KRYPTOGRAFIE – INFORMATIK DES VERTRAUENS

ARBEITSBLÄTTER

mit Lösungen

INHALTSVERZEICHNIS

Hinweis: Die Lösungen können durch Bearbeiten der Formatvorlagen ausgeblendet werden:
Absatzvorlage ITG_Lösung – Schrifteffekt ‚ausgeblendet‘
Zeichenvorlage Lösung – Schriftfarbe weiß

Caesar-Chiffre

Informationen

Symmetrische Chiffren sind die ältesten kryptographischen Verfahren. Der Klartext wird mithilfe eines geheimen Schlüssels in einen Chiffretext übertragen.

Die wohl bekannteste Chiffre ist die **Caesar-Chiffre:**

Schlüssel: Abstand Klartextbuchstabe – Chiffrebuchstabe im Alphabet

Verschlüsseln: Jeden Buchstaben des Klartextes verschiebt man im Alphabet um den Schlüsselabstand; den resultierenden Buchstaben schreibt man in den Chiffretext:

Klartext-/	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtext-alphabet	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

Den Chiffriervorgang kann man z.B. so aufschreiben:

Klartext m	K R Y P T O G R A F I E
Schlüssel k	3
Chiffretext c	N U B S W R J U D I L H

Entschlüsseln: Der legitime Empfänger kennt den Schlüssel, macht die Verschiebung buchstabenweise rückgängig und erhält wieder den Klartext.

Links

INF-SCHULE.DE: ERKLÄRUNG UND AUFGABEN ZUM CAESAR-VERFAHREN
INF-SCHULE.DE: ANGRIFFE AUF VERSCHIEBEVERFAHREN
MATHEPRISMA: CAESAR-VERFAHREN

Videos

SPANNAGEL, CHRISTIAN: CAESAR-VERSCHLÜSSELUNG. (15MIN)
KRYPTO IM ADVENT: CAESAR-VERSCHLÜSSELUNG. (4MIN)

Aufgaben

1. Schickt euch zu zweit Nachrichten mit der Caesar-Chiffre.
2. Tauscht eure Chiffretexte (ohne Schlüsselangabe!) mit einem anderen Team aus und versucht, den Klartext zu ermitteln. Wie seid ihr vorgegangen? Schreibt eine Anleitung zum Brechen der Caesar-Chiffre in Stichpunkten auf und testet sie an zwei weiteren Chiffretexten aus dem Kurs.
3. Ihr fangt folgende Nachrichten ab - Wie ist der Schlüssel? Wie lautet die Nachricht?
   Caesar-verschlüsselte Nachricht auf Deutsch:
   RKVVYSXPYBWKDSUOB
   Caesar-verschlüsselte Nachricht auf Englisch:
   VDDSBDGCXCVPCSRDCVGPIJAPIXDCHNDJQGDZTIWTRXEWTG

Der deutsche Klartext lautet: halloinformatiker
Wer den Doppelbuchstabe an Stelle 3+4 bemerkt, kann HALLO raten und beim Angriff viel Zeit sparen.
Der engliche Klartext lautet: goodmorningandcongratulationsyoubrokethecipher

Vordruck zum Bau einer Caesar-Krone.

Klartextalphabet									Klartextalphabet									Klartextalphabet								
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z			

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z			
Geheimtextalphabet									Geheimtextalphabet									Geheimtextalphabet								

1. Basteln: Oben entlang der fett gedruckten Linien ausschneiden. Dann erst den Klartextstreifen zu einem Ring kleben, so dass Z neben A liegt. Dann auch den Geheimtextstreifen zu einem Ring kleben (aber so, dass er noch auf den Klartextring draufpasst!).

2. Schlüssel einstellen: Zwei Partner vereinbaren einen Buchstaben als gemeinsames Geheimnis (den nennt man dann ihren „Schlüssel“) und stellen die Krone so ein, dass der Schlüsselbuchstabe unter dem Klartext-A steht. Den Schlüssel darf sonst niemand wissen!

Beispiel: Für den Schlüssel „D“ drehen beide den unteren Ring so, dass das Geheimtext-D unter dem Klartext-A steht.

3. Verschlüsseln (Chiffrieren): Der Absender schreibt seine Nachricht im Klartext auf. Dann verschlüsselt er jeden einzelnen Buchstaben, indem er ihn an der Krone von oben nach unten abliest. Beispiel: Mit Schlüssel „D“ wird aus „HALLO“ der Geheimtext „KDOOR“.

4. Entschlüsseln (Dechiffrieren): Der Empfänger entschlüsselt, indem er wieder buchstabenweise abliest, aber jetzt von unten nach oben.

5. Angriff: Wer die Botschaft abfängt, kann versuchen sie zu brechen.Das heißt den verwendeten Schlüssel herauszufinden und damit die Nachricht zu lesen. Wie könnte man das machen?

Substitutionschiffre

Information

Die Verwendung dieser Chiffre wird Karl dem Großen und Hildegard von Bingen nachgesagt. Sie schließt einen brute-force-Angriff wie auf die Caesar-Chiffre aus und stellt damit die nächste Stufe in der Entwicklung der Kryptografie dar.

Schlüssel: Das Alphabet wird nicht mehr rotiert, sondern „verwürfelt“. Jedem Buchstaben des Alphabets wird ein anderer Buchstabe zugeordnet; diese Zuordnung haben Absender und Empfänger vorher vereinbart und halten sie geheim.

Verschlüsseln: Jeder Buchstaben des Klartextes wird in der Chiffre durch den zugehörigen Geheimtextbuchstaben ersetzt.

Klartext-/	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtext-Alphabet	B	L	I	E	S	P	U	N	Z	O	W	Q	R	A	G	Y	X	V	C	T	F	D	K	J	H	M

Die obere Zeile lautet natürlich immer gleich und ist damit nicht geheim. Der Schlüssel besteht also aus der zweiten Zeile dieser Tabelle.

Den Chiffriervorgang kann man z.B. so aufschreiben:

Klartext m	K R Y P T O G R A F I E
Schlüssel k	(s.o.)
Chiffretext c	W V H Y T G U V B P Z S

Entschlüsseln: Der legitime Empfänger kennt den Schlüssel, macht die Zuordnung buchstabenweise rückgängig und erhält wieder den Klartext.

Links

UNIVERSITÄT TÜBINGEN: SUBSTITUTIONS-CHIFFRE.

Aufgaben

4. Vereinbare mit deinem Nachbarn einen Schlüssel für diese Chiffre, verschlüssele eine kurze Nachricht für ihn, tauscht die Geheimtexte aus und entschlüsselt sie.
5. Widersteht diese Chiffre jetzt einem brute-force-Angriff? Es sollen alle hier möglichen Schlüssel durchprobiert werden. Wie viele denkbare Schlüssel hat die Substitution?

Antwort: Der Schlüssel ist eine Permutation des Alphabets, es gibt also $26! \approx 4 \cdot 10^{26}$ *verschiedene Schlüssel. Ausführlicher: Für den Schlüsselbuchstaben unter A gibt es 26 Möglichkeiten, für den unter B nur noch 25 usw. Insgesamt gibt es also* $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 2 \cdot 1 = 26!$ *verschiedene Schlüssel.*

6. Ist 26! genug?

→ *Skript*

7. Informiere dich über Häufigkeitsanalyse als Verfahren in der Kryptografie. Dokumentiere deine Quellen und führe das Verfahren an einem Beispiel durch.

Vigenère

Informationen

Um die einfache Häufigkeitsanalyse abzuwehren, entstanden polyalphabetische Systeme wie die Vigenère-Chiffre – sie galt sogar 300 Jahre lang als unangreifbar. Hier verwendet man für aufeinanderfolgende Buchstaben jeweils verschiedene Alphabete, so dass sich die Häufigkeiten der Buchstaben im Geheimtext weitgehend nivellieren.

Schlüssel: Man wählt ein Schlüsselwort k, z.B. k=TOM

Verschlüsseln: Man schreibt das Schlüsselwort wiederholend unter den Klartext:

Klartext m	A	U	S	K	L	A	R	T	E	X	T	W	I	R	D	C	H	I	F	F	R	E	T	E	X	T
Schlüssel k	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O

Nun wird das erste A mit dem Schlüsselalphabet T verschlüsselt (also wie mit einem Caesar-Ring in der Stellung „T unter A“). Das U wird mit dem Alphabet O, das S mit T und das K wieder mit T verschlüsselt.

Geheimtext c	T	I	E	D	Z	M	K	H	Q	Q	H	I	B	F	P	V	V	U	Y	T	D	X	H	Q	Q	H

Entschlüsseln: Man schreibt den Schlüssel unter den Geheimtext und verfolgt die Buchstaben zurück: Er findet dabei (was vielen Schülern nicht gleich klar ist) den Geheimtextbuchstaben im Inneren der Tabelle, den Schlüssel auf der einen und den Klartext auf der anderen Achse.

Geheimtext c	T	I	E	D	Z	M	K	H	Q	Q	H	I	B	F	P	V	V	U	Y	T	D	X	H	Q	Q	H
Schlüssel k	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O
Klartext m	A	U	S	K	L	A	R	T	E	X	T	W	I	R	D	C	H	I	F	F	R	E	T	E	X	T

Links

Inf-Schule.de: Chiffrierung mit dem Vigenère-Verfahren.
Wikipedia: Vigenère-Verschlüsselung.
Universität Tübingen: Vigenère-Chiffre.

Videos:

Krypto im Advent: Vigenère Verschlüsselung. (4min)
s41b0tproductions: Kryptologie - Vigenere Code (6min)

Aufgaben

8. Vereinbare mit deinem Nachbarn ein Schlüsselwort. Jeder chiffriert einen kurzen Text (wenige Wörter), ihr tauscht die Geheimtexte aus und jeder dechiffriert die Nachricht des anderen.
9. Vigenère soll nun angegriffen werden. Wir nehmen der Einfachheit halber an, die Schlüssellänge sei bekannt: L=3. Wie attackierst du den Geheimtext c= VRUJEGXEAVNGVBXEDXISILR?

Antwort: Bei Schlüssellänge 3 ist jeder dritte Buchstabe mit demselben Schlüsselbuchstaben verschlüsselt. Daher ist der Angriff identisch mit Caesar – nur auf die Buchstaben 1,4,7,... / 2,5,8,... / 3,6,9,... Dies führt über die Häufigkeitsanalyse zum Schlüssel RAT, der Klartext ERBSENGEHENNEBENDERSPUR.

Arbeitshilfe: Vigenère-Quadrat

(Lautebach)

Klartextbuchstaben in dieser Zeile suchen --->

Schlüsselbuchstaben in dieser Spalte suchen --->

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		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
0	A	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
1	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	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
4	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

↑ Chiffretextbuchstaben im Inneren der Tabelle suchen ↑

Angriffe auf Vigenère

Kasiski-Test zur Bestimmung der Schlüssellänge

Im obigen Geheimtext fällt bei genauem Hinsehen die Folge HQQH auf:

Geheimtext c	T	I	E	D	Z	M	K	H	Q	Q	H	I	B	F	P	V	V	U	Y	T	D	X	H	Q	Q	H
Startposition								8															23			

Auch ohne Kenntnis des Klartextes liegt die Vermutung nahe, dass hier das gleiche Textfragment mehrfach verschlüsselt wurde, und zwar beide Male mit dem gleichen Teil des Schlüssels.

Abstand $23-8=15=3\cdot 5$ → L=3 oder L=5 oder L=15. Dann kann der obige Angriff wieder mit diesen Schlüssellängen erfolgen.

Autokorrelation

Die Vigenère-Chiffre ebnet zwar die Häufigkeitsunterschiede *zwischen* den Gruppen ein, aber *innerhalb* einer Gruppe sind immer die gleichen Buchstaben häufig (bzw. selten). Das nutzt man aus, indem man den Geheimtext buchstabenweise verschiebt und seine Übereinstimmungen mit sich selber zählt. Wenn nach der richtigen Verschiebung (nämlich um genau eine Schlüssellänge) alle Buchstaben wieder mit denen ihrer eigenen Gruppe zusammentreffen, fällt das bei der Zählung sofort auf:

↓ Verschiebungsweite																	Anzahl der Übereinstimmungen ↓
0	**W**	**E**	**K**	**Z**	**E**	**G**	**S**	**E**	**K**	**V**	**I**	**M**	**V**	**N**	**X**	**I**	**H**	**X**	**S**	**L**	**B**	**T**	**H**	**X**	**W**	**R**	**X**	**L**	**D**	**X**					
1		W	E	K	Z	E	G	S	E	K	V	I	M	V	N	X	I	H	X	S	L	B	T	H	X	W	R	X	L	D	X				0
2			W	E	K	Z	E	G	S	E	K	V	I	M	V	N	X	I	H	X	S	L	B	T	H	X	W	R	X	L	D	X			0
3				W	**E**	K	Z	**E**	G	S	E	K	**V**	I	M	V	N	**X**	I	H	X	S	L	B	T	H	**X**	W	R	**X**	L	D	X			6
4					W	E	K	Z	E	G	S	E	K	V	I	M	V	N	X	I	H	X	S	L	B	T	H	X	W	R	X	L	D	X		0

Partieller Brute-Force Angriff

Da Vigenere bei bekannter Schlüssellänge so einfach zu brechen ist, kann man den Angriff auch einfach mit *allen* möglichen Schlüssellängen durchführen. Sobald man die richtige Länge rät, fällt das anhand der statistischen Eigenschaften der Buchstabengruppen sofort auf. Auch dieser Angriff ist leicht zu automatisieren.

Links

CRYPTOOL ONLINE: AUTOKORRELATION.
WIKIPEDIA: KASISKI-TEST.

Videos

SEIDEL, MICHAEL: VIGENÈRE UND KASISKI. (6MIN)

Aufgaben

10. Ermittle bei bekannter Schlüssellänge mittels Häufigkeitsanalyse Schlüsselwort und Klartext.

Klartext: Erbsengehennebenderspur   Schlüsselwort: RAT

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Vigenère mit Schlüssellänge 3

VRUJEGXEAVNGVBXEDXISILR

Aufgaben

11. Schneide die Streifen entlang der Unterstreichung aus, lege sie paarweise verschoben untereinander und zähle für jede Verschiebung die Übereinstimmungen.

Klartext: „wielautetderkuerzesteinformatikerwitzantwortsodasmuesstedannjetztfunktionieren“ *Schlüssel: „vier“*

RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQIIZV

RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQIIZV

RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQIIZV

RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQIIZV

RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQIIZV

RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQIIZV

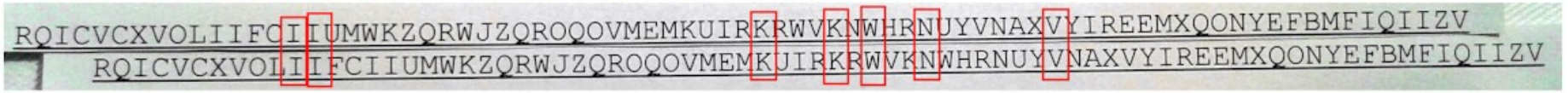
Musterlösung zu Aufgabe 11.
Die Streifen ausschneiden lassen (2 je Schüler) und untereinander legen. Die Häufigkeiten übereinstimmender Zeichen sind signifikant bei Vielfachen der Schlüssellänge.

Verschiebung um 1 Stelle

Verschiebung um 2 Stellen

Verschiebung um 3 Stellen

Verschiebung um 4 Stellen -> Auffallend viele Überreinstimmungen



Aufgaben

12. Schneide die Streifen entlang der Unterstreichung aus, lege sie paarweise verschoben untereinander und zähle für jede Verschiebung die Übereinstimmungen.
13. Suche Digramme im Chiffretext und ermittle die Schlüssellänge aus deren Abständen.

Teil 1

MVSFMVXSVQJFPNJBLYJFIHXZMRIGLRWAIPMHMFNQPRNBMATHMRIGQFYRIFKSVF

Teil 2

YSZANQPGIWKUYIVQFBLEJFARNHAANQPGIWMGZSZRLSAPMZWFXSVQFBVMJSPQX

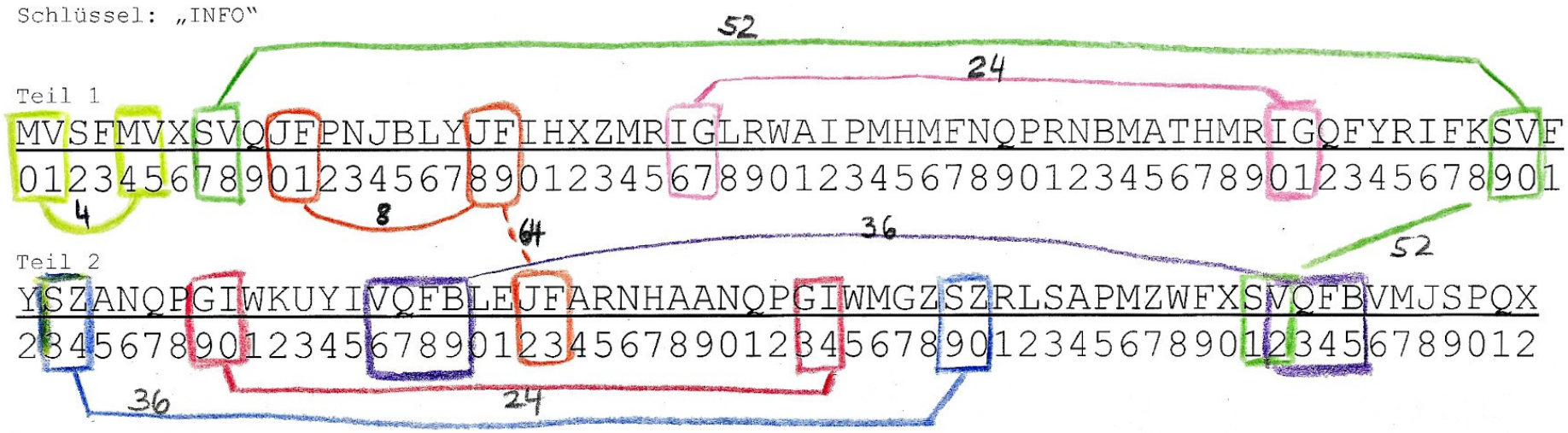
Teil 1

MVSFMVXSVQJFPNJBLYJFIHXZMRIGLRWAIPMHMFNQPRNBMATHMRIGQFYRIFKSVF

Teil 2

YSZANQPGIWKUYIVQFBLEJFARNHAANQPGIWMGZSZRLSAPMZWFXSVQFBVMJSPQX

Musterlösung für Kasiski-Angriff zu Aufgabe Fehler: Verweis nicht gefunden. Für eine bessere Übersicht unbedingt mit Farbstiften machen lassen.
Die Abstände zwischen den Digrammen weisen auf Schlüssellänge 4 hin, es gibt sogar ein 4-Gramm.



Aufgaben

14. Schneide die Streifen entlang der Unterstreichung aus, lege sie paarweise und verschoben untereinander und zähle für jede Verschiebung die Übereinstimmungen.

Trotz der vielen „E“ ist ein Schlüsselbuchstabe nicht gleich eindeutig. Dennoch relativ leicht.

Lösung für den Lehrer: Klartext: „ferienbereitenerheblichefreude“ Schlüssel: „RAT“
Cryptool liefert bei der Analyse SAT als Schlüssel und damit dann einen Buchstabensalat als entschlüsselte Nachricht. Die Schüler schließen daraus schnell, dass das Beispiel ‚falsch‘ sei. An diesem Punkt kann sehr gut gezeigt werden, dass eine naive Anwendung eines Algorithmus nicht immer zu einem Ergebnis führt – hier ist die zweit wahrscheinlichste Lösung die passende.

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

WEKZEGSEKVIMVNXIHXSLBTHXWRXLDX

One Time Pad

Information

Schlüsselerzeugung: Der Schlüssel muss

1. absolut zufällig gewählt werden,
2. mindestens so lang sein wie die Nachricht
3. natürlich geheim bleiben
4. darf nur ein einziges Mal verwendet werden.

Schlüssel k	F	K	H	M	F	Q	Z	D	G	R
Nachricht m	B	I	L	D	U	N	G			
Chiffretext c	G	S	S	P	Z	D	F			

Verschlüsseln: Genau wie bei Vigenère schreibt man Schlüssel und Klartext untereinander und benutzt die Vigenère-Tabelle, d.h. man ermittelt wieder $c = m \oplus k$.

Den nicht benutzten Teil des Schlüssels kann man für die nächste Nachricht aufheben oder wegwerfen. Den verwendeten Teil *muss* man wegwerfen.

Entschlüsseln: Genau wie bei Vigenère schreibt man Schlüssel und Geheimtext untereinander und benutzt die Vigenère-Tabelle.

Links

INF-SCHULE.DE: ONE-TIME-PAD.
WIKIPEDIA: ONE-TIME-PAD.

Videos

KHAN ACADEMY: ONE-TIME-PAD. (3MIN)

Aufgaben

1. Erzeuge mit deinem Nachbarn zwei OTP-Schlüsselfolgen mit jeweils zehn Buchstaben Länge. Warum müssen es zwei sein?

Antwort: Man braucht zwei, damit beide dem anderen eine Nachricht schicken können. Jeder Schlüsselabschnitt darf ja nur ein einziges Mal verwendet werden.

2. Muss man a) mit, oder b) ohne Zurücklegen ziehen, oder c) ist das egal?

*Antwort: Man **muss** mit Zurücklegen ziehen. Sonst entsteht eine Beziehung zwischen den Buchstaben des Schlüssels, und damit wäre er nicht mehr zufällig.*

3. Chiffriert beide eine Nachricht, tauscht sie aus und entschlüsselt sie gegenseitig.
4. Warum ist OTP nun perfekt sicher?

Antwort: Auch mit dem Wissen c=GSSPZDF kann Eve keinen einzigen (siebenbuchstabigen) Klartext ausschließen. Anders gesagt: Sie kann zu jedem hypothetischen Klartext m' auch einen Schlüssel k' angeben, der aus diesem m den Chiffretext c=GSSPZDF gemacht hätte (nämlich $k' = c \ominus m'$; hier macht sich die algebraische Schreibweise bezahlt), und dieses k' ist genauso wahrscheinlich wie alle anderen auch. Sie muss also alle m' nach wie vor in Betracht ziehen. Eve erfährt daher nichts Neues über m (was sie nicht auch schon vor dem Abfangen der Nachricht wusste).

5. Wir unterstellen beliebig hohe Rechenleistung – wie würde man OTP mit brute force angreifen?

Antwort: Auch das bringt nichts. Brute force liefert eine Liste aller Klartexte (mit passender Länge) – und kein einziger sticht irgendwie heraus. Man hat nichts gewonnen. Es gibt eben keine Angriffe auf OTP, nicht heute und nicht morgen. Sie können auch nicht erfunden werden. Weder schnellere Maschinen noch Quantencomputer können OTP angreifen. Wenn die Information im Chiffretext gar nicht drinsteckt – dann kann auch kein Verfahren sie herausholen.

6. OTP ist perfekt sicher. Prima! Dann waren ja alle kryptografischen Probleme schon 1880

gelöst. Aber woran arbeiten Kryptografen dann überhaupt?

Antwort: OTP ist zwar sehr einfach und sehr sicher, wirft aber in der praktischen Anwendung massive Probleme auf. → Schlüsselverwaltung → Schlüsselaustausch

7. Überlege dir (in groben Zügen) einen Angriff auf OTP, wenn der Schlüssel kürzer ist als die Nachricht und deshalb innerhalb der Nachricht wiederholt wird.

Antwort: Dann handelt es sich nur noch um eine Vigenere-Chiffre.

8. Überlege dir (in groben Zügen) einen Angriff auf OTP, wenn der Schlüssel nicht absolut zufällig, sondern ohne Zurücklegen gezogen wird (und man nach 26 Buchstaben alle wieder in die Tüte wirft).

Antwort: Dann sind die Schlüsselbuchstaben innerhalb des ersten 26er-Blocks alle verschieden (die im zweiten auch usw.). Wenn innerhalb eines Blockes zwei gleiche Chiffretextbuchstaben auftreten, weiß man also, dass sie verschiedene Klartextbuchstaben repräsentieren müssen. Das erlaubt Rückschlüsse auf den Klartext.

9. Überlege dir (in groben Zügen) einen Angriff auf OTP, wenn der Schlüssel nicht zufällig ist, sondern aus einem deutschen Text besteht.

Beispiel:
> Key: `DIESISTDERSCHLUESSELUNDSEHRSCHWERZURATEN`

> Message: GEHEIMBLEIBTGEHEIMDARFNIEMANDERFAHREN

> Chiffrat: `GQIKQKMGIIKEOWOIKKIWOAGKIOIKEOSIIYOIAMIA`

Antwort: Man subtrahiert von jeder Stelle des Chiffretextes Wörter, die im Klartext und/oder Schlüssel wahrscheinlich vorkommen (zur Not nimmt man einfach UND, DIE oder DER) und sucht in der Differenz nach sinnvollen Buchstabenfolgen. Wer oft Kreuzworträtsel löst, erweitert die Fundstellen leicht nach links und rechts.

Vgl. Calc-Sheet Angriff_OTP1.ods

10. Überlege dir (in groben Zügen) einen Angriff auf OTP, wenn der Schlüssel bei vielen Nachrichten wiederverwendet wird.

Antwort: Bei allen Nachrichten haben dann die ersten Buchstaben den gleichen Schlüssel-buchstaben, die zweiten untereinander auch usw. Wie bei Vigenere greift man diese Gruppen einzeln an.

11. Überlege dir (in groben Zügen) einen Angriff auf OTP, wenn der Schlüssel bei einer zweiten Nachricht nochmals, danach aber nie wieder verwendet wird.

Antwort: Die Chiffretexte sind $c_1 = m_1 \oplus k$ *und* $c_2 = m_2 \oplus k$ *. Eve berechnet deren Differenz* $c_1 \ominus c_2 = (m_1 \oplus k) \ominus (m_2 \oplus k) = m_1 \oplus k \ominus m_2 \ominus k = m_1 \ominus m_2$ *. Das ist aber nur die Differenz der Klartexte: Sie hängt vom Schlüssel gar nicht mehr ab. Man kann sie wieder mit der Methode des wahrscheinlichen Wortes angreifen (nur muss man es jetzt überall addieren).*

Vgl. Calc-Sheet Angriff_OTP2.ods

Homophone Chiffren

Information

Die *homophone Chiffre* gilt als monoalphabetische Chiffre auf der Basis von Buchstabensubstitution. Der Unterschied zu anderen monoalphabetischen Chiffren besteht darin, dass die charakterischen Häufigkeiten der Buchstaben in Texten verschleiert werden. Dies wird erreicht, indem für die häufigeren Buchstaben mehrere Ersetzungszeichen zur Verfügung stehen.

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
88	42	60	87	32	76	94	21	57	20	29	38	65	01	82	9	18	27	90	53	07	43	52	61	70	79
97	51	69	96	41	85	03	30	66			47	74	10	91			36	99	62	16					
06		78	05	50		12	39	75			56	83	19	00			45	08	71	25					
15			14	59			48	84				92	28				54	17	80	34					
24			23	68				93					37				63	26	89						
33				77				02					46				72	35	98						
				86				11					55				81	44							
				95									64												
				04									73												
				13																					
				22																					
				31																					
				40																					
				49																					
				58																					
				67																					

Abbildung 1: Codierung der Zeichen bei Homophoner Chiffre.
Quelle: https://www.kryptographiespielplatz.de abgerufen November 2016

Die Anzahl der je Buchstabe verfügbaren Ersetzungszeichen orientiert sich grob an der Häufigkeit des zu ersetzenden Buchstaben. Als Ersetzungszeichen lassen sich beliebige Zeichen verwenden.

Links

CRYPTOOL: HOMOPHONE CHIFFRE.

Aufgaben

12. Chiffriere eine Nachricht mit der homophonen Chiffre nach obiger Tabelle.
13. Erstelle ein Calc-Sheet, das die homophone Chiffre umsetzt.

Asymmetrische Chiffren

Information

Alle bisher besprochenen Chiffren sind symmetrisch in dem Sinne, dass Alice und Bob im Besitz des gleichen Geheimnisses (eben ihres gemeinsamen Schlüssels) sein müssen. Letztlich ist es diese Symmetrie, die erhebliche Probleme verursacht: der Schlüssel muss auf einem sicheren Kanal ausgetauscht werden, bevor eine verschlüsselte Kommunikation möglich ist.

Ein asymmetrisches Kryptosystem arbeitet ohne diesen gemeinsamen geheimen Schlüssel. Ein Benutzer erzeugt hier ein Schlüsselpaar, das aus zwei Teilen besteht: einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Mit dem öffentlichen Schlüssel ist eine Entschlüsselung der Daten nicht mehr möglich! [nach Wikipedia: RSA]

Links

INF-SCHULE.DE: ASYMMETRISCHE VERFAHREN – EINFÜHRUNG.
GRAMM, ANDREAS: VERTRAULICHKEIT DURCH ASYMMETRISCHE KRYPTOLOGIE

Videos

GRAMM, ANDREAS: VERTRAULICHKEIT DURCH ASYMMETRISCHE KRYPTOLOGIE (8MIN)

Aufgaben

14. Deine Schule möchte verschlüsselte Mails bzw. Chatsitzungen innerhalb der Schülerschaft möglich machen. Jeder Schüler soll jedem anderen spontan verschlüsselte Mails (oder Chatnachrichten) schicken können, ohne dafür in dem Moment einen Schlüssel übermitteln zu müssen. Warum eignen sich symmetrische Chiffren dafür ganz grundsätzlich nicht?

Antwort: Damit das auch spontan klappt, müssen alle Schlüssel vorher vorbereitet werden. Wenn deine Schule z.B. 500 Schüler hat, müsstest du mit 499 Personen einen Schlüssel vereinbaren bzw. übergeben und die anschließend alle geheim halten. Die Schlüsselverwaltung wäre zu aufwändig. So viele Geheimnisse will man aber lieber nicht haben.

15. Ein spontaner, verschlüsselter Nachrichtenaustausch soll auch zur Vorbereitung des Frankreich- (noch besser Australien-)Austauschs möglich sein. Warum eignen sich symmetrische Chiffren dafür ganz grundsätzlich nicht?

Antwort: Wenn man sich nicht vorab zum →Schlüsselaustausch persönlich treffen kann, braucht man dafür einen vertrauenswürdigen Boten, oder einen anderen sicheren Kommunikationskanal. Dann braucht man aber auch keine Verschlüsselung.

16. Zeichne ein Flussdiagramm zum Ablauf eines eMail-Austausches mit asymmetrischer Verschlüsselung.

Lösung: Diagramm im Skript

17. Bob besitzt eine Kopie von Alice' öffentlichem Schlüssel. Was ist in dieser Situation gewährleistet und was nicht?

Bob kann eine geheime Nachricht an Alice schicken, sie aber nicht an ihn.
Alice kann eine offene Nachricht unterschreiben und Bob diese auf Authentizität prüfen – umgekehrt aber nicht. Hierfür bräuchte auch Bob ein Schlüsselpaar und müsste Alice seinen öffentlichen Schlüssel zur Verfügung stellen.

18. Bei einem Man-in-the-Middle Angriff fängt Mallory den initialen Schlüsselaustausch ab und ersetzt die Angaben durch seine. Er kontrolliert dann die komplette Kommunikation. Zeichne ein Sequenzdiagramm, aus dem dieses Vorgehen am Beispiel der Vorhängeschlösser

aus dem Unterricht hervor geht.

Lösung: Diagamm im Skript

19. *Zeige auf, welche Kriterien bei einem kryptografischen Kommunikationssystem betrachtet werden.

***Vertraulichkeit**: Nur der designierte Empfänger kann die Nachricht lesen.*
***Integrität**: Der Empfänger kann feststellen, ob die Nachricht nach ihrer Erzeugung verändert wurde.*
***Authentizität**: Der Absender der Nachricht ist überprüfbar.*
***Verbindlichkeit**: Der Absender kann seine Urheberschaft nicht abstreiten.*

Kryptobox

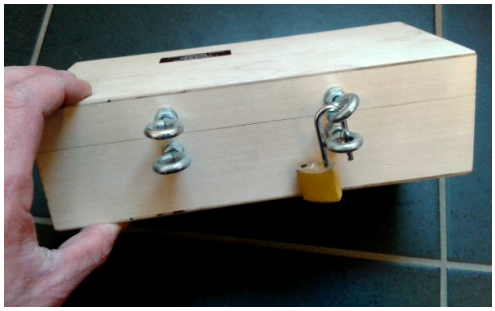


Abbildung 2: Kryptobox (eigenes Bild)

Das Problem der Schlüsselverwaltung kann auf einer anschaulichen Ebene sehr elegant gelöst werden, wenn man auf Kisten mit Vorhängeschlössern zurückgreift.

Spielregeln:

- Kiste und Schloss widerstehen brute-force-Angriffen.
- Von allem, was man in der Hand hält, kann man auch Kopien machen (wie von Dateien).
- Dem Schloss sieht man nicht an, wie der zugehörige Schlüssel aussieht.
- Der Transport der Kiste zwischen Alice und Bob (überhaupt ihre gesamte Kommunikation) erfolgt über Dritte, die zwischen ihnen sitzen und nicht vertrauenswürdig sind.

Ein Vorhänge-Zahlenschloss kann für die Veranschaulichung symmetrischer Verfahren sowie für Secret Sharing verwendet werden.

Für die Darstellung asymmetrischer Verfahren werden zusätzlich mehrere gleichschließende Vorhängeschlösser benötigt.

Abbildung 3: Zahlenschloss (eigenes Bild)

Abbildung 4: Schlössersatz für die Kryptobox (eigenes Bild)

Einkaufsliste

1	*Kiste mit Klappdeckel*
4 *8*	*Ringschrauben,* *Muttern*
1	*Vorhänge-Zahlenschloss*
4	*Sets mit je 2 (besser 4) gleichschließenden Schlössern*
	Lack oder Klebeband für farbliche Markierung

Es bietet sich an, die Schlösser gleich in größeren Sets mit zB je 4 Schlössern anzuschaffen, um Verlusten vorzubeugen und dann nicht ganze Sets austauschen zu müssen.

Das zweite Ringpaar dient der Veranschaulichung des Diffie-Hellman-Austauschs. Möchte man das Verfahren nicht ansprechen, sollten diese Ringschrauben weggelassen werden .

Ablaufbeschreibungen zur Kryptobox - Lehrerhandreichung

Senden einer asymmetrisch verschlüsselten Nachricht

Schritt	Schlüssel-/Schloss-Bild	Asymmetrisches Verfahren
1	Alice hat ein Schlüssel-/Schloss-Paar	… erzeugt ein Schlüsselpaar (mit privatem und öffentlichem Schlüssel)
2	Alice macht eine Kopie des Schlosses, beschriftet sie mit „Alice“ und schickt sie an Bob	schickt eine Kopie des öffentlichen Schlüssels an Bob
3	Bob macht eine Kopie des Schlosses, steckt die Nachricht in eine Kiste, verschließt sie mit dem Schloss...[1]	Bob chiffriert die Nachricht mit Alice' öffentlichem Schlüssel...
4	… und schickt sie ab.	… und schickt sie ab.
5	Alice öffnet das Schloss mit ihrem Schlüssel.	Alice entschlüsselt die Nachricht mit ihrem privaten Schlüssel.

Senden einer asymmetrisch verschlüsselten Nachricht mit 3-Wege-Handshake

Schritt	Schlüssel-/Schloss-Bild
1	Alice hat ein Schlüssel-/Schloss-Paar, Bob ebenfalls.
2	Alice steckt die Nachricht in eine Kiste, verschließt sie mit ihrem Schloss
2b	... und schickt sie an Bob.
3	Bob empfängt die Kiste, verschließt diese zusätzlich mit seinem Schloss
3b	… und schickt sie an Alice zurück.
4	Alice entfernt ihr Schloss von der Kiste
4b	... und schickt sie wieder an Bob.
5	Bob empfängt die Kiste zum zweiten Mal und kann nun sein eigenes Schloss öffnen, um die Nachricht zu lesen.

Stellt man einen offenen Arbeitsauftrag, der nur die sichere Übermittlung an den Empfänger formuliert, kommen die meisten Schüler auf diesen 3-Wege-Handshake. Das ist eine nette Denkaufgabe, aber hat keine Entsprechung in einem Asymmetrischen Kryptographie-Verfahren. Insbesondere ist es kein Diffie-Hellman-Austausch, wie häufig missverstanden.

1 Schüler kopieren in der Regel nicht das Schloss an dieser Stelle, sondern verwenden das Exemplar, das ihnen geschickt wurde. Damit müssten sie für die nächste Nachricht wieder ein neues Schloss anfordern, mit allen damit verbundenen Problemen. Diesen Punkt sollte man spätestens dann thematisieren, wenn der Man-in-the-Middle-Angriff durchgespielt wird, um den Schlüsselaustausch als kritische Phase zu veranschaulichen.

Man-in-the-middle-Angriff auf den initialen Schlüsselaustausch
(passt für alle asymmetrischen Kryptoverfahren)

Schritt	Schlüssel-/Schloss-Bild	RSA (und alle asymm. Verfahren)
1	Alice kauft ein Schlüssel-/Schloss-Paar	Alice erzeugt ein Schlüsselpaar (mit privatem und öffentlichem Schlüssel)
2	Alice macht eine Kopie des Schlosses, beschriftet sie mit „Alice“ und schickt sie an Bob	Alice schickt eine Kopie des öffentlichen Schlüssels an Bob
2b	Mallory fängt das Schloss von Alice ab und behält es.	Mallory fängt den öffentlichen Schlüssel ab und behält ihn.
2c	Mallory nimmt eines seiner eigenen Schlösser, beschriftet es mit „Alice“ und schickt es an Bob.	Mallory erzeugt ein eigenes Schlüsselpaar und schickt den öffentlichen Teil an Bob.
3	Bob macht eine Kopie des Schlosses, steckt die Nachricht in eine Kiste, verschließt sie mit dem Schloss...	Bob chiffriert die Nachricht mit dem öffentlichem Schlüssel...
4	… und schickt sie ab.	
4b	Mallory öffnet sein Schloss (mit „Alice“ beschriftet!) mit seinem Schlüssel.	Mallory dechiffriert die Nachricht mit seinem privaten Schlüssel
5	Mallory hat die Wahl: Er kann die Nachricht lesen und anschließend weiterschicken oder wegwerfen; er kann sie aber auch durch eine gänzlich andere ersetzen. Wenn er etwas weiterschickt, muss es jedenfalls mit Alice' Schlüssel chiffriert (bzw. mit Alice' Schloss verschlossen) werden.	
5b	Alice öffnet das Schloss mit ihrem Schlüssel. Der Inhalt der Kiste scheint von Bob zu kommen.	Alice entschlüsselt die Nachricht mit ihrem privaten Schlüssel.

KeyServer: Öffentliche Schlösser auf d Tisch mit Namen → Notwendigkeit Verifikation

Schritt	Schlüssel-/Schloss-Bild	RSA (und alle asymm. Verfahren)
1	Die Schlösser werden auf einem zentralen Tisch verteilt, mit Namen ihrer Besitzer versehen	Die öffentlichen Schlüssel liegen auf einem Keyserver, markiert mit der eMail-Adresse (für PGP)
2	Bob nimmt sich ein mit Alice' Namen beschriftetes Schloss, steckt die Nachricht in eine Kiste, verschließt sie mit dem Schloss...	Bob holt sich vom Keyserver den öffentlichen Schlüssel mit Alice' eMail-Adresse, verschlüsselt seine Nachricht damit
2b	… und schickt sie ab.	
3	Alice öffnet das Schloss mit ihrem privaten Schlüssel und liest die Nachricht.	Alice entschlüsselt mit ihrem privaten Schlüssel die Nachricht.

Ablauf mit MITM

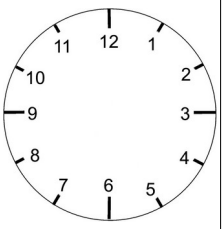
Schritt	Schlüssel-/Schloss-Bild	RSA (und alle asymm. Verfahren)
1	Die Schlösser werden auf einem zentralen Tisch verteilt, mit Namen ihrer Besitzer versehen.	Die öffentlichen Schlüssel liegen auf einem Keyserver, markiert mit der eMail-Adresse (für PGP) .
2	Mallory legt sein Schloss dazu, beschriftet mit Alice' Namen.	Mallory erzeugt sich einen gefälschten Schlüssel für Alice' Mailadresse.
3	Bob nimmt sich das mit Alice' Namen beschriftetes Schloss von Mallory, steckt die Nachricht in eine Kiste, verschließt sie mit dem Schloss...	Bob holt sich vom Keyserver den (von Mallory erzeugten) öffentlichen Schlüssel mit Alice' eMail-Adresse, verschlüsselt seine Nachricht damit
4	… und schickt sie ab.	
4b	Mallory fängt die Kiste ab, öffnet sein Schloss (auch wenn es mit „Alice“ beschriftet ist) mit seinem Schlüssel.	Mallory fängt die Nachricht ab und dechiffriert die Nachricht mit seinem privaten Schlüssel
5	Alice erhält eine Kopie der Kiste, kann sie aber nicht öffnen. Sie weiß nun, dass gefälschte Schlösser im Umlauf sind – kann diese aber nicht aus dem Verkehr ziehen.	Alice erhält die Nachricht, die sie nicht entschlüsseln kann. Sie weiß nun, dasses gefälschte öffentliche Schlüssel zu ihrer eMail-Adresse gibt, kann diese aber nicht zurückziehen.
5b	Sie muss sich einen neuen Namen zulegen.	Ihre eMail-Adresse ist damit kryptographisch unbrauchbar und muss ersetzt werden.

Der Man-in-the-Middle-Angriff macht die Notwendigkeit eines Schlüsselverifikationsverfahrens deutlich. Die heutigen Antworten darauf sind Zertifikate und das Web of Trust.

Modulare Arithmetik für die Kryptografie

Information

Die modulare Arithmetik ist wesentlich für das RSA-Verfahren in der Kryptologie. Wir biegen den Zahlenstrahl zum Zahlenkreis und rechnen wie gewohnt.



Darin gibt es jetzt nur noch die Zahlen 1 bis 12.

Sieben Stunden nach zehn Uhr ist es 5 Uhr.

Sechs Stunden vor zwei Uhr war es 8 Uhr.

Wenn man (ab null Uhr) vier mal sieben Stunden wartet, ist es 4 Uhr.

$0 + 4 \cdot 7 = 28 \equiv 4 \pmod{12}$ wird ausgesprochen „28 ist kongruent 4 modulo 12“. Es bedeutet: „Im 12er-Zahlenkreis spielt die 4 die gleiche Rolle wie die 28.“

Aufgaben

20. Zum Üben und Vorbereiten

5+9	≡ 2 (mod 12)	9*5	≡ 5 (mod 20)	8–8	≡ 0 (mod 12)
5–9	≡ 8 (mod 12)	10*5	≡ 10 (mod 20)	5+ 7	≡ 0 (mod 12)
5+9	≡ 1 (mod 13)	11*5	≡ 15 (mod 20)	21+ 10	≡ 0 (mod 31)
5–9	≡ 15 (mod 19)	3*15	≡ 5 (mod 20)	21+ 41	≡ 0 (mod 31)
88	≡ 37 (mod 51)	4*15	≡ 0 (mod 20)	31	≡ 0 (mod 31)
3*5	≡ 15 (mod 17)	5*15	≡ 15 (mod 20)	7*(15+9)	≡ 14 (mod 22)
5*5	≡ 8 (mod 17)	2+10	≡ 12 (mod 20)	7* (2)	≡ 14 (mod 22)

Information

Um diese Arithmetik anwenden zu können, müssen wir uns einige grundlegende Eigenschaften dieser Arithmetik ansehen:

- Gibt es auch im Zahlenkreis eine Art „Nullzahl“, deren Addition zu einer anderen Zahl x wieder x ergibt?
- Gibt es auch im Zahlenkreis zu jeder Zahl x eine „Gegenzahl“, deren Addition zu x immer Null ergibt?
- Das Gleiche für die Multiplikation: Gibt es auch im Zahlenkreis eine „Eins“, die man zu jeder anderen Zahl x dazu multiplizieren kann, so dass wieder x herauskommt?
- Und hat immer noch jede Zahl x eine Kehrzahl k_x, so dass $k \cdot k_x = 1$?

Links

Wikipedia: Kongruenz (Zahlentheorie).
Rhein-Wied-Gymnasium Neuwied: Mathematische Grundlagen von RSA.

Aufgaben

21. Welche gewohnten Rechenregeln gelten auch modulo N?

Gilt die...	**… für die Addition modulo N? Beispiel, Begründung**	**… für die Multiplikation modulo N? Beispiel, Begründung**
Kommutativität	*5 + 8 = 13 ≡ 4 (mod 9)* *8 + 5 = 13 ≡ 4 (mod 9)* *Folgt aus der Kommutativität der Addition in N*	*5 · 8 = 40 ≡ 4 (mod 9)* *8 · 5 = 40 ≡ 4 (mod 9)* *Folgt aus der Kommutativität der Multiplikation in N*
Assoziativität	*5 + (2+6) = 13 ≡ 4 (mod 9)* *(5+2) + 6 = 13 ≡ 4 (mod 9)* *Folgt aus der Assoziativität der Addition in N*	*5 · (2·4) = 40 ≡ 4 (mod 9)* *(5·2) · 4 = 40 ≡ 4 (mod 9)* *Folgt aus der Assoziativität der Multiplikation in N*
Existenz des neutralen Elements	*5 + 0 = 5 ≡ 5 (mod 9)* *Das neutrale Element aus N bleibt auch hier neutral.*	*5 · 1 = 5 ≡ 5 (mod 9)* *Das neutrale Element aus N bleibt auch hier neutral.*
Existenz des inversen Elements	*5 + 4 = 9 ≡ 0 (mod 9)* *5 + (9-5) = 9 ≡ 0 (mod 9)* *Das additive Inverse steht dem Element im Zahlenkreis gegenüber.*	*5 · 2 = 10 ≡ 1 (mod 9)* *4 · 7 = 28 ≡ 1 (mod 9)* *Für die 3 und die 6 findet man kein multiplikatives Inverses, da sie nicht teilerfremd zur 9 sind.*

Evtl kann die Abgeschlossenheit noch betrachtet werden.

Weitere Rechenregeln:

Distributivgesetz.....

22. Kehrzahlen bestimmen

Kehrwerte modulo 13				**Kehrwerte modulo 15**			
z	$z^{-1}(mod\,13$	z	$z^{-1}(mod\,13)$	z	$z^{-1}(mod\,15)$	z	$z^{-1}(mod\,15)$
0	---	8	5	0	---	8	2
1	1	9	3	1	1	9	---
2	7	10	4	2	8	10	---
3	9	11	6	3	---	11	11
4	10	12	12	4	4	12	---
5	8			5	---	13	7
6	11			6	---	14	14
7	2			7	13		

RSA

Information

Das RSA-Kryptosystem von Rivest, Shamir und Adleman aus dem Jahr 1977 ist eines der ersten praktisch eingesetzten Public-Key-Kryptosysteme und für kryptografische Datenübertragung weit verbreitet. Die Idee basiert auf der praktischen Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen – das Faktorisierungsproblem.

Erzeugung eines RSA-Schlüsselpaares für Alice		
Was tut sie?	**Beispiel mit Zahlen**	**Wie macht sie das?**
Sie wählt zwei Primzahlen, die sie p und q nennt;	p=7 q=11	Primzahltest, z.B. Miller-Rabin-Test (hier nicht behandelt)
… berechnet deren Produkt $N_{Alice}=p\cdot q$	$N=7\cdot 11=77$	Normale Multiplikation
… berechnet die Zahl $\varphi(N)=(p-1)\cdot(q-1)$	$\varphi(77)=(7-1)\cdot(11-1)=6\cdot 10=60$	Normale Multiplikation
… wählt einen Verschlüsselungs-(„encryption“)exponenten e_{Alice}, der er zu $\varphi(N_{Alice})$ teilerfremd ist;	$e_{Alice}=17$ Probe: ggt(17,60) = 1	Sie wählt ihr e z.B. durch Probieren und prüft es, indem sie den größten gemeinsamen Teiler von e und N bestimmt, z.B. mit dem euklidischen Algorithmus
… berechnet ihren Entschlüsselungs-(„decryption“)exponenten d_{Alice},indem sie das Inverse von e_{Alice} modulo $\varphi(N)$ bestimmt;	$d_{Alice}=17^{(-1)} \bmod 60 = 53$ [Probe: $17\cdot 53=901\equiv 1 \pmod{60}$]	Erweiterter euklidischer Algorithmus (hier nicht behandelt)
… löscht p, q und $\varphi(N)$;		
… veröffentlicht das Zahlenpaar (N_{Alice}, e_{Alice}), das ihren öffentlichen Schlüssel $öff_{Alice}$ darstellt.	$öff_{Alice}=(77,17)$	
… hält die Zahl d_{Alice} sorgfältig geheim; sie ist ihr privater Schlüssel.	$priv_{Alice}=53$	

RSA kommt in vielen aktuellen Anwendungen zum Einsatz – beispielsweise der E-Mail-Verschlüsselung mit PGP.

Die Verwendung innerhalb einer Kommunikation an einem Beispiel mit kleinen Zahlen:

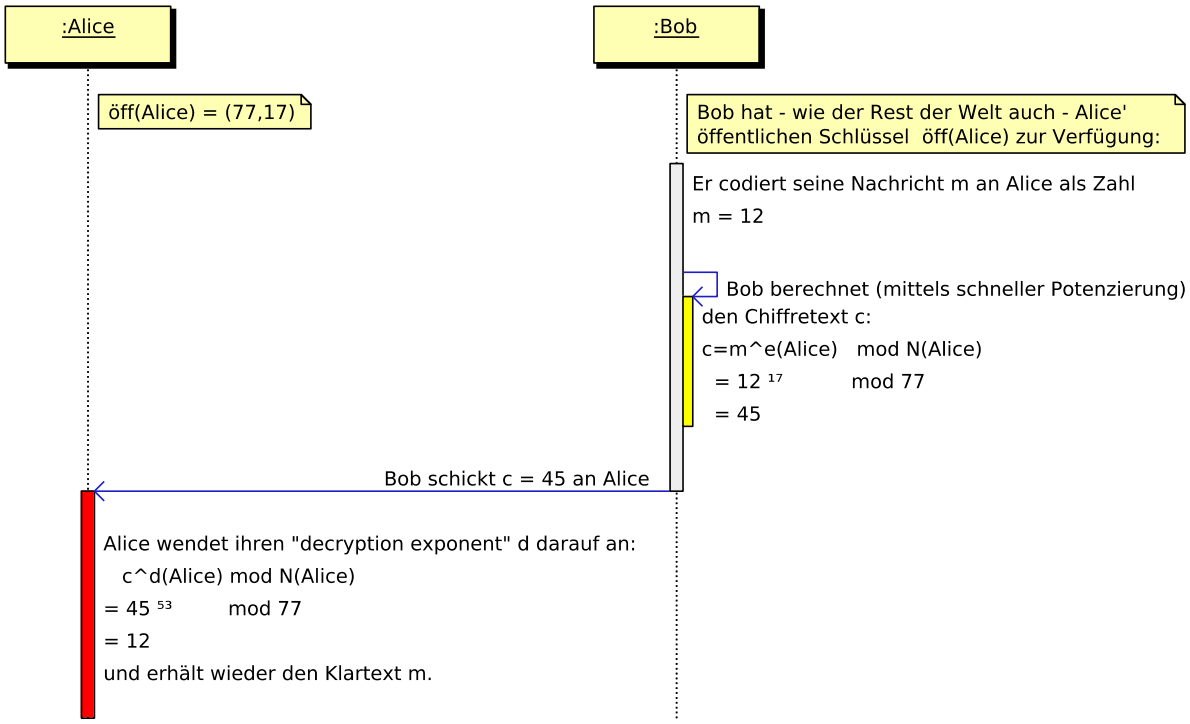


Abbildung 5: Ver- und Entschlüsselung mit RSA am Zahlenbeispiel

Links

MATHEPRISMA. RSA.
INF-SCHULE.DE: RSA.
INF-SCHULE.DE: SICHERER E-MAIL-AUSTAUSCH.
SPIEGEL ONLINE: REKORD-ENTSCHLÜSSELUNG: MATHEMATIKER KNACKEN ZAHL MIT 200 DEZIMALSTELLEN.
INFORMATIK IM KONTEXT: E-MAIL (NUR?) FÜR DICH.

Videos

SPANNAGEL, CHRISTIAN: RSA: VER- UND ENTSCHLÜSSELUNG (15MIN)
SPANNAGEL, CHRISTIAN: RSA: KONSTRUKTION DER SCHLÜSSEL. (17MIN)
SEMPERVIDEO: PGP VERSCHLÜSSELUNG - THEORIE. (9MIN)
HEINLEINSUPPORT: WIE FUNKTIONIERT E-MAIL-VERSCHLÜSSELUNG MIT PGP? (3MIN

Aufgaben

23. Kommuniziere mit einem kleinen RSA-Schlüsselpaar mit einem Partner – die Nachrichten sind ebenfalls kleine Zahlen.

Verwendung des AB Kleine bzw. sehr kleine Schlüsselpaare für RSA

24. Begründe: Die Verwendung kleiner natürlicher Zahlen als Nachrichten ist eine sinnvolle Vereinfachung – das Verfahren kann problemlos auf Texte, Bilder, Ton u.ä. übertragen werden.

Querbezug zur Codierung → ASCII, Hexedit, Bildcodierung

25. (*) Führe die Schlüsselerzeugung mit kleinen Zahlen selbst durch. Für die Berechnung der multiplikativen Inversen kannst du einen Webrechner[2] verwenden.

2Etwa auf *www.cs.princeton.edu/~dsri/modular-inversion-answer.php*

Kleine bzw. sehr kleine Schlüsselpaare für RSA[3]

Achtung: Mit allen Schlüsseln wird c=m, falls m ein Vielfaches von p oder q ist. Der Effekt irritiert die Schüler, und tritt bei sehr kleinen Schlüsseln oft auf (s. Hintergrundskript Seite 25).

Sehr klein (p, q < 20)		**Klein (p, q < 200)**	
Öffentlich	**Privat**	**Öffentlich**	**Privat**
(35;17)	5	(3071;5)	1181
(55;33)	17	(7663;5)	4493
(55;27)	3	(7979;7)	3343
(55;23)	7	(11021;5)	4325
(133;5)	65	(13589; 5)	10685
(91;5)	29	(17399; 11)	9347
(77;7)	43	(15481; 3)	10155
(55;3)	27	(21509; 5)	16973
(85;3)	43	(25591; 5)	10109
(115;3)	59	(15811; 11)	8483
(119;5)	77	(21353; 7)	15043
(91;5)	29	(31133; 7)	26383

3 Generator unter *https://tools.justus-d.de/rsa/* (abgerufen 5.3.2022)

Moderne Anwendungen asymmetrischer Verfahren

Information

Wir haben bisher nur Chiffren behandelt und auch RSA nur als Chiffre kennen gelernt – dabei ist Kryptografie wesentlich vielseitiger als „immer nur Chiffrieren“. Neben der reinen Geheimhaltung kann auch die Authentizität einer Nachricht („kommt sie wirklich von Bob?“) sowie deren Integrität („hat die Nachricht auch niemand verändert?“) mithilfe von RSA gesichert werden. Man spricht dann von einer „kryptografischen Unterschrift“, einer *Signatur*.

Die Grundidee ist diesmal, dass Alice zuerst ihren privaten Schlüssel auf die Nachricht anwendet. Das Ergebnis ist eine Zahl, die nur Alice erzeugt haben kann, eben weil ihr privater Schlüssel in die Berechnung eingeht. Danach verwendet Bob ihren öffentlichen Schlüssel, um die Unterschrift zu verifizieren: Weil sich Ver- und Entschlüsselungsexponent gegenseitig aufheben, kommt wieder die Nachricht heraus. Jeder kann die Unterschrift prüfen, denn der dazu nötige Schlüssel $\text{öff}_{\text{Alice}}$ ist ja öffentlich.

Anders als eine Unterschrift mit Tinte sichert die digitale zusätzlich auch die Integrität des signierten Texts: Sie wird ja nicht nur „darunter gesetzt“, sondern erstreckt sich über den gesamten Text m (hier der Einfachheit halber nur die Zahl 20); jede Veränderung des Textes führt dazu, dass er nicht mehr zur Signatur s passt. Eine Übereinstimmung garantiert, dass m genau der Text ist, den Alice unterschrieben hat.

Aufgaben

26. Welche Eigenschaften hat eine eigenhändige Unterschrift, z.B. auf einer Entschuldigung in der Schule oder dem Zeugnis am Schuljahresende?

Authentizität: Die Echtheit kann anhand der Handschrifterkennung überprüft werden.
Verbindlichkeit: Sie ist damit auch nicht abstreitbar.

27. Wo finden sich diese Eigenschaften in einer digitalen Signatur wieder?

Die Unterschrift kann nur von Alice sein, denn nur sie hat den privaten Schlüssel $\text{priv}_{\text{Alice}}$, mit dem die Signatur offensichtlich erzeugt worden ist, sonst hätte die Anwendung von $\text{öff}_{\text{Alice}}$ daraus keine lesbare Nachricht gemacht. Sie ist also fälschungssicher.
Aus dem gleichen Grund ist die Unterschrift auch nicht abstreitbar, so dass Alice sich an den Inhalt des Textes bindet – wie mit einer realen Unterschrift auch.

28. Alice erzeugt sich ein Schlüsselpaar, Bob aber nicht. Welche kryptografischen Möglichkeiten haben die beiden in dieser Situation?

Interessanterweise kann nämlich Bob an Alice chiffrierte (also geheime) Nachrichten schicken, sie umgekehrt aber nicht an ihn.
Alice kann an Bob signierte (also authentische) Nachrichten schicken, er aber nicht an sie.

Diese Einseitigkeit ist eine unmittelbare Folge des asymmetrischen Verfahrens.

29. Was muss für einen geheimen E-Mail-Austausch gegeben sein?

Für einen E-Mail-Austausch wird Bob sich normalerweise auch ein Schlüsselpaar erzeugen.

30. Welche kryptografischen Voraussetzungen sind für einen E-Mail-Austausch nötig, der Authentizität sicherstellt?

Bob und Alice müssen jeweils die öffentlichen Schlüssel $\text{öff}_{\text{Alice}}$, öff_{Bob} des anderen kennen und ihre Nachrichten mit ihrem eigenen privaten Schlüssel signieren.

Die genannte Einseitigkeit taucht aber auch bei SSL/TLS wieder auf und wird dort anders gelöst.

31. Entwirf ein Sequenzdiagramm für folgendes Szenario:
Alice und Bob möchten geheim und authentisch per E-Mail kommunizieren. Sie haben zuvor ihre öffentlichen Schlüssel schon erfolgreich ausgetauscht.

Lösung: Diagramm im Skript / Protokoll_geh_auth_Kommunikation.sd

Man in the Middle

Information

Für die geheime und authentische Kommunikation sind wir davon ausgegangen, dass Alice und Bob den Austausch ihrer öffentlichen Schlüssel bereits erfolgreich durchgeführt haben. Allerdings sind asymmetrische Verfahren in der Phase des Schlüsselaustauschs durch einen Man-in-the-middle-Angriff verwundbar, den wir noch unterbinden müssen.

Im Gegensatz zum Schlüsselaustausch bei symmetrischen Verfahren müssen die Schlüssel aber nicht mehr geheim gehalten, sondern nur noch gegen Manipulation gesichert werden:

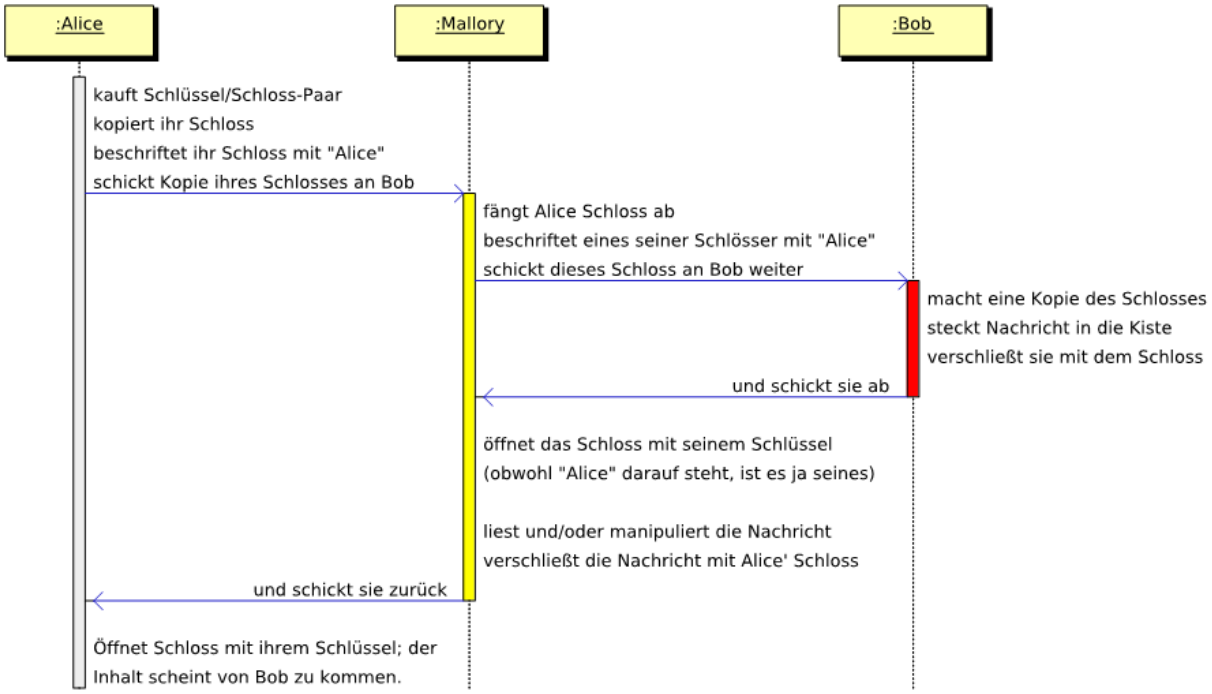


Abbildung 6: Man-in-the-Middle Angriff auf den initialen Schlüsselaustausch

Links

BSI: G 5.143: Man-in-the-Middle Angriff.
Wikipedia: Man-in-the-Middle Angriff.
Deiniger, Matthias: Man-in-the-Middle Angriff (Facharbeit)

Videos

SemperVideo: Man-in-the-Middle Angriff (10min)

Aufgaben

32. Schlage ein Verfahren vor, mit dem Alice und Bob ihren Schlüsselaustausch gegen einen MITM-Angriff absichern können.

> *Antwort: Unter diesem recht freien Auftrag entwerfen die Schüler häufig Protokolle, die sich in irgend einer Weise entweder auf eine persönliche Begegnung, oder aber auf vertrauenswürdige Dritte stützen. Erstere lösen offensichtlich das Problem natürlich nicht, zeigen aber oft viel Kreativität. Der Einbezug vertrauenswürdiger Dritter ist tatsächlich die einzige Möglichkeit, die Anforderung zu erfüllen.*

Zertifikate und das Web of Trust

Information

Um die Authentizität eines Schlüssels zu garantieren, bleibt nur die Zertifizierung durch einen vertrauenswürdigen Dritten. Dieser kann eine Person oder Institution sein, denen alle Netzteilnehmer vertrauen (man spricht dann von einer *Certificate Authority*, kurz CA), so dass sich um diese CAs herum eine stark zentralisierte Vertrauensstruktur bildet.

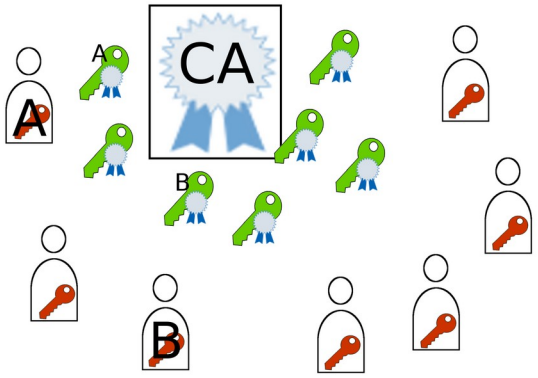


Abbildung 7: Zentrale Vertrauensarchitektur mit CA

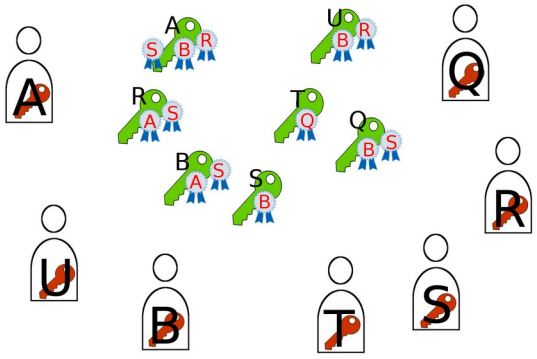


Abbildung 8: Dezentrale Vertrauensarchitektur im WoT

Nach einer anderen Vorgehensweise kann jeder Nutzer aber auch nur für sein näheres Umfeld festlegen, wem und wie stark er vertraut. Diese stark dezentrale Struktur heißt *Web of Trust* (WoT).

Links

INF-SCHULE.DE: SICHERHEITSINFRASTRUKTUR.
WIKIPEDIA: PUBLIC KEY INFRASTRUKTUR.

Videos

SEMPERVIDEO: WEB OF TRUST. (9MIN)

Aufgaben

33. Alice lässt sich von Carmen ein Zertifikat ausstellen und legt es Bob vor. Danach weiß Bob sicher, dass er Alice' richtigen öffentlichen Schlüssel hat, und kann ihn zum Chiffrieren seiner Nachrichten an sie (und zum Verfizieren der Nachrichten von ihr) verwenden. Welches Vertrauen wird hier vorausgesetzt?

Voraussetzung dafür ist, dass Bob Carmens Sorgfalt vertraut.

34. Alice schickt Bob eine verschlüsselte Mail. Seinen Öffentlichen Schlüssel hat sie von einem Keyserver heruntergeladen, er wurde von Quentin, Tarantino und Star signiert. Welches Vertrauen wird hier vorausgesetzt und wovon ist dieses abhängig?

Alice muss wenigstens einer der drei signierenden Personen vertrauen. Die Verlässlichkeit dieser Signaturen hängt nicht direkt von der Anzahl ab – sondern vor allem davon, ob Alice davon ausgehen kann, dass diese Personen Bob kennen und die Echtheit des Schlüssels sorgfältig geprüft haben.
Zu diesem Zweck kann man beim Signieren von Schlüsseln ein Vertrauenslevel angeben.
Überprüfbar ist die Signatur für Alice nur, wenn sie mindestens eine der drei Personen anhand deren Signatur überprüfen kann, d.h. Kennt.

SSL / TLS

Information

Um miteinander sicher zu kommunizieren müssen Alice und Bob sich ziemlich gut auskennen und dann noch eine gewisse Sorgfalt walten lassen.

Um als Laie verschlüsselt mit beispielsweise facebook.com oder dem Onlinebanking-System meiner Bank zu kommunizieren, müssen auch Nutzer, die weder Schlüsselpaar noch Zertifikat besitzen, eine Möglichkeit haben, kryptografisch gesicherte Verbindungen aufzubauen.

Für dieses Problem gibt es die Protokollfamilie TLS, die aus dem veralteten SSL hervorgegangen ist. Mit TLS baut der Browser selbsttätig (ohne dass der Nutzer es bemerkt oder gar den Mechanismus verstehen muss!) eine Verbindung auf, die in *beiden* Richtungen geheim und immerhin in *einer* Richtung authentisch ist – und das auch für Nutzer, die weder Schlüsselpaar oder Zertifikat, noch Informatikkenntnisse besitzen.

Der entscheidende Trick ist die Erzeugung eines kurzlebigen (sogenannten Sitzungs-) Schlüssels für eine *symmetrische* Chiffre auf der Client-Seite, also im Browser. Dieser Schlüssel kann nämlich (asymmetrisch chiffriert!) sicher an den Server geschickt werden.

Ein Schlüsselpaar bietet grundsätzlich nicht beiden Partnern die gleichen Möglichkeiten: Alice kann mit $öff_{Bob}$ immer nur chiffrieren, Bob mit $priv_{Bob}$ immer nur signieren. Diese Asymmetrie manifestiert sich auch bei TLS wieder darin, dass der Client sich dem Server gegenüber prinzipiell nicht authentifizieren kann. Jedenfalls nicht automatisch – mit Loginnamen und Passwort natürlich schon, die deswegen auch immer noch nicht ausgedient haben. Aber erstens werden sie schon mal verschlüsselt übertragen (das gewährleistet TLS ja), und zweitens kann sich ein facebook-Nutzer dann auch darauf verlassen, dass sein Browser wirklich mit facebook verbunden ist und nicht mit einem „man in the middle“.

Der abgeschlossene TLS-Handshake wird z.B. im Firefox durch ein grünes Vorhängeschloss dargestellt, das auch detailliertere Informationen bereithält:

Links

WIKIPEDIA: TRANSPORT LAYER SECURITY.

Videos

CERTCENTERAG: SICHERE WEBSEITEN MIT SSL. (3MIN)

Aufgaben

35. Warum kann Lauscherin Eve bei TLS nicht das Passwort mitlesen, das der Nutzer an den Server schickt?

> *Weil der Austausch durch den Sitzungsschlüssel in beiden Richtungen chiffriert stattfindet.*

36. Was kann Eve über die angezeigten Webseiten erfahren?

> *Sie bekommt mit, wann und wie viele Daten der Nutzer erhält. Das kann gewisse Rückschlüsse auf den Inhalt der Seiten erlauben, aber direkt lesen kann sie nichts.*

37. Welche Möglichkeiten für eine Manipulation bleiben Mallory?

> *Nach erfolgreichem TLS-Handshake kann er nur noch die Verbindung kappen. Mangels privatem Schlüssel kann er sich dem Browser gegenüber nicht als Server ausgeben, und mangels Passwort dem Server gegenüber nicht als Nutzer.*

38. Eine naheliegende Frage ist natürlich, ob und welcher „CArmen“ man denn vertrauen kann. Für verschlüsselten Webverkehr trifft diese Entscheidung der Hersteller des Browsers, der bereits eine ganze Anzahl von CAs mit ihren Root-Zertifikaten (im Wesentlichen ihren öffentlichen Schlüsseln) vorinstalliert hat.
Finde heraus, wo in deinem Browser CAs hinterlegt sind.

In Firefox findet man die CAs im Menü „Extras“ unter „Einstellungen/Erweitert/Zertifikate/Zertifikate anzeigen/Zertifizierungsstellen“.

39. Nimm Stellung zu den gefundenen Zertifizierungsstellen.

Die Liste ist nicht nur unerwartet lang, sondern enthält auch eine Anzahl CAs, deren Namen bei Schülern regelmäßig Heiterkeit oder Stirnrunzeln auslösen:

40. So raffiniert SSL/TLS auch ausgedacht ist, so fragil ist es leider in der Praxis. Überlege dir einen Weg, wie Mallory SSL/TLS aushebeln kann.

*Mallory wird versuchen, sich von einer beliebigen(!) certificate authority ein Zertifikat beispielsweise für die Domain *.google.com signieren zu lassen. Wenn er das schafft, kann er damit als Google auftreten. Eine solche illegitime (aber echte!) Signatur einer einzigen anerkannten CA ist quasi ein Generalschlüssel für fast alle Browser weltweit. Die Absicherung der gesamten Zertifikatsinfrastruktur muss also entsprechend hoch motivierten Angreifern standhalten.*