Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Einführung IT Security

Kapitel 1

Inhalte

Kapitel 1: Grundlagen & Begriffe

- Sicherheit & Schutzziele
- Kryptologie, Kryptografie, Steganografie
- Geschichte der Kryptografie
- Kerckhoffs'sches Prinzip
- Entropie
- Algorithmus & Protokoll

Image by 8385 from Pixabay

Inhalte

Kapitel 2: Verschlüsselungsverfahren

- symmetrische Verschlüsselung
- Stromchiffren, One Time Pad
- Blockchiffren: Betriebsmodi
- asymmetrische Verschlüsselung
- Schlüsselaustausch
- Snake Oil

Image by 8385 from Pixabay

Inhalte

Kapitel 3: kryptografische Bausteine

- Hashfunktionen
- Digitale Signaturen
- PKI
- MAC, HMAC

Image by 8385 from Pixabay

Kapitel 4: Authentifizierung & Zugriffskontrolle

- Identifizierung, Authentifizierung
- Passwörter
- Zugriffskontrollparadigmen

Image by 8385 from Pixabay

Inhalte

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Kapitel 5: Protokolle

- SSH
- TLS

Image by 8385 from Pixabay

Kapitel 6: Weiterführende Konzepte

- Schwachstellen
- Malware
- Verfügbarkeit, Backup
- ISMS
- Risikomanagement

Image by 8385 from Pixabay

Grundlagen & Begriffe

Die Zukunft ist digital!

analog / physisch

- gewohnt
- langsam
- physische Objekte
- Kopieren verlustbehaftet

digital

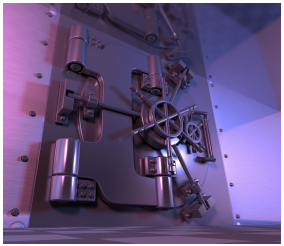
- „alles ist besser“
- neu & ungewohnt
- Information
- Kopieren verlustfrei

Sicherheit

Safety
Betriebssicherheit

Schutz gegen Unfälle und Naturgewalten

Security
„Schutz“



Schutz gegen zielgerichtete Angriffe

Image by 8385 from Pixabay

Warum ist Sicherheit so kompliziert?

- Sicherheit ist komplex
- Sicherheit ist fragil
- Sicherheit ist kostspielig

Was heißt sicher?

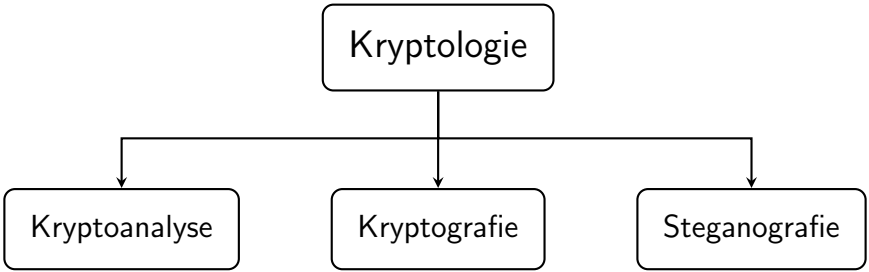
Vertraulichkeit	**C**	Confidentiality
Integrität	**I**	Integrity
Verfügbarkeit	**A**	Availability

Vertraulichkeit	Schutz gegen unbefugte Kenntnisnahme
Integrität	Schutz gegen unbemerkte Veränderung
Verfügbarkeit	Schutz gegen Beeinträchtigung und Ausfall

Schutzziele

Authentizität	Authenticity
Verbindlichkeit	Nonrepudiation
Abstreitbarkeit	Deniability
Anonymität	Anonymity
Fairness	Fairness

Geschichte der Kryptologie



Wissenschaft der Geheimschriften

umfasst

- Kryptografie
- Kryptoanalyse
- Steganografie

Image by 8385 from Pixabay

Verschlüsselung von Informationen

Verschlüsselung durch

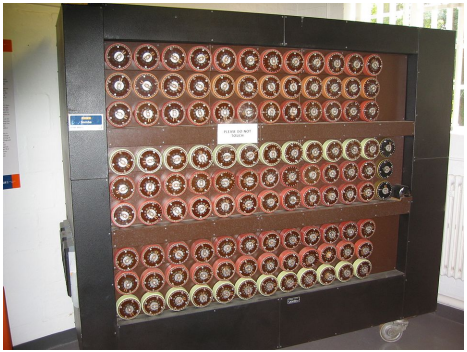
- Transposition
- Substitution

By ArnoldReinhold - Own work

unberechtigte Entschlüsselung

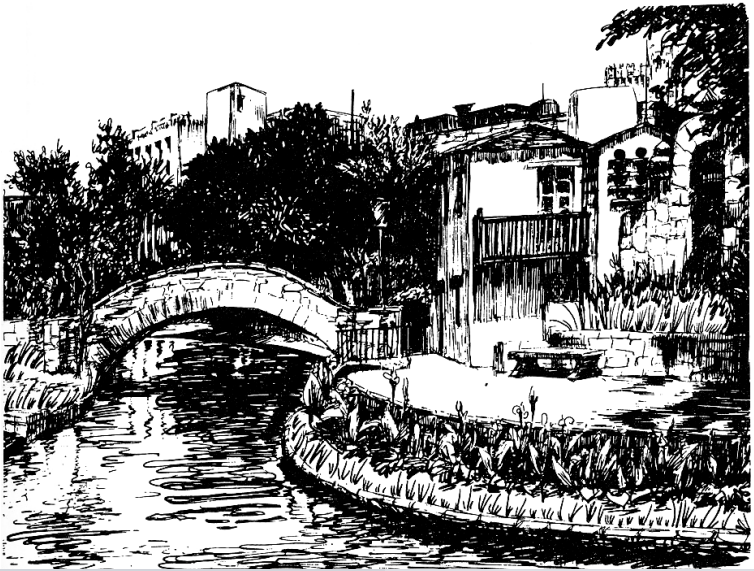
historisch: Linguisten

heute: Mathematiker & Informatiker



Verborgene Übermittlung von Nachrichten

Das Ziel der Steganografie ist es, das Vorhandensein einer Nachricht zu verbergen, so dass die Übermittlung unbemerkt bleibt.



Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Digitale Wasserzeichen

digital watermarking

Das Ziel von *digital watermarking* ist es, dass das digitale Wasserzeichen unbemerkt bleibt und bei der Wiedergabe der Dateiinhalte den Benutzer nicht stört.

By Manfred Sauke - Own work, ECB decisions ECB/2003/4 and ECB/2003/5

Chiffre

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Transposition

Reihenfolge der Zeichen einer Nachricht wird verändert

Beispiel *Skytale*

Substitution

jedes Zeichen einer Nachricht wird ersetzt

Beispiel *Caesar-Chiffre*

monoalphabetische Substitution:

Ersetzung ist immer gleich

By photographer: Anderson / Alfred von Domaszewski

Beispiel für Chiffrat einer monoalphabetischen Substitutionschiffre:

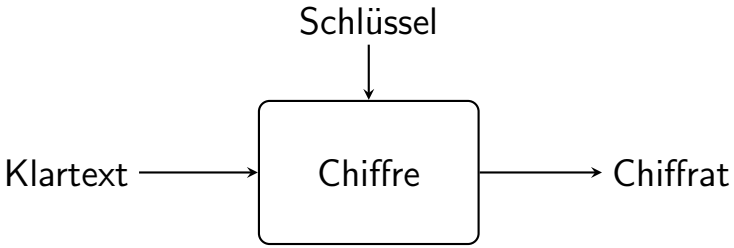
TDB OZBPYDB XDBMBYO RDBX, LSBY TBU ABZBDUIDG TBG LXOBI SYDIAO GDB KIG TPQZ IDQZO ILBZBY. FBTBIMLXXG SDI DQZ KBSBYHBKAO TLRPI, TLGG TBY IDQZO CKBYMBXO.

Kryptoanalyse mit CrypTool Online

Kerckhoffs'sche Prinzip

Schlüssellose Verfahren: Ver- und Entschlüsselung sind festgelegt. Im Falle eines Bruchs, z. B. durch Bekanntwerden der Chiffre, muss die komplette Chiffre getauscht werden.

Kerckhoffs'sche Prinzip



Kerckhoffs'sche Prinzip

Auguste Kerckhoffs (1835 – 1903)

Kerckhoffs'sche Prinzip:

Die Sicherheit einer Chiffre darf nicht auf Ihrer Geheimhaltung beruhen.

Eugen Drezen, Historio de la Mondo Lingvo

Steganografie und Kerckhoffs'sches Prinzip

Steganografie verstößt gegen das Kerckhoffs'sche Prinzip und spielt in der modernen Kryptografie nur eine untergeordnete Rolle.

Eugen Drezen, Historio de la Mondo Lingvo

Substitutionschiffre

Vigenère-Chiffre

- Giovan Bellaso 1553
- später Blaise de Vigenère zugeschrieben
- polyalphabetische Substitutionschiffre
- erst im 19. Jhd. gebrochen

By Thomas de Leu - Woodcut Photograph

Vigenère-Chiffre

- Giovan Bellaso 1553
- später Blaise de Vigenère zugeschrieben
- polyalphabetische Substitutionschiffre
- erst im 19. Jhd. gebrochen

	k	l	a	r	t	e	x	t
+	**G**	**E**	**H**	**E**	**I**	**M**	G	E
	Q	P	H	V	B	Q	D	X

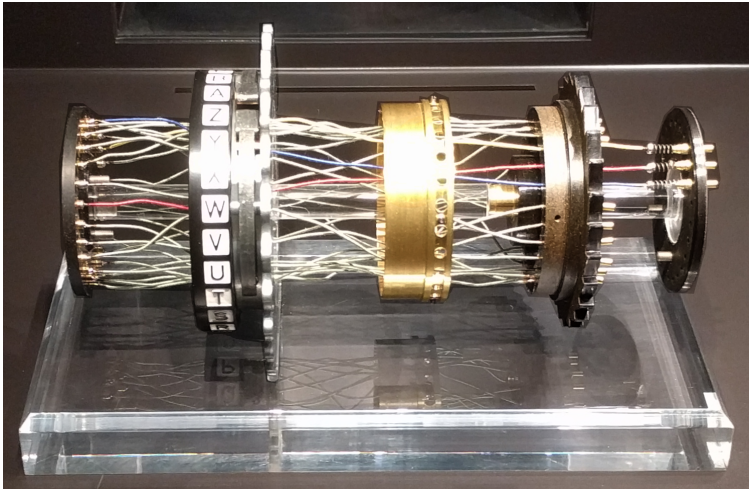
Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

d	i	e	s	i	s	t	e	i	n	b	e	i	s	p	i	e	l	t	e	x	t
G	**E**	**H**	**E**	**I**	**M**	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E
J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E	X
J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E	X
X	J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E

Enigma

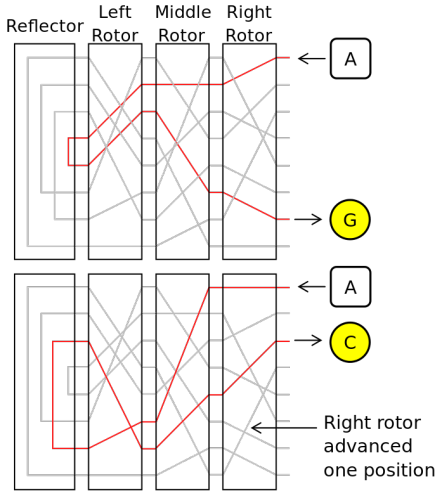
By Greg Goebel - Web page Image

Funktionsweise Enigma



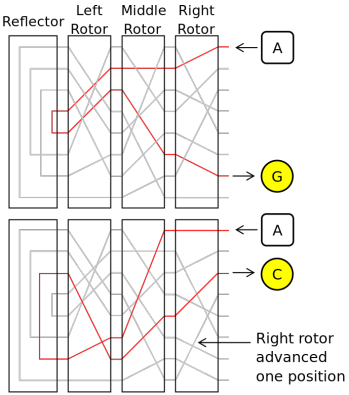
eigenes Foto, Deutsches Museum

Funktionsweise Enigma



Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

Schwäche der Enigma



Verschlüsselung: fixpunktfreie Permutation

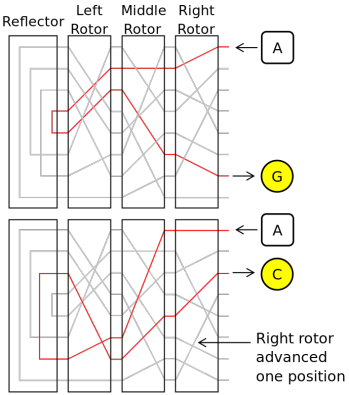
Chiffrat	JFGNB	PSSNK	EFX
Kandidat 1	ANGRI	FFSOF	ORT
Kandidat 2	RUECK	ZUGJE	TZT

Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

Erwarten Sie einen Angriff oder einen Rückzug?

Chiffrat	JFGNB	PSSNK	EFX
Kandidat 1	ANGRI	FFSOF	ORT
Kandidat 2	RUECK	ZUGJE	TZT

Schwäche der Enigma



Verschlüsselung: fixpunktfreie Permutation

Chiffrat	JFGNB	PSSNK	EFX
Kandidat 1	ANGRI	FFSOF	ORT
Kandidat 2	RUECK	ZUGJE	TZT

Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt (*known plaintext*)
4. gewählter Klartext (*chosen plaintext*)
5. Entschlüsselungsorakel (*chosen ciphertext*)

Ziel des Angreifers

1. ohne Schlüssel entschlüsseln (*totaler Bruch*)
2. einen Schlüssel herausfinden
3. ein Chiffrat entschlüsseln
4. zwei bekannte Klartexte unterscheiden
5. zwei gewählte Klartexte unterscheiden

Paradigmenwechsel der Kryptologie

Die Enigma markierte das Ende der klassischen Kryptologie und den Beginn der modernen Kryptologie.

1910er & 1920er (elektro-)mechanische Chiffriermaschinen

1920er & 1930er Kommerzialisierung & zivile Nutzung

1930er & 1940er Kryptoanalyse: Linguisten $\rightarrow$ Mathematiker

Moderne Kryptologie

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

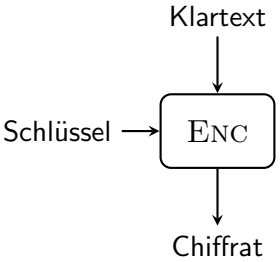
	symmetrische Kryptologie	**asymmetrische Kryptologie**
Vertraulichkeit	symmetrische Verschlüsselung	asymmetrische Verschlüsselung
Integrität	MAC	Signaturen
Authentizität		PKI
Schlüsselaustausch	symmetrischer Schlüsselaustausch	asymmetrischer Schlüsselaustausch
Kryptoanalyse	symmetrische Kryptoanalyse	Mathematik
	Implementierungsangriffe	
	Seitenkanalanalyse	
Bausteine	Hashfunktionen ⋮	⋮

Moderne Kryptologie

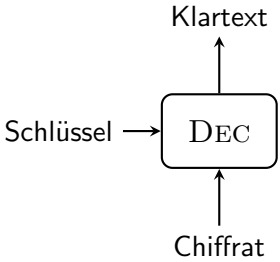
Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

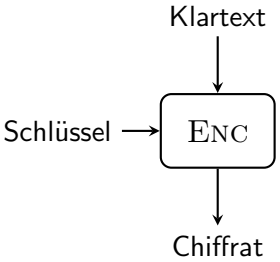
	symmetrische Kryptologie	**asymmetrische Kryptologie**
Vertraulichkeit	symmetrische Verschlüsselung	asymmetrische Verschlüsselung
Integrität	MAC	Signaturen
Authentizität		PKI
Schlüsselaustausch	symmetrischer Schlüsselaustausch	asymmetrischer Schlüsselaustausch
Kryptoanalyse	symmetrische Kryptoanalyse	Mathematik
	Implementierungsangriffe	
	Seitenkanalanalyse	
Bausteine	Hashfunktionen	
	⋮	⋮

Verschlüsselung



Entschlüsselung



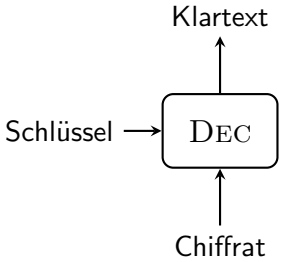


Verschlüsselung

- kombiniert Klartext mit Schlüssel
- erzeugt Chiffrat (oder Chiffretext)

Entschlüsselung

- kombiniert Chiffrat mit Schlüssel
- erzeugt Klartext
- Entschlüsselung ohne Schlüssel ist schwer



Schlüssel

- gleicher Schlüssel für Ver- und Entschlüsselung
- unstrukturierter Bitstring
- (fast) jeder Bitstring (entsprechender Länge) ist gültiger Schlüssel
- Länge entspricht Komplexität

Image by 8385 from Pixabay

Was ist $\log_2 8$?

$\log_2 8 = 3$ denn $2^3 = 8$.

Eigenschaften den Logarithmus:

- $\log(a \cdot b) = \log a + \log b$
- $\log a^x = x \cdot \log a$
- $\log \frac{1}{a} = -\log a$

Wie viel Entropie enthält eine Zeichenkette?

- Was ist Entropie?
- Wie viel Entropie enthält ein Zeichen?
- Wie berechnet sich die Entropie einer Zeichenkette?

Image by OpenClipart-Vectors from Pixabay

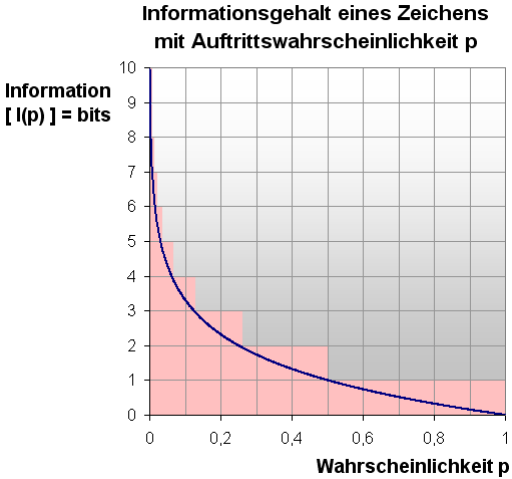
Informationsgehalt I eines Zeichens z

$$I(z) = -\log_2 p_z \qquad p_z : \text{ Wahrscheinlichkeit von } z$$

Beispiel: fairer Münzwurf $\rightarrow I(\text{‘Zahl’}) = 1$ Bit

Beispiel: Würfelwurf $\rightarrow I(\text{‘6’}) \approx 2,6$ Bit

Entropie



von Akribix - Eigenes Werk

Entropie

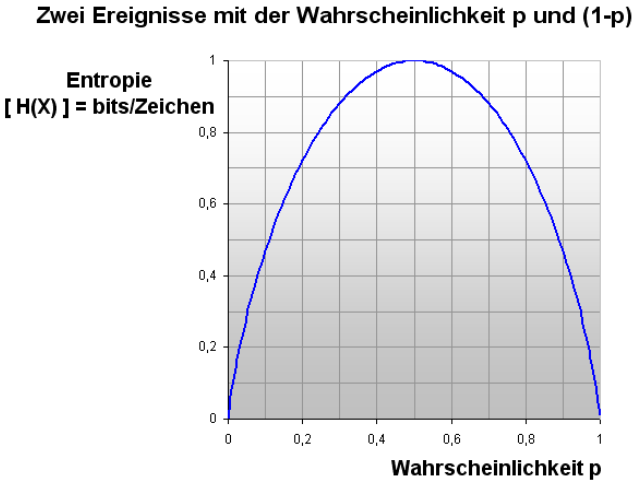
Entropie einer Quelle ist der erwartete (mittlere) Informationsgehalt eines Zeichens

$$H = \mathbb{E}[I] = \sum_z p_z \cdot I(z) = -\sum_z p_z \cdot \log_2 p_z$$

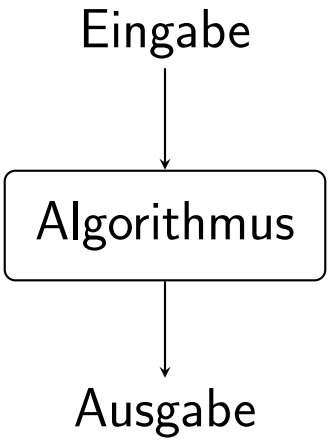
Sonderfall: alle n Zeichen gleich wahrscheinlich:

$$H = -\log_2 \frac{1}{n} = \log_2 n$$

Entropie



von Akribix - Eigenes Werk


Eingabe
Algorithmus
Ausgabe

Ein Algorithmus ist eine Liste von

- endlich vielen,
- wohldefinierten

(Rechen-)Schritten zur Lösung einer Klasse von Problemen.

Eigenschaften eines Algorithmus

Finitheit	endliche, eindeutige Beschreibung
Ausführbarkeit	konkrete, wohldefinierte Schritte
Determinismus	nächster Schritt eindeutig bestimmt (auch Vollständigkeit)
Determiniertheit	identische Eingabe $\rightarrow$ gleiche Ausgabe

Ein Algorithmus besitzt

- eine Eingabe und
- eine Ausgabe (wenn er terminiert)

Probabilistische Algorithmen

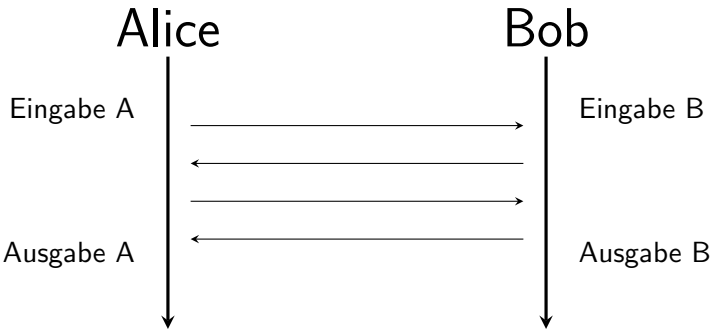
- Ausgabe hängt vom Zufall ab

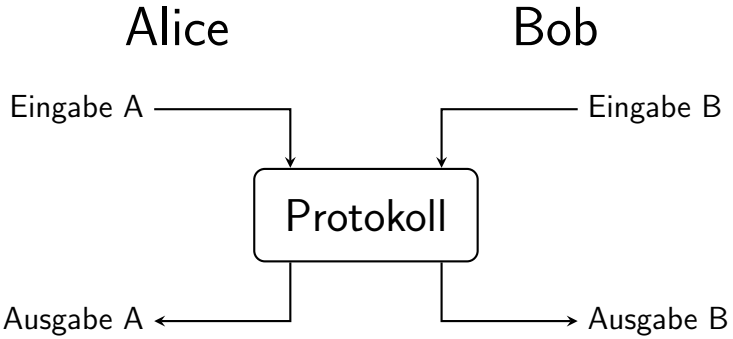
Deterministische Algorithmen

- Ausgabe folgt deterministisch (eindeutig festgelegt) aus den Eingaben

Zufall wird als eigene Eingabe des Algorithmus betrachtet und für den Lauf unverändert festgelegt.

Damit ist ein probabilistischer Algorithmus deterministisch.


Alice
Bob
Eingabe A
Eingabe B
Ausgabe A
Ausgabe B


Alice
Bob
Eingabe A
Eingabe B
Protokoll
Ausgabe A
Ausgabe B

Ein Protokoll ist eine Liste von

- endlich vielen,
- wohldefinierten

(Rechen-)Schritten und Regeln für den Nachrichtenaustausch zur Lösung einer Klasse von Problemen.

Eigenschaften eines Protokolls

Finitheit	endliche, eindeutige Beschreibung, die jedem Teilnehmer bekannt ist
Ausführbarkeit	konkrete, wohldefinierte Schritte
Determinismus	nächster Schritt für jeden Teilnehmer eindeutig bestimmt
Determiniertheit	identische Eingabe $\rightarrow$ gleiche Ausgabe

Ein Protokoll besitzt für jede Partei

- eine Eingabe und
- eine Ausgabe (wenn es terminiert).

Ein Protokoll ist ein „interaktiver Algorithmus“.

Protokollparteien

Parteien

Alice

Bob

Carol

Dave

Angreifer

Eve – eavesdropping (Lauscher)

Mallory – malicious (boshaft)