Vorlesung Informationssicherheit

Thema 2: Grundlagen der Kryptographie

Robert Baumgartl

13. März 2024

Krypt-was?

Zwei Teilgebiete:

Kryptografie beschäftigt sich mit der sicheren Übertragung von Nachrichten

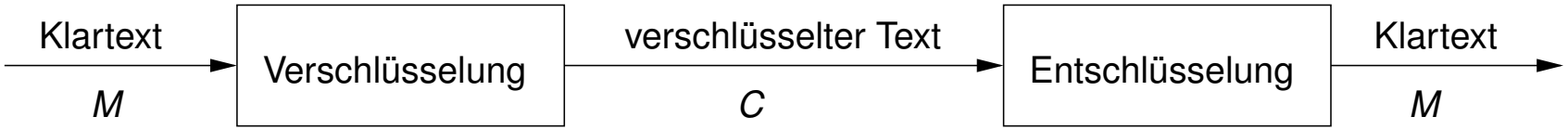
Kryptanalyse ist das Brechen von kryptografisch verschlüsselten Nachrichten

Kryptologie umfasst beide Teildisziplinen und ist selbst ein Teilgebiet der Mathematik.

Grundbegriffe

Sender und **Empfänger** tauschen **Nachrichten** aus.

Damit niemand außer den beiden Teilnehmern den Inhalt der Nachrichten lesen kann, werden diese beim Sender **verschlüsselt** und beim Empfänger **entschlüsselt**:



Verschlüsselungsfunktion E (*encryption*)
Entschlüsselungsfunktion D (*decryption*)

Die unverschlüsselte Nachricht wird **Klartext** (P, *Plain Text*, oder M, *Message*) genannt. Die verschlüsselte Nachricht heißt **Chiffrat** (C).

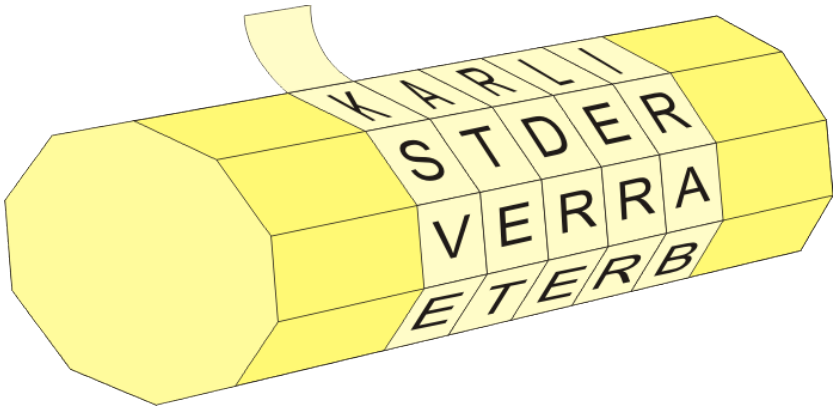
$$E(M) = C \qquad D(C) = M \qquad \text{und damit} \quad D(E(M)) = M.$$

Historie: Skytale

- älteste (dokumentierte) kryptografische Methode (Sparta, $\approx$ 500 v.u.Z.)

Prinzip:

- Pergament- bzw. Lederstreifen um Holzstab definierter Dicke gewickelt
- längs beschriftet
- abgewickelt unlesbar
- Empfänger kann Botschaft nur lesen, wenn Holzstab gleicher Dicke benutzt



Prinzip der Skytale[1]

[1] Abb.: CrypTool-Projekt, `http://www.cryptool.org`, Skytale3d de, CC BY-SA 3.0

Historie: Chiffrierung durch Transposition

Idee: Nur die Positionen der zu kodierenden Zeichen werden manipuliert.

Beispiel: Spaltentransposition

Klartext: COMPUTER GRAPHICS MAY BE SLOW BUT AT LEAST IT'S EXPENSIVE

```
COMPUTERGR
APHICSMAYB
ESLOWBUTAT
LEASTITSEX
PENSIVEXXX
```

Chiffrat: CAELP OPSEE MHLAN PIOSS UCWTI TSBIV EMUTE RATSX GYAEX RBTXX

Historie: Chiffrierung mittels Substitution

- Idee: Elemente im Klartext werden durch andere Elemente im Chiffretext ersetzt
- Dechiffrierung durch Umkehrung der Substitution

Einfachste Form: **monoalphabetische** Substitution

- jedem Zeichen im Klartext ist *genau ein* Zeichen im Chiffrat zugeordnet ($\rightsquigarrow$ genau ein Alphabet)
- Caesar-Verschlüsselung (Pos. im Alphabet + 3 modulo 26)
- ROT-13 Pos. im Alphabet + 13 modulo 26
- unter Ausnutzung relativer Buchstabenhäufigkeiten sehr leicht zu brechen

Buchstabenhäufigkeit

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6.51	n	9.78
b	1.89	o	2.51
c	3.06	p	0.79
d	5.08	q	0.02
e	17.40	r	7.00
f	1.66	s	7.27
g	3.01	t	6.15
h	4.76	u	4.35
i	7.55	v	0.67
j	0.27	w	1.89
k	1.21	x	0.03
l	3.44	y	0.04
m	2.53	z	1.13

Tabelle: Häufigkeit von einzelnen Buchstaben in deutschen Gebrauchstexten (in Prozent)

geordnet nach Auftrittswkt.: e, n, i, s, r, a, t, d, n, u, l, c, g, m, o, b, w, f, k, z, p, v, j, y, x, q

Historie: Chiffrierung mittels Substitution

Weitere Kategorien von Substitutionsverfahren

homophone Substitution

- ein Zeichen Klartext kann auf verschiedene Zeichen Chiffre abgebildet werden
- Zeichenvorrat des Chiffrats größer

polygrafische Substitution

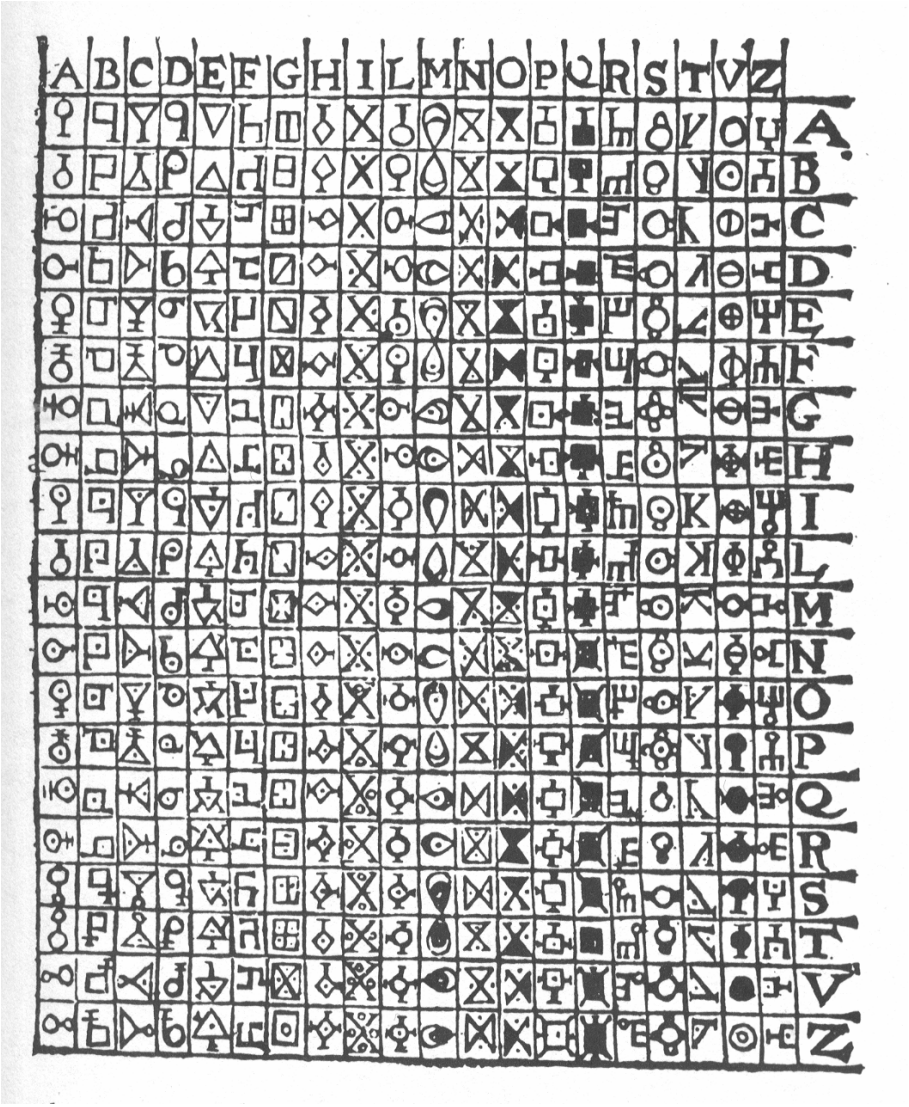
- Blöcke von Zeichen im Klartext werden auf Blöcke von Zeichen im Chiffrat abgebildet

polyalphabetische Substitution

- je nach Position des Zeichens werden *unterschiedliche* Kodierungsalphabete genutzt
- z. B. Vigenère-Verschlüsselung

Historie: Chiffrierung mittels Substitution

Digrafisches System von Giovanni Battista Porta (1563)



Paare von Buchstaben werden durch graphische Symbole ersetzt
(David Kahn: *The Codebreakers.* Scribner, 1996, S. 139)

Vigenère-Verschlüsselung

- Idee: Nutzung mehrerer (bis zu 26) monoalphabetischer Verschlüsselungen im Wechsel; Anordnung im sog. Vigenère-Quadrat
- entwickelt von Blaise de Vigenère (1523-1596)
- Basis vieler Verschlüsselungen, die bis heute genutzt werden
- gleicht unterschiedliche Auftrittswahrscheinlichkeiten der Buchstaben aus
- $\rightsquigarrow$ über Analyse der Buchstabenhäufigkeiten nicht zu brechen

Vigenère-Verschlüsselung

Hilfsmittel: Vigenère-Quadrat oder -Tableau

Klartext

Schluessel	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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

Anwendung

Wahl eines Schlüsselworts – Zuordnung Buchstaben des Schlüsselwortes zu Klartextbuchstaben (ggf. mehrfach)

Verschlüsselung: Schnittpunkt Zeile Schlüsselbuchstabe - Spalte Klartextbuchstabe liefert Chiffratbuchstaben

Entschlüsselung: Schlüsselbuchstabe selektiert wieder monoalphabetische Chiffre, Aufsuchen des Chiffratbuchstabens in Chiffre, darüberliegender Spaltenkopf ist Klartextbuchstabe

Beispiel: (Schlüsselwort: „Elba“)

Schlüssel	E	L	B	A	E	L	B	A	E	L	B	A	E	L	B	A	E
Klartext	a	n	g	r	i	f	f	z	w	e	i	u	h	r	m	e	z
Chiffrat	E	Y	H	R	M	Q	G	Z	A	P	J	U	L	C	N	E	D

Friedrich Wilhelm Kasiski (1863) beobachtete:

Schlüssel	E	L	B	A	E	L	B	A	E	L	B	A	E	L	B	A	E
Klartext	·	·	e	i	n	·	·	·	·	·	·	e	i	n	·	·	·
Chiffrat	·	·	F	I	R	·	·	·	·	·	·	E	M	Y	·	·	·

Schlüssel	E	L	B	A	E	L	B	A	E	L	B	A	E	L	B	A	E
Klartext	·	·	·	e	i	n	·	·	·	·	·	e	i	n	·	·	·
Chiffrat	·	·	·	E	M	Y	·	·	·	·	·	E	M	Y	·	·	·

- Identische Klartextpassagen werden auf identische Chiffratphrasen abgebildet, wenn sie unter identischen Buchstaben des Schlüsselwortes stehen.
- Abstand ist ein Vielfaches der Schlüssellänge!

Vigenère-Verschlüsselung

Kasiski-Test

- Suche nach sich wiederholenden Buchstabenfolgen der Länge 3 und größer im Chiffrat
- Bestimmung des Abstandes dieser gleichen Buchstabenfolgen
- Abstand ist Vielfaches der Schlüssellänge
- Gibt es mehrere Abstände, so muss die Schlüssellänge alle (bzw. die allermeisten) Abstände teilen.
- Ermittlung der Schlüssellänge ist ausreichend, um Vigenère-Verschlüsselung zu brechen.

Vigenère-Verschlüsselung

Kasiski-Test: Beispiel

```
EYRYC FWLJH FHSIU BHMJO UCSEG
TNEER FLJLV SXMVY SSTKC MIKZS
JHZVB FXMXK PMMVW OZSIA FCRVF
TNERH MCGYS OVYVF PNEVH JAOVW
UUYJU FOISH XOVUS FMKRP TWLCI

FMWVZ TYOIS UUIIS ECIZV SVYVF
PCQUC HYRGO MUWKV BNXVB VHHWI
FLMYF FNEVH JAOVW ULYER AYLER
VEEKS OCQDC OUXSS LUQVB FMALF
EYHRT VYVXS TIVXH EUWJG JYARS

ILIER JBVVF BLFVW UHMTV UAIJH
PYVKK VLHVB TCIUI SZXVB JBVVP
VYVFG BVIIO VWLEW DBXMS SFEJG
FHFVJ PLWZS FCRVU FMXVZ MNIRI
GAESS HYPFS TNLRH UYR
```

Folge	Abstand	Zerlegung
TNE	50	2·5·5
FCRV	265	5·53
NEVHJAOVWU	90	2·3·3·5
VWU	75	3·5·5
(OIS)	(26)	(2·13)

Vermutete Schlüssellänge: $\mathrm{ggT}(50, 265, 90, 75) = 5$.

Vigenère-Verschlüsselung

Friedman-Test: Koinzidenzindex

- William Friedman (1925)
- statistische Größe
- kann zur Kryptanalyse unbekannter Chiffrate eingesetzt werden.

Mit welcher Wahrscheinlichkeit ‘erwischt’ man bei zufälliger Auswahl zweier Zeichen aus einem gegebenen Text zwei gleiche Zeichen?

Vigenère-Verschlüsselung

Friedman-Test: Koinzidenzindex

- Anzahl Buchstabenpaare ‘aa’ aus einem Text, der n_1-mal ’a’ enthält:

$$\frac{n_1(n_1 - 1)}{2}$$

- Anzahl Buchstabenpaare ’aa’, ‘bb’, . . . , ‘zz’ aus einem Text, der n_1-mal ‘a’, n_2-mal ‘b’, . . . , n_{26}-mal ‘z’ enthält:

$$\frac{n_1(n_1 - 1)}{2} + \frac{n_2(n_2 - 1)}{2} + \cdots + \frac{n_{26}(n_{26} - 1)}{2} = \sum_{i=1}^{26} \frac{n_i(n_i - 1)}{2}$$

- Wahrscheinlichkeit, bei zufälliger Auswahl zweier Zeichen aus einem Text der Länge n zwei gleiche Zeichen zu erhalten:

$$\frac{\sum_{i=1}^{26} \frac{n_i(n_i - 1)}{2}}{\frac{n(n-1)}{2}} = \frac{\sum_{i=1}^{26} n_i(n_i - 1)}{n(n-1)} = \kappa$$

- κ (Kappa) ist der *Friedmansche Koinzidenzindex*

Vigenère-Verschlüsselung

Koinzidenzindex mit Auftrittswahrscheinlichkeiten

Gegeben: Text deutscher Sprache (Auftrittswahrscheinlichkeiten der einzelnen Buchstaben bekannt)

- Wkt., dass erster Buchstabe des Paares ein ‘a’ ist, ist p_1
- Wkt., dass zweiter Buchstabe des Paares ein ‘a’ ist, ist ebenfalls p_1
- Wkt., bei zufälliger Auswahl zweier Zeichen aus einem deutschen Text zweimal ‘a’ zu erhalten ist damit p_1^2.
- Wkt., bei zufälliger Auswahl zweier Zeichen aus einem deutschen Text zwei gleiche Buchstaben zu erhalten:

$$\kappa = p_1^2 + p_2^2 + \cdots + p_{26}^2 = \sum_{i=1}^{26} p_i^2 .$$

κ der deutschen Sprache ist damit:

$$\kappa_{DE} = 0.0651^2 + 0.0189^2 + \cdots + 0.0113^2 \approx 0.0762. \quad (\kappa_{EN} \approx 0.0667)$$

Für einen Text aus zufälligen Buchstaben ergibt sich hingegen:

$$\kappa_{RND} = \sum_{i=1}^{26} p_i^2 = \sum_{i=1}^{26} \left(\frac{1}{26}\right)^2 = 26 \cdot \frac{1}{26^2} = \frac{1}{26} \approx 0.0385.$$

gegeben:

- Chiffrat der Länge n ($\rightsquigarrow$ Koinzidenzindex κ des Chiffrats trivial zu ermitteln)
- Wissen über die Sprache des Klartextes (z. B. Deutsch, κ_{DE} bekannt)

Dann beträgt die Länge h des Schlüssels näherungsweise (Friedman, 1925):

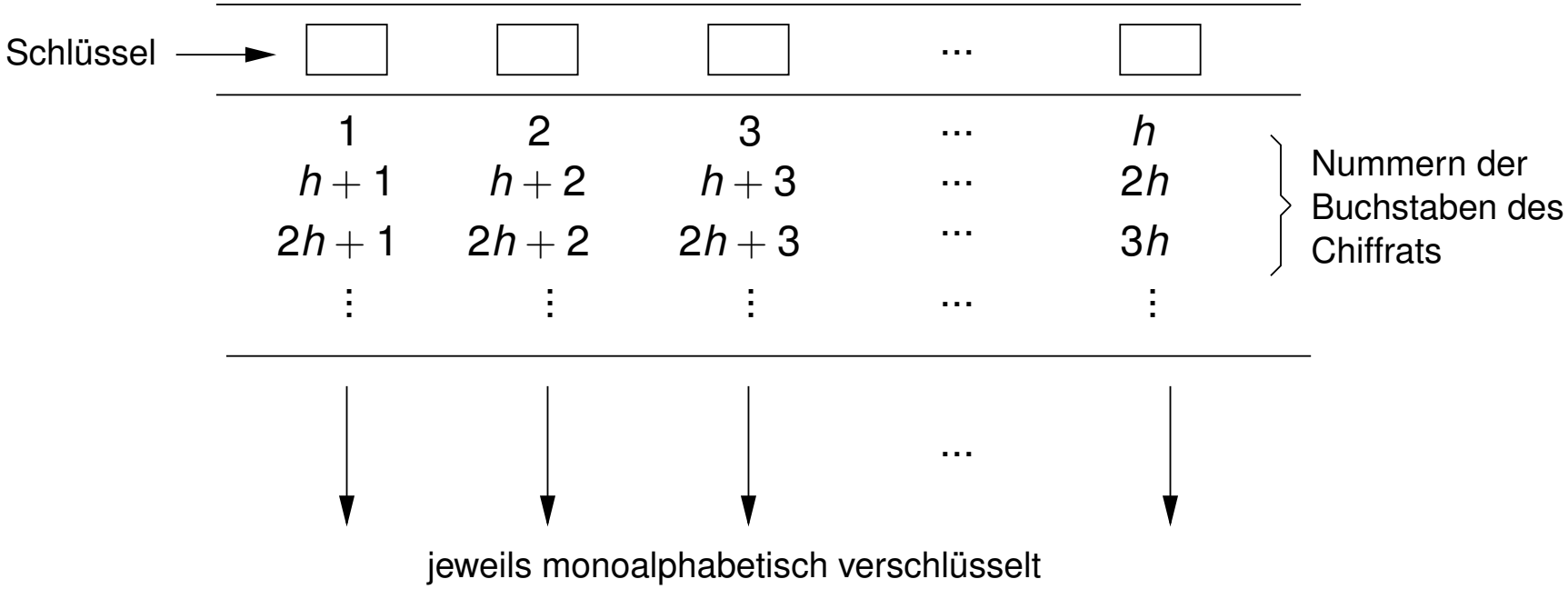
$$h \approx \frac{n(\kappa_{DE} - \kappa_{RND})}{\kappa \cdot (n-1) + \kappa_{DE} - n\kappa_{RND}}.$$

Literatur: Albrecht Beutelspacher: *Kryptologie.* 9. Auflage, Wiesbaden, 2009, S. 34–40.

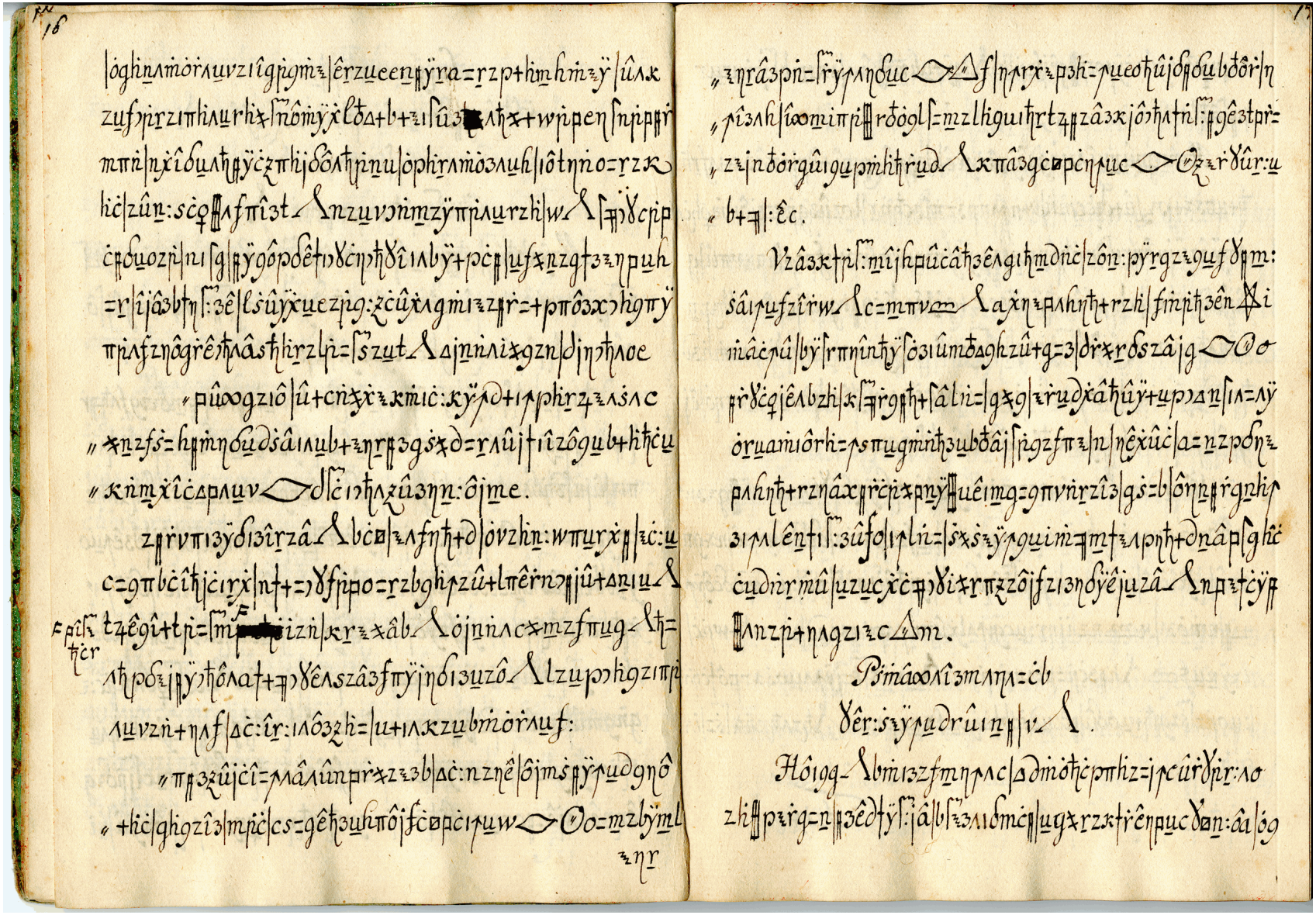
Vigenère-Verschlüsselung

Von der Schlüssellänge zur Dechiffrierung

Schlüsselwortlänge $h \rightsquigarrow$ Chiffrat besteht aus h Folgen, die monoalphabetisch verschlüsselt sind:



Historie: Codex Copiale[2]



[2] Abb.: gemeinfrei

Historie: Codex Copiale

- verschlüsselte Handschrift aus dem 18. Jh.
- homophone Verschlüsselung
- 2011 entschlüsselt (Kevin Knight et al: *The Copiale Cipher.* Proceedings of the 4th Workshop on Building and Using Comparable Corpora. Stroudsburg PA, 2011)
- deutscher Klartext
- Beschreibung geheimer Initiationsriten einer deutschen freimaurerähnlichen Gesellschaft („Oculisten“)

Historie: Das Voynich-Manuskript[3]

- wahrscheinlich zwischen 1404 und 1438 geschrieben
- 102 (erhaltene) Pergament-Blätter, beschrieben in einer unbekannten Sprache
- „Text“ gehorcht bestimmten natürlichsprachigen Statistiken
- bis heute nicht entschlüsselt (Freiwillige vor!)

[3] Abb.: gemeinfrei

Playfair-Chiffre

1. Vorbereitung Klartext

- Kleinbuchstaben in Großbuchstaben umwandeln
- Interpunktionszeichen eliminieren
- Substitution des ‘J’ durch ‘I’
- Ersetzung der Umlaute durch Zwielaute (‘Ä’ $\rightarrow$ ‘AE’ usw.)
- Unterteilung in Bigramme, dabei Einfügen eines ‘X’, falls Buchstaben in ein- und demselben Bigramm doppelt auftreten
- Anfügen eines ‘X’, falls ungerade Anzahl Zeichen resultiert

Beispiel-Klartext: „Jawoll, Ostern ist schön!“
Resultat Vorbereitung: „IA WO LX LO ST ER NI ST SC HO EN“

Playfair-Chiffre

2. Erstellung des Playfair-Quadrates

Anordnung aller Buchstaben des Alphabets (ohne ‘J’) in 5x5-Quadrat nach folgender Vorschrift:

- links oben beginnend nach rechts Schlüsselwort eintragen, dabei doppelt vorkommende Buchstaben auslassen
- danach die restlichen Buchstaben in alphabetischer Reihenfolge
- Beispielschlüssel: „Osterhase“

Beispiel:

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

Sender und Empfänger generieren Quadrat; müssen also Schlüssel kennen.

Playfair-Chiffre

3. (Bigrammweise) Verschlüsselung

a) Stehen beide Zeichen des Plaintextes in ein- und derselben Zeile, dann Ersetzung der Zeichen durch die jeweils **rechts** davon stehenden Zeichen (mit „Wrap-Around"). Beispiel: ST → TE

b) Stehen beide Zeichen des Plaintextes in ein- und derselben Spalte, dann Ersetzung durch die jeweils **darunterstehenden** Zeichen (mit „Wrap-Around"). Beispiel: HO → FH

c) Ansonsten Ersetzung der Zeichen des Plaintextes durch die **diagonal gegenüberliegenden „Ecken“** des aufgespannten Rechtecks; Zeile zuerst. Beispiel: LX → IZ

Beispiel:

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

Playfair-Chiffre

Verschlüsselung des Beispiels

Klartext	Chiffrat
IA	GB
WO	VS
LX	IZ
LO	FR
ST	TE
ER	RO
NI	PG
ST	TE
SC	EA
HO	FH
EN	SQ

Playfair-Quadrat:

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

Playfair-Chiffre

Anmerkungen

- Entschlüsselung erfolgt in (geometrisch) umgekehrter Richtung.
- Verfahren ist monoalphabetisch bigraphisch.
- überlegen ggü. Verfahren mit einzelnen Zeichen
- sehr leicht zu erlernen und auszuführen (Forderung Nr. 6 der Kerckhoffs'schen Prinzipien)
- 1854 von Sir Charles Wheatstone erfunden; Lord Lyon Playfair zugeschrieben
- genutzt bis ca. zum 1. Weltkrieg
- heute kryptografisch gebrochen, d. . h., unsicher

- Friedrich L. Bauer. *Entzifferte Geheimnisse*. Springer, 1995
- Simon Singh. *Geheime Botschaften*. dtv, 2001
- David Kahn. *The Codebreakers*. Scribner, 1996
- Klaus Schmeh. *Codeknacker gegen Codemacher*. 3. Aufl. w3l AG, 2014

Schlüssel

Ver- und Entschlüsselung erfolgt bei modernen Algorithmen mit sog. Schlüsseln (K, *key*).

- Schlüssel haben i. a. sehr großer Wertebereich (damit man nicht alle durchprobieren kann)
- Schlüssel sind für Ver- und Entschlüsselung nötig

Es gibt sowohl Verfahren, die ein- und denselben Schlüssel für Ver- und Entschlüsselung nutzen, als auch Verfahren, die verschiedene Schlüssel erfordern.

$\rightarrow$ Sicherheit der Verfahren hängt maßgeblich von Schlüsseln ab.

Zwei Kategorien von Verschlüsselungsverfahren

Kryptografische Algorithmen mit Schlüsseln:

1. symmetrische Verfahren
   - Chiffrier- und Dechriffrierschlüssel meist identisch
   - aka *secret key*, *single key*
   - Schlüssel muss zwischen Sender und Empfänger vereinbart werden
   - **Schlüssel muss unbedingt geheim bleiben!**
   - blockbasierte vs. strombasierte Verfahren
2. asymmetrische Verfahren
   - 2 verschiedene Schlüssel
   - Chiffrierschlüssel ist öffentlich (*public key*)
   - Dechiffrierschlüssel ist geheim (*private key*)
   - jeder kann eine Nachricht verschlüsseln
   - nur der Besitzer des Dechiffrierschlüssels kann diese entschlüsseln

Ein *Kryptosystem* ist ein Verschlüsselungsalgorithmus sowie alle möglichen Klartexte, Chiffren und Schlüssel.

Kerckhoffs'sches Prinzip

Anforderungen an ein sicheres Kryptosystem:

- Das System muss im Wesentlichen, am besten mathematisch, unentschlüsselbar sein.
- Das System darf keine Geheimhaltung erfordern und kann durch den Gegner gestohlen werden.
- Es muss leicht übermittelbar sein und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können, Schlüssel müssen leicht austauschbar sein.
- Das System sollte mit telegraphischer Kommunikation kompatibel sein.
- Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern.
- Das System muss einfach anwendbar sein [. . .].

(Auguste Kerckhoffs: *La Cryptographie Militaire.* In: Journal des Sciences Militaires, Januar 1883, S. 12)

Blockbasierte vs. strombasierte Verfahren

blockbasiert:

1. Klartext wird in Blöcke gleicher Länge strukturiert
2. ggf. werden Nullbytes aufgefüllt (*Padding*)
3. Ver- und Entschlüsselung erfolgen blockweise
4. typische Längen: 64 Bit (DES), 128 Bit (AES), 1024 (RSA)
5. meiste moderne Verfahren

strombasiert:

- Strom von Bits, Bytes oder Zeichen
- Ver- und Entschlüsselung erfolgt bit-, byte- oder zeichenweise
- Vigenère-Verfahren, XOR-Verschlüsselung, RC4, A5/1 (GSM)
- Vorteil: es muss nicht auf Komplettierung des ersten Blockes gewartet werden (niedrige Latenz)

Beschränkte Algorithmen

- nicht publiziert (geheimgehalten)
- breiter wissenschaftlichen Diskussion entzogen (kein *Peer Review*)
- beziehen ihre „Sicherheit“ aus der Geheimhaltung des Algorithmus
- ein Algorithmus kann *immer* aus dem Binärabbild disassembliert werden
- aka *Security By Obscurity*
- $\rightarrow$ häufig inhärent unsicher (viele Beispiele)

  „Die besten Algorithmen sind diejenigen, die veröffentlicht, jahrelang von den weltbesten Kryptographen angegriffen und bislang nicht geknackt wurden“

Beispiel: RC4, Stromchiffre, die 7 Jahre lang geheim war, bis 1994 jemand anonym den Quelltext publizierte

Kryptanalyse

Voraussetzungen:

- Gegner hat vollständigen Zugang zur verschlüsselten Nachricht
- Kryptografischer Algorithmus ist bekannt.

Ziel: Ermittlung des Klartextes ohne Kenntnis des Schlüssels (oder Ermittlung des Schlüssels).

Algorithmen, deren Sicherheit von ihrer Geheimhaltung abhängen, sind *beschränkt* und sollten nicht eingesetzt werden.

Versuch der Kryptanalyse wird **Angriff** genannt.

1. Ciphertext-only-Angriff

Gegeben:

- Menge von chiffrierten Nachrichten
- $C_1 = E_k(P_1), C_2 = E_k(P_2), \ldots, C_i = E_k(P_i)$
- nichts weiter

Gesucht:

- $P_1, P_2, \ldots, P_i$ und k
- oder ein Algorithmus, um P_{i+1} aus $C_{i+1} = E_k(P_{i+1})$ abzuleiten

2. Known-plaintext-Angriff

Gegeben:

- Menge von chiffrierten Nachrichten sowie die dazugehörigen Klartexte
- $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), \ldots, P_i, C_i = E_k(P_i)$

Gesucht:

- k
- oder ein Algorithmus, um P_{i+1} aus $C_{i+1} = E_k(P_{i+1})$ abzuleiten

3. Chosen-plaintext-Angriff

Gegeben:

- $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), \ldots, P_i, C_i = E_k(P_i)$
- $P_1, P_2, \ldots, P_i$ kann durch den Analytiker vorgegeben werden

Gesucht:

- k
- oder ein Algorithmus, um P_{i+1} aus $C_{i+1} = E_k(P_{i+1})$ abzuleiten

Kann der Analytiker, den zu verschlüsselnden Klartext in Abhängigkeit vorangehender Verschlüsselungen variieren, so spricht man von *Adaptive-chosen-plaintext-Angriff*

4. Gummischlauch-Kryptanalyse

Der Analytiker bedroht, erpresst oder quält den Schlüsselbesitzer solange, bis dieser den Schlüssel verrät.

> *“a process for key discovery that he describes as ‘can take a surprisingly short time and is quite computationally inexpensive’.” (Quelle: http://groups.google.com/...)*

$\rightarrow$ so „gewonnene“ Erkenntnisse sind zumindest in Deutschland *nicht* gerichtsverwertbar („Früchte des vergifteten Baumes“).

Schlechte Verschlüsselung: XOR-Verschlüsselung

- symmetrisches Verfahren
- Klartext wird zeichenweise mit Schlüssel „ex-oder-iert“, also $C = P \oplus K$

x	y	$x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

Tabelle: Wahrheitstabelle der Exclusive-Or-Funktion (XOR, $x \oplus y$)

- Schlüssel wird immer wieder von vorn gelesen
- schnell, aber (sehr) unsicher

XOR-Verschlüsselung, cont'd

- Entschlüsselung mit gleichem Schlüssel, da

$$a \oplus k \oplus k = a \oplus 0 = a.$$

Problem: **Known-Plaintext-Angriff**

Bewertung:

> *„An XOR might keep your kid sister from reading your files, but it won't stop a cryptanalyst for more than a few minutes.“ (Bruce Schneier: Applied Cryptography)*

Eine nützliche Eigenschaft von XOR

Satz: Es sei A eine (beliebig verteilte) Zufallsvariable[1] über $\{0,1\}^n$ und X eine *gleichverteilte* Zufallsvariable über $\{0,1\}^n$. Dann ist $Y = A \oplus X$ stets eine *gleichverteilte* Zufallsvariable über $\{0,1\}^n$.

Beweisidee: Auftrittswahrscheinlichkeiten der Werte für A und X bei n=1:

A	Pr(A)
0	p_0
1	p_1

X	Pr(X)
0	0.5
1	0.5

, da gleichverteilt

$\rightsquigarrow$ Auftrittswahrscheinlichkeit der Werte für Y:

Y	Pr(Y)
0	$p_0 \cdot 0.5 + p_1 \cdot 0.5 = 0.5(p_0 + p_1) = 0.5$
1	0.5

[1] $\{0,1\}^n$ sei eine n Bit lange Binärzahl.

Perfekte Verschlüsselung: One-Time-Pads

aka Einmalblöcke

Eigenschaften:

- Schlüssel besteht aus zufälligen Zeichen und hat *gleiche Länge* wie Klartext
- Schlüssel darf nur *ein einziges Mal* genutzt werden
- Verschlüsselung: jedes Zeichen des Klartextes wird mit dem zugehörigen Zeichen des Schlüssels XOR-verknüpft
- Entschlüsselung: wie Verschlüsselung (gleicher Schlüssel)
- $\rightarrow$ symmetrisches Verfahren
- Jedes Zeichen des Schlüssels darf nur *ein einziges Mal* genutzt werden

Werden diese Eigenschaften zugesichert, so ist eine Kryptanalyse des Chiffrats **unmöglich**.

Angriffe auf One-Time-Pads

- Abfangen des Schlüssels
- Schlüssel nicht zufällig (z. B. pseudozufällig, d. h. computergeneriert)
- Mehrfachverwendung des Schlüssels

Literatur:
http://www.ranum.com/security/computer_security/papers/otp-faq/

Kryptografische Protokolle

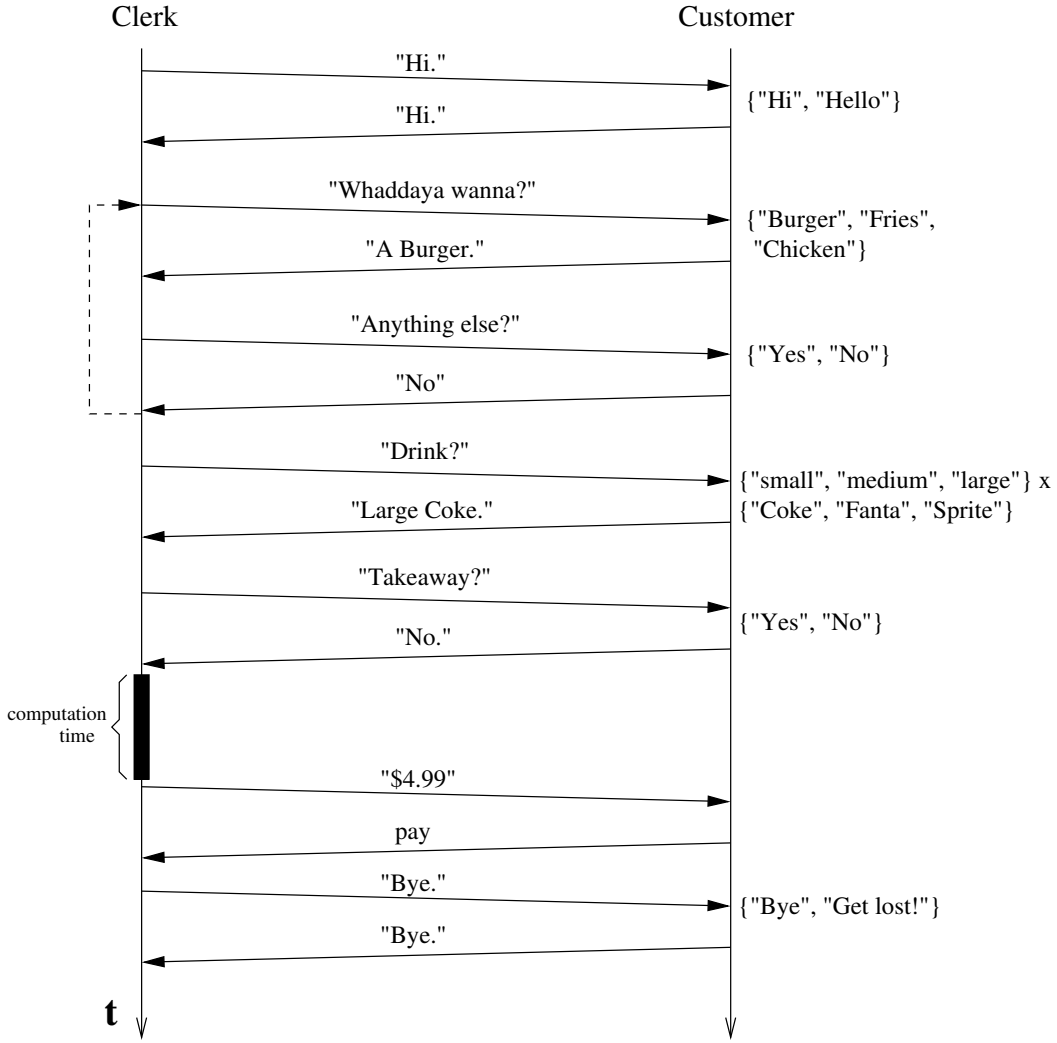
Begriff des Protokolls:

- beschreibt den dynamischen Aspekt einer Relation kommunizierender Komponenten
- beschreibt also den *Ablauf* der Kommunikation
- umgangssprachlich: eine Menge von „Wenn-Dann“-Beziehungen („Wenn Alice einen Schlüssel schickt, dann verschlüsselt Bob damit irgendwas. . . “)
- muss allen Teilnehmern bekannt sein
- darf keine Mehrdeutigkeiten enthalten
- erfordert (mindestens) zwei Teilnehmer

Der statische Aspekt der Relation wird durch die *Schnittstelle* beschrieben.

Beispiel eines Protokolls

Kommunikation eines Kunden mit dem *Clerk* bei McDonald's



Anstatt schwerfälliger Begriffsungetüme verwendet man für die Kennzeichnung der Kommunikationsparteien in der Kryptografie die folgenden Namen[2]:

Name	*Funktion*
Alice	Erste Teilnehmerin am Protokoll
Bob	Zweiter Teilnehmer am Protokoll
Carol	Dritte Teilnehmerin (wenn nötig)
Dave	Vierter Teilnehmer (wenn nötig)
Eve	Lauscherin (*eavesdropper*)
Mallory	Bösartiger aktiver Angreifer (*malicious*)
Trent	(vertrauenswürdiger) Treuhänder (*trust*)

[2] Egal, welches Krypto-Buch Sie aufschlagen

Kommunikation bei symmetrischen Verfahren

Prinzipieller Ablauf

1. Alice und Bob einigen sich auf ein Kryptosystem.
2. Alice und Bob vereinbaren einen Schlüssel K.
3. Alice chiffriert Klartext M mittels Schlüssel K und dem vereinbarten Algorithmus:

$$C = E_K(M)$$

4. Alice sendet Chiffretext-Nachricht C an Bob.
5. Bob dechiffriert Chiffretext mittels desselben Algorithmus und Schlüssels und liest den Klartext:

$$M = D_K(C) = D_K(E_K(M))$$

Analogie: Safe, zu dem mehrere Personen Zugang haben.

Kommunikation bei symmetrischen Verfahren

Störungsmöglichkeiten

- Eve kann durch Belauschen von 2. den Schlüssel abfangen
  - kann danach alle Nachrichten von Alice an Bob mitlesen
- Mallory kann alles was Eve kann und zusätzlich
  - Nachrichten von Alice abfangen (diese erreichen Bob nie)
  - Nachrichten fälschen (indem er eigene Nachrichten mit dem gestohlenen Schlüssel verschlüsselt und einspeist)

d. h., Sicherheit des Verfahrens hängt *maßgeblich* von Geheimhaltung des Schlüssels ab

Kommunikation bei symmetrischen Verfahren

(systemimmanente) Nachteile

- Verteilung unter Geheimhaltung des Schlüssels ist aufwändig/teuer/riskant.
- kompromittierter Schlüssel erlaubt das Mitlesen und Fälschen von Nachrichten
- da jeweils 2 Partner einen Schlüssel benötigen, wächst die nötige Schlüsselanzahl quadratisch mit der Teilnehmerzahl

  Für $n = 100$ Teilnehmer benötigt man

$$\frac{n(n-1)}{2} = 4950 \text{ Schlüssel.}$$

Kommunikation bei symmetrischen Verfahren

(systemimmanente) Nachteile

- Verteilung unter Geheimhaltung des Schlüssels ist aufwändig/teuer/riskant.
- kompromittierter Schlüssel erlaubt das Mitlesen und Fälschen von Nachrichten
- da jeweils 2 Partner einen Schlüssel benötigen, wächst die nötige Schlüsselanzahl quadratisch mit der Teilnehmerzahl

  Für $n = 100$ Teilnehmer benötigt man

$$\frac{n(n-1)}{2} = 4950 \text{ Schlüssel.}$$

Kommunikation mit Public-Key-Kryptografie

- erfordert für jeden Teilnehmer genau *zwei* Schlüssel
  - einen *öffentlichen* zum Verschlüsseln
  - einen *privaten* zum Entschlüsseln
- privater Schlüssel kann nicht[3] aus dem öffentlichen errechnet werden
- jeder kann öffentlichen Schlüssel nutzen, um etwas zu verschlüsseln
- nur der Besitzer des privaten Schlüssels kann dieses wieder entschlüsseln
- Analogie: Briefkasten (am Haus)

[3] besser gesagt, nur sehr sehr schwer

Kommunikation mit Public-Key-Kryptografie

Prinzipieller Ablauf

1. Alice und Bob einigen sich auf ein Kryptosystem mit öffentlichem Schlüssel.
2. Bob macht Alice seinen öffentlichen Schlüssel E_{K_B}[4] zugänglich.
3. Alice chiffriert ihre Nachricht mit E_{K_B}:

$$C = E_{K_B}(M).$$

4. Alice schickt C an Bob.
5. Bob dechiffriert C mittels seines privaten Schlüssels D_{K_B}

$$M = D_{K_B}(C).$$

Das Problem der Schlüsselübermittlung ist gelöst!

[4] Der öffentliche Schlüssel kann nur zum *Ver*schlüsseln verwendet werden, daher bezeichnen wir wir ihn mit E.

Kommunikation mit Public-Key-Kryptografie

(systemimmanente) Nachteile

- ca. um den Faktor 1000 langsamer als symmetrische Verfahren
- durch *chosen-plaintext*-Angriffe gefährdet, wenn Anzahl möglicher Nachrichten gering
  - da öffentlicher Schlüssel bekannt, kann man „durchprobieren“ und zu einem Chiffrat den zugehörigen Klartext ermitteln
  - funktioniert bei symm. Verfahren nicht, da Schlüssel dem Angreifer unbekannt

$\rightarrow$ Kombination symmetrischer und asymmetrischer Verfahren (aka hybride Kryptosysteme)

Hybride Kryptosysteme

Prinzipieller Ablauf

1. Bob übermittelt Alice seinen öffentlichen Schlüssel E_{K_B}.
2. Alice generiert einen zufälligen Sitzungsschlüssel K und chiffriert ihn mit E_{K_B}.

$$C = E_{K_B}(K)$$

3. Alice übermittelt C an Bob.
4. Bob entschlüsselt die Nachricht C mit seinem privaten Schlüssel und erhält den Sitzungsschlüssel.

$$K = D_{K_B}(C)$$

5. Beide verschlüsseln ihre Kommunikation nun symmetrisch mit K, dem Sitzungsschlüssel.

Hybride Kryptosysteme

Fazit

- Public-Key-Kryptografie dient hier zum sicheren Schlüsseltransport
- Schlüsselverwaltungsproblem also auch gelöst
- Kommunikation trotzdem effizient, da symmetrisch verschlüsselt
- Flexibilisierung: Schlüssel kann jederzeit aufwandsarm ersetzt werden (z. B. bei Kompromittierung)
- Angriffsmöglichkeit: bei der initialen Übermittlung der öffentlichen Schlüssel

Zusammenfassung: Was haben wir gelernt?

1. historische Verfahren (Transpositions- vs. Substitionschiffren)
2. Vigenère-Verschlüsselung, Einsatz und Kryptanalyse
3. Kerckhoffs'sches Prinzip eines 'guten' Kryptosystems
4. 4 Typen Angriffe auf Kryptosysteme
5. symmetrische vs. asymmetrische Kryptografie
6. Perfekte Verschlüsselung mit One-Time-Pads
7. Wer sind Alice und Bob?