese Dir eine verschlüsselte E-Mail zukommen lassen können. Wie Du den öffentlichen Schlüssel einer anderen Person nutzen kannst, siehst Du in ‚WBT 02 – Verschlüsseln, Entschlüsseln und Signieren von Dateien'.

Zum Signieren Deiner Nachrichten und zum Entschlüsseln von Nachrichten an Dich benötigst Du Deinen privaten Schlüssel. Diesen musst Du geheim halten, damit nur Du Deine E-Mails signieren und entschlüsseln kannst."

3. Welche Verschlüsselungs-Software wird benötigt?

Anna Fröhlich (Werkstudentin):

„Wenn Du E-Mails unter Windows mit Outlook verschlüsseln, entschlüsseln und signieren willst, benötigst Du die Verschlüsselungs-Software Gpg4win und Outlook als E-Mail Client."

4. Welches Plugin ist notwendig?

Anna Fröhlich (Werkstudentin):

„Von den möglichen Plugins gibt es eine ganze Reihe, wie Du Dich sicher erinnerst. Das Outlook-Plugin GpgOL (Abb. 25) ist im Gpg4win-Paket enthalten und ermöglicht, E-Mails direkt in Microsoft Outlook zu verschlüsseln, zu entschlüsseln und zu signieren. Dabei werden auch Anhänge verschlüsselt.

GpgOL wurde bei der Installation von Gpg4win bereits automatisch in Deinem Outlook installiert.“

Abb. 25: Das Logo von GpgOL

4.2.2 Überprüfung des Outlook-Plugins

Anna Fröhlich (Werkstudentin):

„Das mitgelieferte Outlook-Plugin GpgOL ermöglicht es, E-Mails direkt in Microsoft Outlook zu verschlüsseln, zu entschlüsseln und zu signieren.

Das heißt, bevor wir damit loslegen können, müssen wir überprüfen, ob das Outlook-Plugin GpgOL erfolgreich in Outlook installiert wurde. Das kannst Du ganz einfach überprüfen, indem Du eine neue E-Mail in Outlook öffnest.“

Wenn das Symbol von GpgOL in Outlook zu sehen ist, dann war die Installation des Outlook-Plugins erfolgreich (Abb. 26).

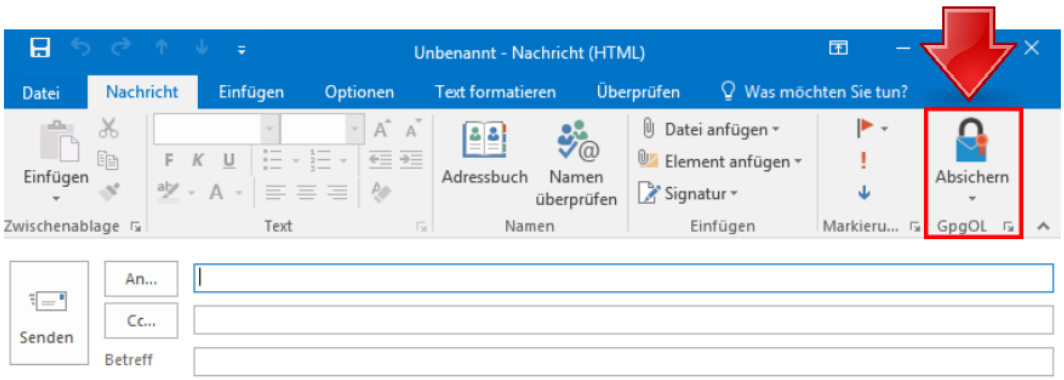


Abb. 26: Überprüfung des Outlook-Plugins GpgOL

4.2.3 Das Verschlüsseln und Signieren einer E-Mail mit Gpg4win

Anna Fröhlich (Werkstudentin):

„Das Verschlüsseln und Signieren einer E-Mail ist ganz einfach. Wir testen das Ganze mit unseren privaten E-Mail-Adressen, denn die geschäftliche ist bereits vollständig eingerichtet. Meinen öffentlichen Schlüssel hast Du ja bereits in Kleopatra aufgenommen. Also los geht's!"

Robin Schmidt (Praktikant):

„Alles klar, dann schicke ich Dir jetzt eine verschlüsselte und signierte E-Mail zu."

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

4.2.4 Das Entschlüsseln einer E-Mail mit Gpg4win

Robin Schmidt (Praktikant):

„Verschickt!"

Anna Fröhlich (Werkstudentin):

„Sehr gut Robin!
Ich habe Deine verschlüsselte E-Mail erhalten. Ich entschlüssle diese schnell und schicke Dir eine verschlüsselte E-Mail zurück. Dann bist Du mit der Entschlüsselung an der Reihe."

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

4.2.5 Das Abschlussgespräch

Frau Jung (Senior Consultant):

„Ja, bitte!"

Anna Fröhlich (Werkstudentin):

„Hallo Frau Jung, ich wollte Ihnen nur Bescheid geben, dass wir fertig sind. Wir haben uns heute erfolgreich die Verschlüsselung, Entschlüsselung und das Signieren von E-Mails angeschaut."

Frau Jung (Senior Consultant):

„Sehr schön, vielen Dank Anna!

Dann würde ich sagen, wir machen noch einen kleinen Abschlusstest. Danach bekommt ihr ein gemeinsames Projekt der Securenet Consulting GmbH zugewiesen. Robin, bist Du bereit für den Abschlusstest?“

4.3 Verschlüsseln, Entschlüsseln und Signieren von E-Mails mit macOS

4.3.1 Die Vorbereitung

Anna Fröhlich (Werkstudentin):

„Bevor wir loslegen, hast Du noch Fragen?“

Robin Schmidt (Praktikant):

„Ja, ich habe mir eben bereits ein paar Fragen aufgeschrieben, bei welchen ich mir unsicher bin.“

1. Brauche ich ein Schlüsselpaar zur Verschlüsselung von E-Mails?

Anna Fröhlich (Werkstudentin):

„Du benötigst natürlich auch zum Verschlüsseln, Entschlüsseln und Signieren von E-Mails ein Schlüsselpaar, welches aus einem öffentlichen und privaten Schlüssel besteht. Dieses Schlüsselpaar haben wir bereits in ‚WBT 02 - Verschlüsseln, Entschlüsseln und Signieren von Dateien‘ mit GPG Suite erstellt.“

2. Welche Schlüssel benötige ich?

Anna Fröhlich (Werkstudentin):

„Bevor wir mit der Verschlüsselung, Entschlüsselung und dem Signieren von E-Mails starten, ist es wichtig, dass Du alle notwendigen Schlüssel besitzt.

Zum Verschlüsseln einer E-Mail benötigst Du den öffentlichen Schlüssel des Empfängers. Das heißt, Du kannst Deinen öffentlichen Schlüssel beliebig vielen Personen mitteilen, damit diese Dir eine verschlüsselte E-Mail zukommen lassen können. Wie Du den öffentlichen Schlüssel einer anderen Person nutzen kannst, siehst Du in ‚WBT 02 Verschlüsseln, Entschlüsseln und Signieren von Dateien‘.

Zum Signieren Deiner Nachrichten und zum Entschlüsseln von Nachrichten an Dich, benötigst Du Deinen privaten Schlüssel. Diesen musst Du geheim halten, damit nur Du Deine E-Mails signieren und entschlüsseln kannst.“

3. Welche Verschlüsselungs-Software wird benötigt?

Anna Fröhlich (Werkstudentin):

„Wenn Du E-Mails unter macOS über Apple Mail verschlüsseln, entschlüsseln und signieren willst, benötigst Du die Verschlüsselungs-Software GPG Suite und Apple Mail als E-Mail Client."

4. Welches Plugin ist notwendig?

Anna Fröhlich (Werkstudentin):

„Von den möglichen Plugins gibt es eine ganze Reihe, wie Du Dich sicher erinnerst. Das Apple Mail-Plugin GPGMail (Abb. 27) ist im GPG Suite-Paket enthalten und ermöglicht, E-Mails direkt über Apple Mail zu verschlüsseln, zu entschlüsseln und zu signieren. Dabei werden auch Anhänge verschlüsselt.

GPGMail wurde bei der Installation von GPG Suite bereits automatisch in Apple Mail installiert."



Abb. 27: Das Logo von GPGMail

4.3.2 Überprüfung des Apple Mail-Plugins

Anna Fröhlich (Werkstudentin):

„Das mitgelieferte Apple Mail-Plugin GPGMail ermöglicht es, E-Mails direkt in Apple Mail zu verschlüsseln, zu entschlüsseln und zu signieren.

Das heißt, bevor wir damit loslegen können, müssen wir überprüfen, ob das Apple Mail-Plugin GPGMail erfolgreich in Apple Mail installiert wurde. Das kannst Du ganz einfach überprüfen, indem Du eine neue E-Mail in Apple Mail öffnest."

Wenn die Symbole von GPGMail in Apple Mail zu sehen sind, dann war die Installation des Apple Mail-Plugins erfolgreich (Abb. 28).

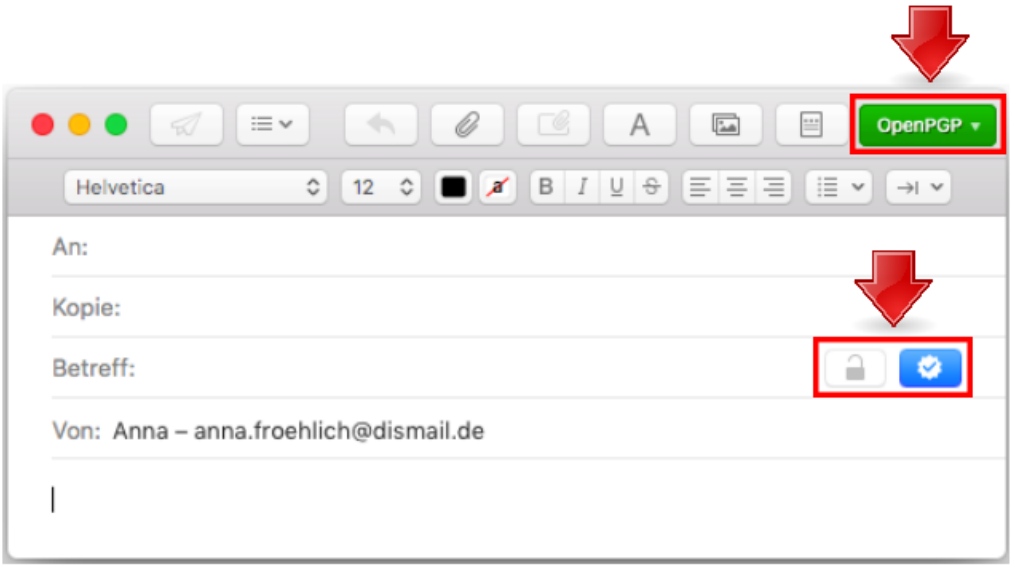


Abb. 28: Überprüfung des Apple Mail-Plugins GPGMail

4.3.3 Das Verschlüsseln und Signieren einer E-Mail mit GPG Suite

Anna Fröhlich (Werkstudentin):

„Das Verschlüsseln und Signieren einer E-Mail ist ganz einfach. Wir testen das Ganze mit unseren privaten E-Mail-Adressen, denn die geschäftliche ist bereits vollständig eingerichtet. Meinen öffentlichen Schlüssel hast Du ja bereits in GPG Suite aufgenommen. Also los geht's!"

Robin Schmidt (Praktikant):

„Alles klar, dann schicke ich Dir jetzt eine verschlüsselte und signierte E-Mail zu."

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

4.3.4 Das Entschlüsseln einer E-Mail mit GPG Suite

Robin Schmidt (Praktikant):

„Verschickt!"

Anna Fröhlich (Werkstudentin):

„Sehr gut Robin!

Ich habe Deine verschlüsselte E-Mail erhalten. Ich entschlüssle diese schnell und schicke Dir eine verschlüsselte E-Mail zurück. Dann bist Du mit der Entschlüsselung an der Reihe.“

Hinweis: An dieser Stelle wäre ein Video zur Veranschaulichung der Inhalte zu finden.

4.3.5 Das Abschlussgespräch

Frau Jung (Senior Consultant):

„Ja, bitte!“

Anna Fröhlich (Werkstudentin):

„Hallo Frau Jung, ich wollte Ihnen nur Bescheid geben, dass wir fertig sind. Wir haben uns heute erfolgreich die Verschlüsselung, Entschlüsselung und das Signieren von E-Mails angeschaut.“

Frau Jung (Senior Consultant):

„Sehr schön, vielen Dank Anna!

Dann würde ich sagen, wir machen noch einen kleinen Abschlusstest. Danach bekommt ihr ein gemeinsames Projekt der Securenet Consulting GmbH zugewiesen. Robin, bist Du bereit für den Abschlusstest?“

4.4 Abschlusstest – WBT 03

4.4.1 Abschlusstest

Bitte beantworten Sie die folgenden Fragen durch Ankreuzen der korrekten Antworten (Tab. 4). Bei einigen Fragen können auch mehrere Antworten richtig sein.

Nr.	Frage	Richtig	Falsch
1	Damit Sie ein E-Mail verschlüsselt versenden können, benötigen Sie		
	den öffentlichen Schlüssel des Empfängers.		
	den privaten Schlüssel des Empfängers.		
	Ihren eigenen öffentlichen Schlüssel.		

2	Um eine E-Mail in Outlook bzw. Apple Mail direkt verschlüsseln, entschlüsseln und signieren zu können, benötigt man ein zusätzliches Plugin der Verschlüsselungs-Software.		
	Richtig		
	Falsch		
3	Das notwendige Plugin zur Verschlüsselung, Entschlüsselung und zum Signieren von E-Mails muss manuell im E-Mail-Programm installiert werden.		
	Richtig		
	Falsch		
4	Für die Signatur einer E-Mail benötigen Sie		
	Ihren öffentlichen Schlüssel.		
	Ihren privaten Schlüssel.		
	den privaten Schlüssel des Empfängers.		
5	Eine verschlüsselte E-Mail können Sie nur mit Ihrem privaten Schlüssel entschlüsseln.		
	Richtig		
	Falsch		

Tab. 4: Abschlusstest - WBT 03

4.4.2 Drag-and-Drop-Test

Alice möchte Bob eine verschlüsselte Nachricht schicken. Bitte ordnen Sie die Schlüssel für eine asymmetrische E-Mail-Verschlüsselung richtig zu (Abb. 29).

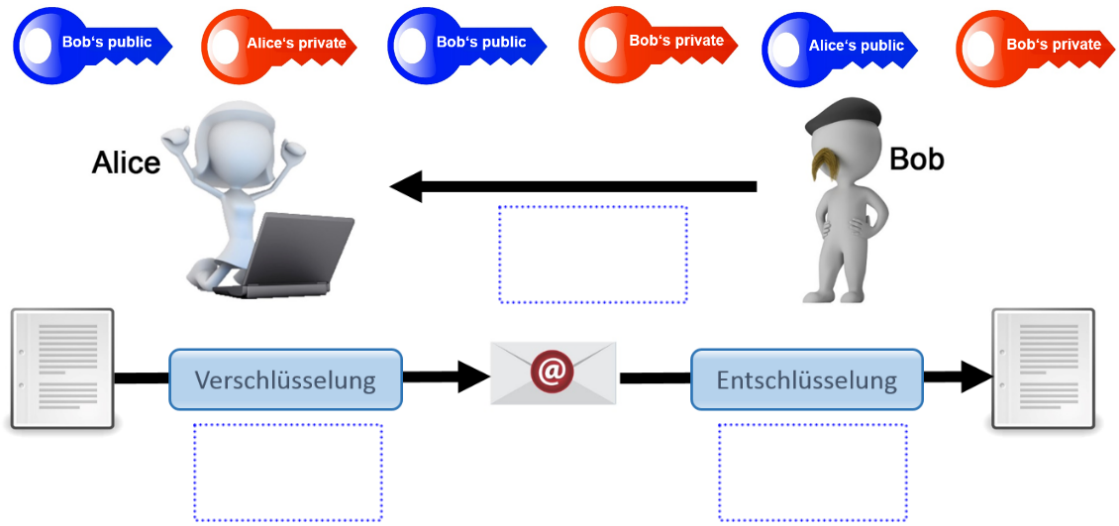


Abb. 29: Drag-and-Drop-Test - WBT 03

5 Anhang

Lösungen des Abschlusstests in WBT 01 (Tab. 5):

Nr.	Frage	Richtig	Falsch
1	Welche Verschlüsselungsverfahren werden unterschieden?		
	Vertikale Verschlüsselung		X
	Asymmetrische Verschlüsselung	X	
	Symmetrische Verschlüsselung	X	
	Horizontale Verschlüsselung		X
2	Verschlüsselung ist die Umwandlung von Informationen mit Hilfe bestimmter Verschlüsselungsverfahren, so dass unberechtigte Personen sie nicht lesen können.		
	Richtig	X	
	Falsch		X
3	Die symmetrische Verschlüsselung wird auch als „Public-Key-Verfahren“ bezeichnet.		
	Richtig		X
	Falsch	X	
4	Welche Schlüssel bilden bei asymmetrischen Verschlüsselungsverfahren ein Schlüsselpaar?		
	Öffentlicher Schlüssel	X	
	Geheimer Schlüssel		X
	Privater Schlüssel	X	
5	Beim der Verschlüsselung einer Datei mit dem asymmetrischen Verschlüsselungsverfahren erfolgt das Verschlüsseln mit dem privaten Schlüssel des Absenders und das Entschlüsseln mit dem öffentlichen Schlüssel des Empfängers.		
	Richtig		X
	Falsch	X	

6	Wozu dient der geheime Schlüssel in symmetrischen Verschlüsselungsverfahren?		
	zum Verschlüsseln	X	
	zum Entschlüsseln	X	
	nichts von beidem		X
7	Jeder, der Ihren öffentlichen Schlüssel kennt, kann für Sie Dateien verschlüsseln, die nur Sie mit Ihrem privaten Schlüssel entschlüsseln können.		
	Richtig	X	
	Falsch		X
8	Aus technischer Sicht besteht ein Schlüsselpaar in asymmetrischen Verschlüsselungsverfahren aus einer langen Zeichenabfolge, die als eigenständige Datei auf dem Rechner gespeichert wird.		
	Richtig		X
	Falsch	X	

Tab. 5: Lösungen Abschlusstests - WBT 01

Lösungen des Drag-and-Drop-Tests Teil 1 in WBT 01 (Abb. 30):

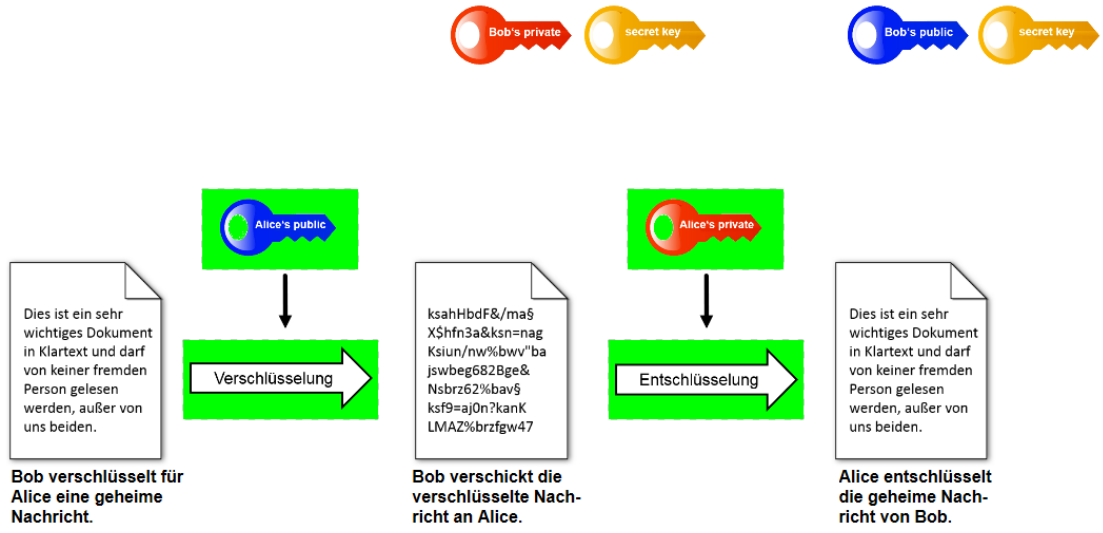


Abb. 30: Lösung Drag-and-Drop-Test - WBT 01 – Teil 1

Lösungen des Drag-and-Drop-Tests Teil 2 in WBT 01 (Abb. 31):

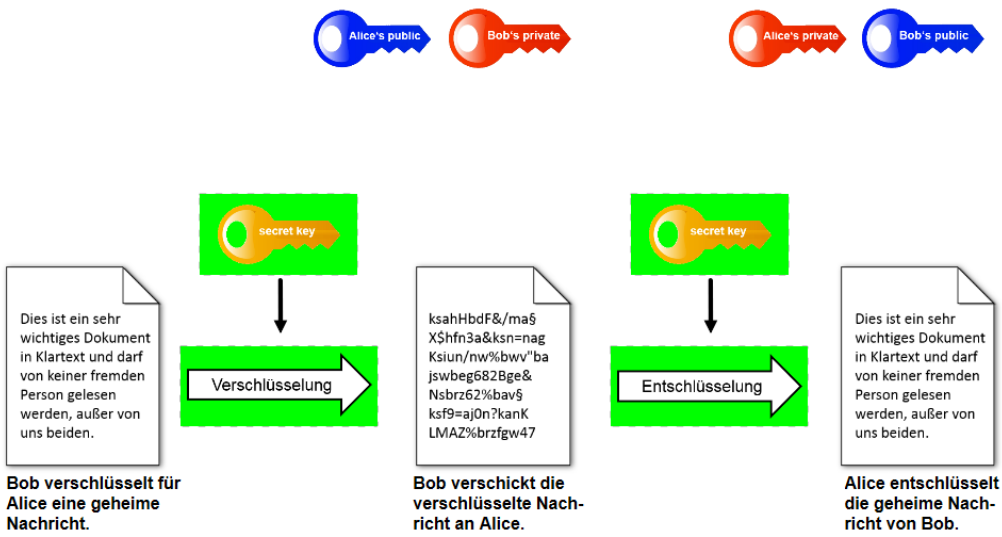


Abb. 31: Lösung Drag-and-Drop-Test - WBT 01 – Teil 2

Lösungen des Abschlusstests in WBT 02 (Tab. 6):

Nr.	Frage	Richtig	Falsch
1	Jeder, der Ihren öffentlichen Schlüssel kennt, kann für Sie Dateien verschlüsseln, die nur Sie entschlüsseln können.		
	Richtig	X	
	Falsch		X
2	Signaturen werden mit privaten Schlüsseln erstellt.		
	Richtig	X	
	Falsch		X
3	Zur Sicherstellung der Echtheit von Schlüsseln, stellt der Schlüssel-ID-Vergleich eine sichere Kontrolle dar.		
	Richtig		X
	Falsch	X	
4	Der Fingerabdruck stellt eine Art Quersumme dar, welche aus dem Schlüsselpaar errechnet wird. Dieser Fingerabdruck hat eine entsprechende Länge und passt weltweit auf		
	nur einen einzigen öffentlichen Schlüssel.		X
	nur einen einzigen privaten Schlüssel.		X

	nur ein einziges Schlüsselpaar.	X	
5	Importieren Sie den falschen öffentlichen Schlüssel des Empfängers und verschlüsseln damit eine Datei, kann er diese trotzdem entschlüsseln.		
	Richtig		X
	Falsch	X	

Tab. 6: Lösungen Abschlusstest - WBT 02

Lösungen des Abschlusstests in WBT 03 (Tab. 7):

Nr.	Frage	Richtig	Falsch
1	Damit Sie ein E-Mail verschlüsselt versenden können, benötigen Sie		
	den öffentlichen Schlüssel des Empfängers.	X	
	den privaten Schlüssel des Empfängers.		X
	Ihren eigenen öffentlichen Schlüssel.		X
2	Um eine E-Mail in Outlook bzw. Apple Mail direkt verschlüsseln, entschlüsseln und signieren zu können, benötigt man ein zusätzliches Plugin der Verschlüsselungs-Software.		
	Richtig	X	
	Falsch		X
3	Das notwendige Plugin zur Verschlüsselung, Entschlüsselung und zum Signieren von E-Mails muss manuell im E-Mail-Programm installiert werden.		
	Richtig		X
	Falsch	X	
4	Für die Signatur einer E-Mail benötigen Sie		
	Ihren öffentlichen Schlüssel.		X
	Ihren privaten Schlüssel.	X	
	den privaten Schlüssel des Empfängers.		X

5	Eine verschlüsselte E-Mail können Sie nur mit Ihrem privaten Schlüssel entschlüsseln.		
	Richtig	X	
	Falsch		X

Tab. 7: Lösungen Abschlusstest - WBT 03

Lösung des Drag-and-Drop-Test WBT 03 (Abb. 32):

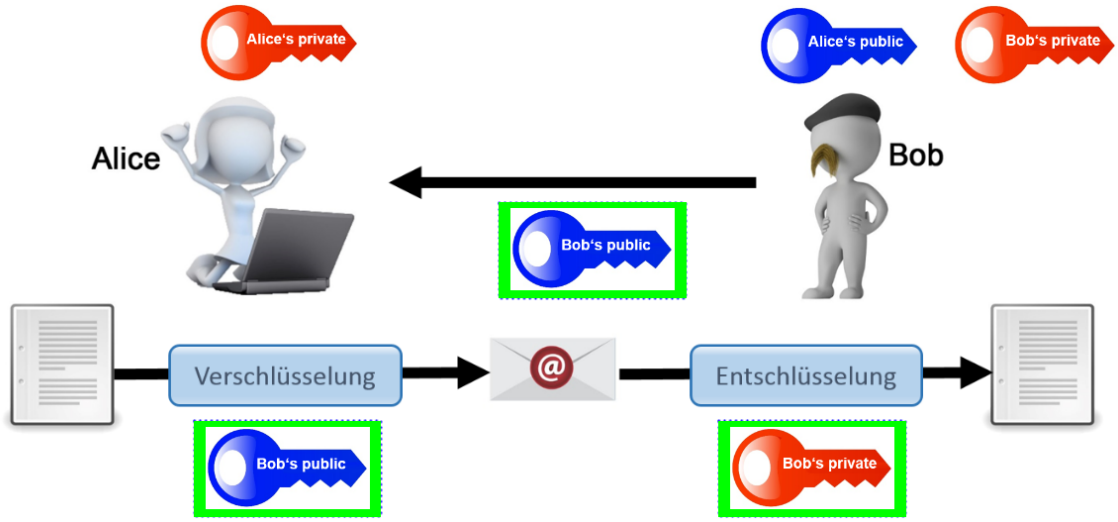


Abb. 32: Lösung Drag-and-Drop-Test - WBT 03

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse http://wi.uni-giessen.de/

Alle Arbeitspapiere der Reihe „Arbeitspapiere WI“ sind einschließlich aller Abbildungen urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Herausgebers unzulässig. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung, Be- und Verarbeitung in elektronischen Systemen. Copyright Professur BWL – Wirtschaftsinformatik