IT-Sicherheit: Verschlüsselung

Kryptographie

Von „Kryptos“ (geheim, verborgen) + „graphein“ (schreiben)

= geheimes Schreiben

Eine Datenmenge wird durch Anwendung eines Schlüssels nach Vorgaben eines Algorithmus’ so in eine andere Datenmenge überführt, dass nur von berechtigten Personen die Ursprungsmenge wieder hergestellt werden kann.

Schlüssel & Algorithmus

Schlüssel

- Eine Information, die in irgendeiner Form mit dem Klartext verbunden wird, um das Chiffrat zu erzeugen
- Im digitalen Bereich: Eine binäre Datei (also eine Folge aus 1 und 0)

Algorithmus

- Vorschrift, die angibt, in welcher Weise der Schlüssel mit dem Klartext kombiniert werden soll.
- Digital also: Wie sollen die Bits im Klartext mit den Bits im Schlüssel verknüpft werden?

ROT 13 & Co

Was ist bei einer Buchstabenvertauschung wie ROT 13 der Algorithmus, was der Schlüssel?

- Algorithmus: Vertausche jeden Buchstaben mit seinem *n*-ten Nachfolger
- Schlüssel: *n* (bei ROT-13 also 13)

Was ist bei einer Transposition der Algorithmus, was der Schlüssel?

- Algorithmus: Entferne alle Leer- und Satzzeichen, schreibe alles groß, nimm, ausgehend vom ersten Buchstaben, jeweils den *n*-ten Buchstaben.
- Schlüssel z.B. 5: Immer den 5ten-Buchstaben

Sicherheit von ROT-13 & Co

Woran hängt die Sicherheit von ROT-13 & Co, was also darf ein Angreifer auf keinen Fall wissen?

- Das *Verfahren* (= der Algorithmus) darf nicht bekannt werden, ansonsten ist der Schlüssel durch bloßes Ausprobieren zu erraten

Warum sind diese Systeme extrem unsicher?

- Das Verfahren ist leicht zu erraten

Welche Konsequenzen hat es, wenn sie geknackt werden?

- Das komplette System ist betroffen, das Verfahren muss gewechselt werden (extrem aufwendig bis manchmal unmöglich)

Auguste Kerckhoffs von Nieuwenhof

Jean Guillaume Auguste Victor François Hubert Kerckhoffs von Nieuwenhof; (1835–1903), niederländischer Mathematiker, Linguist und Kryptologe

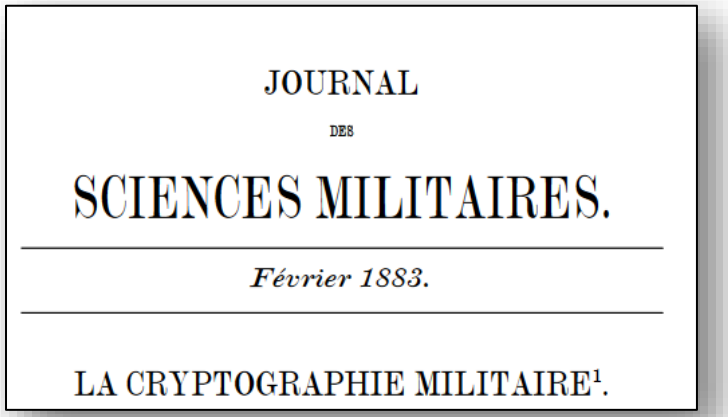
Schrieb *La Cryptograhie militaire* (Februar 1883)

Definiert sechs Prinzipien, denen ein sicheres Kryptosystem gehorchen muss

Eines davon ist als „Kerckhoffs' Prinzip" bis heute gültig



Kerckhoffs' Prinzip


JOURNAL
DES
SCIENCES MILITAIRES.
Février 1883.
LA CRYPTOGRAPHIE MILITAIRE[1].

Das zweite von sechs Prinzipien, heute eine zentrale Forderung an Kryptosysteme:

„2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi "

2. [Das System] darf keine Geheimhaltung verlangen und muss ohne Schwierigkeiten in die Hände des Feindes fallen können

Die Sicherheit eines Kryptosystems darf also *nicht* – wie bei ROT 13 & Co – von der Geheimhaltung des **Verfahrens** abhängen

Die Sicherheit gründet auf der Geheimhaltung des **Schlüssels**

Das **Verfahren** (= der Algorithmus) ist öffentlich bekannt

Der **Schlüssel** wird geheim gehalten

Gründe für Kerckhoffs' Prinzip

Es ist leichter, einen Schlüssel geheim zu halten als das Verfahren

Es ist einfacher, einen Schlüssel zu tauschen als ein Verfahren

Hängt die Sicherheit von der *Geheimhaltung des Verfahrens* ab und wird dieses bekannt, ist das gesamte System kompromittiert

Hängt die Sicherheit von der *Geheimhaltung des Schlüssels* ab, kann das System bestehen bleiben, es muss nur der Schlüssel getauscht werden

Peer Review des Verfahrens

Keine Möglichkeit für geheime Backdoors

Historisches Beispiel

Kerckhoffs' Prinzip klingt absurd bzw. nicht einlösbar – aber es gibt ein historisches Verfahren, das dem Prinzip gehorcht, die „Vigenère-Chiffre“

1508 von Johannes Trithemius (1462–1516) entwickelt

1585 von Blaise de Vigenère (1523–1596) weiterentwickelt (geriet in Vergessenheit)

Schlüsselbuchstabe

Klartextbuchstabe

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Vigenère-Chiffre

Erweiterung der „Cäsar-Chiffre“: 26 Alphabete für 26 Buchstaben

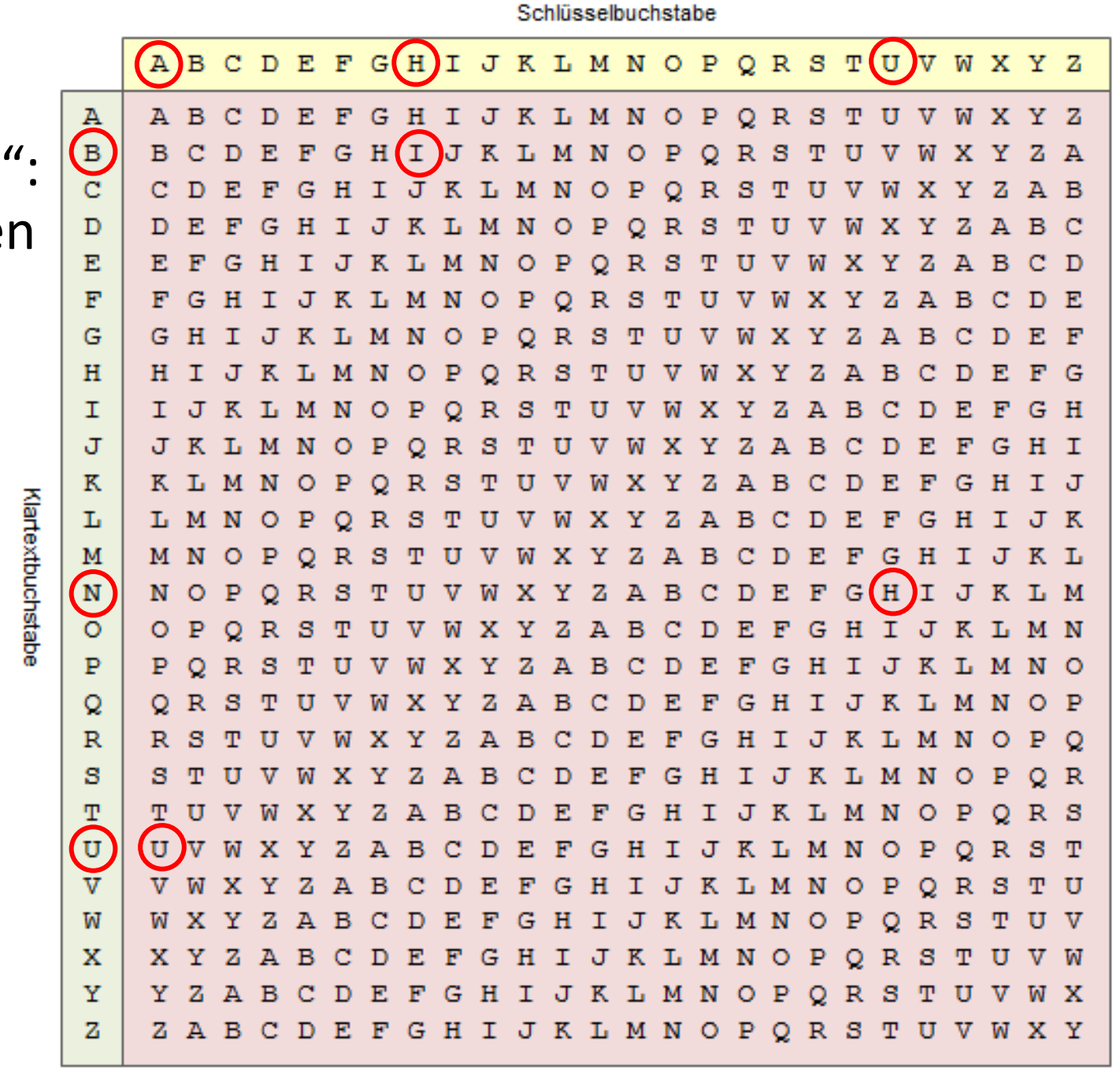
Schlüssel: HAUS

Klartext: BUNDESWEHR

BUNDESWEHR
HAUSHAUSHA

IUHVLSQWOR

Ohne Kenntnis des Schlüssels nur sehr schwer zu brechen – selbst wenn das Verfahren bekannt ist



Enigma: Polyalphabetische Substition

Quelle: Wikipedia





Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

№ 00014

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
0	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
0	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
0	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
0	28.	II	III	IV	05	03	12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AF	ioy	kjv	ykc	fpz
0	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BF	RV	ggf	jus	lrs	glc
0	26.	II	V	I	15	09	06	DS	UL	ZJ	OI	HN	FT	RK	YC	XQ	GB	crl	rht	ksz	ego
0	25.	V	IV	III	26	07	18	WA	QD	XS	UY	LG	JI	FB	HK	MT	CE	pfr	ijw	zgg	ygj
0	24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	FR	AS	nbt	pvd	eqo	wyn
0	23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
0	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	PA	MO	jlw	vrh	vya	pbf
0	21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zit	jlc	jbl	pvi
0	20.	V	II	III	07	18	04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	ctx	gns	xeg	nvo
0	19.	IV	V	I	08	09	22	IT	YK	BL	RZ	VP	FN	JW	QO	MS	AE	lyx	jua	zju	nss
0	18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
0	17.	III	V	I	11	22	16	GY	JN	SF	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	fug
0	16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	FS	HP	afp	uah	tpn	npf
0	15.	II	V	III	03	20	14	JD	BM	XR	LG	PC	OF	ZI	YH	VK	EW	nfk	pvm	vue	cpr
0	14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MC	zgc	cmz	pdf	xuq
0	13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	MQ	VH	FT	UL	RE	zor	ccm	odl	ijs
0	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JF	AX	eqk	whq	avc	zpf
0	11.	V	II	I	08	20	14	HV	FP	CM	AJ	OU	YB	WS	NT	GK	EZ	hvm	icd	nxo	yxk
0	10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	OU	EB	FL	MY	HD	bgd	xka	gsg	sgs
0	9.	III	I	II	14	16	06	LN	IK	HS	DB	TX	CG	WY	EV	OF	RA	myh	ncz	xvx	ees
0	8.	IV	III	I	09	18	14	RG	XU	WZ	AP	LF	IY	SQ	DO	VJ	HT	ooq	xeo	ocn	kde
0	7.	II	I	V	18	13	24	EK	RO	JX	WV	HS	QP	BZ	MU	TN	CA	fmc	mkh	lhe	tmq
0	6.	III	II	IV	23	01	17	DC	VG	OL	UA	EK	ZH	YX	PW	IM	RF	tlc	wbj	sre	kid
0	5.	V	III	I	19	23	15	QP	DG	ZJ	NK	SB	IC	FT	ER	UV	HA	hnp	wla		
0	4.	IV	II	V	26	04	03	MX	QO	HI	TB	GA	KP	LZ	CS	WJ	NV	clc	jdh		

Quelle: Wikipedia

Blockverschlüsselung

Die Vigenère-Chiffre ist ein Beispiel für eine *Blockverschlüsselung*

Ein fester Block Klartext wird mit einem Schlüssel kombiniert

Schlüssellänge üblicherweise 64 bis 256 Bit

Die Verfahren sind bekannt, der Schlüssel wird geheim gehalten

Je kürzer der Schlüssel, desto leichter ist die Entschlüsselung

Moderne Verfahren mit 256-Bit-Schlüsseln gelten als praktisch nicht zu knacken

Praktisch = nicht in angemessener Zeit und mit angemessenen Ressourcen

Stromverschlüsselung

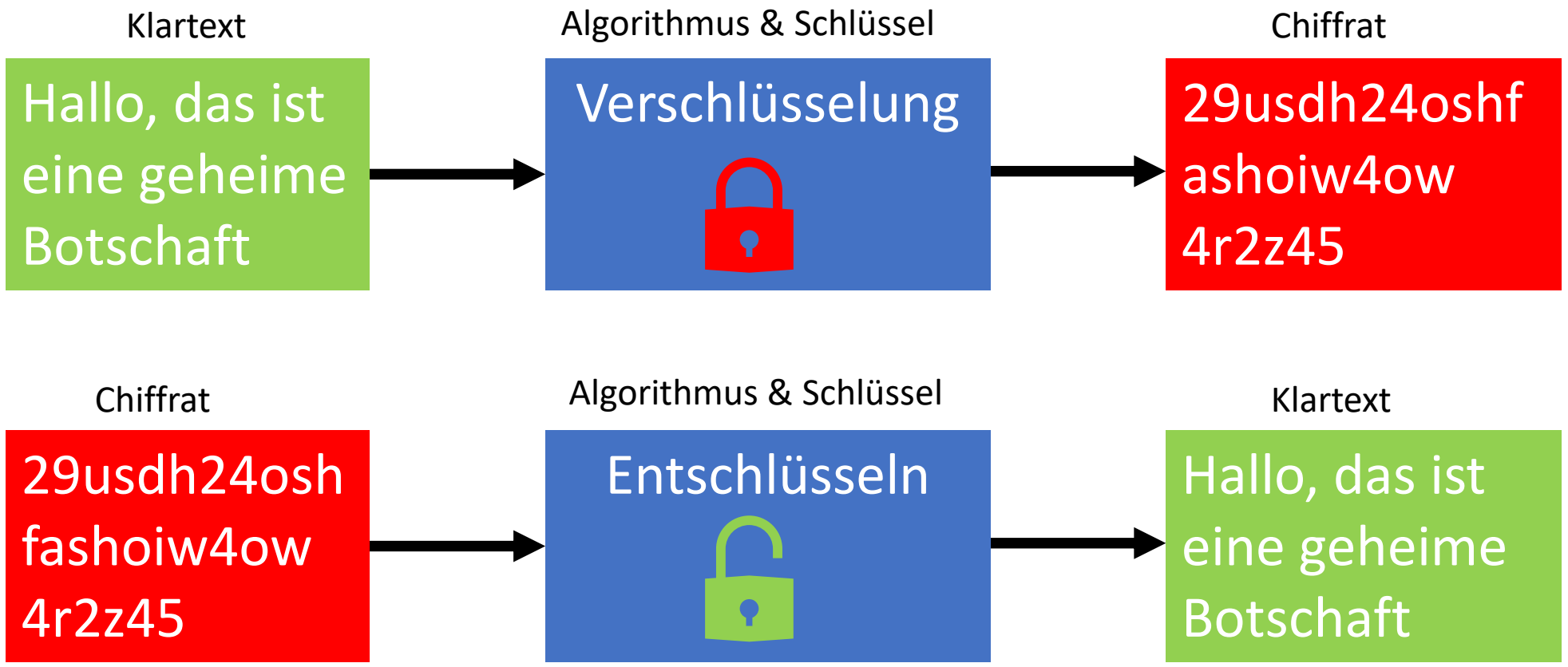
Ein unabgeschlossener Klartext (z.B. gestreamte Informationen) wird mit einem ad hoc erzeugten Schlüsselstrom verschlüsselt

Schlüsselstrom: pseudozufälliger Datenstrom

Wird meistens von einem Schlüssel abgeleitet, es gibt aber auch andere, komplexere Verfahren

Verknüpfung der Bits im Klartext mit den Bits im Chiffrat üblicherweise mit XOR

Verschlüsseln / Entschlüsseln



Symmetrische Verschlüsselung

Zum Ver- und Entschlüsseln wird derselbe Schlüssel benutzt

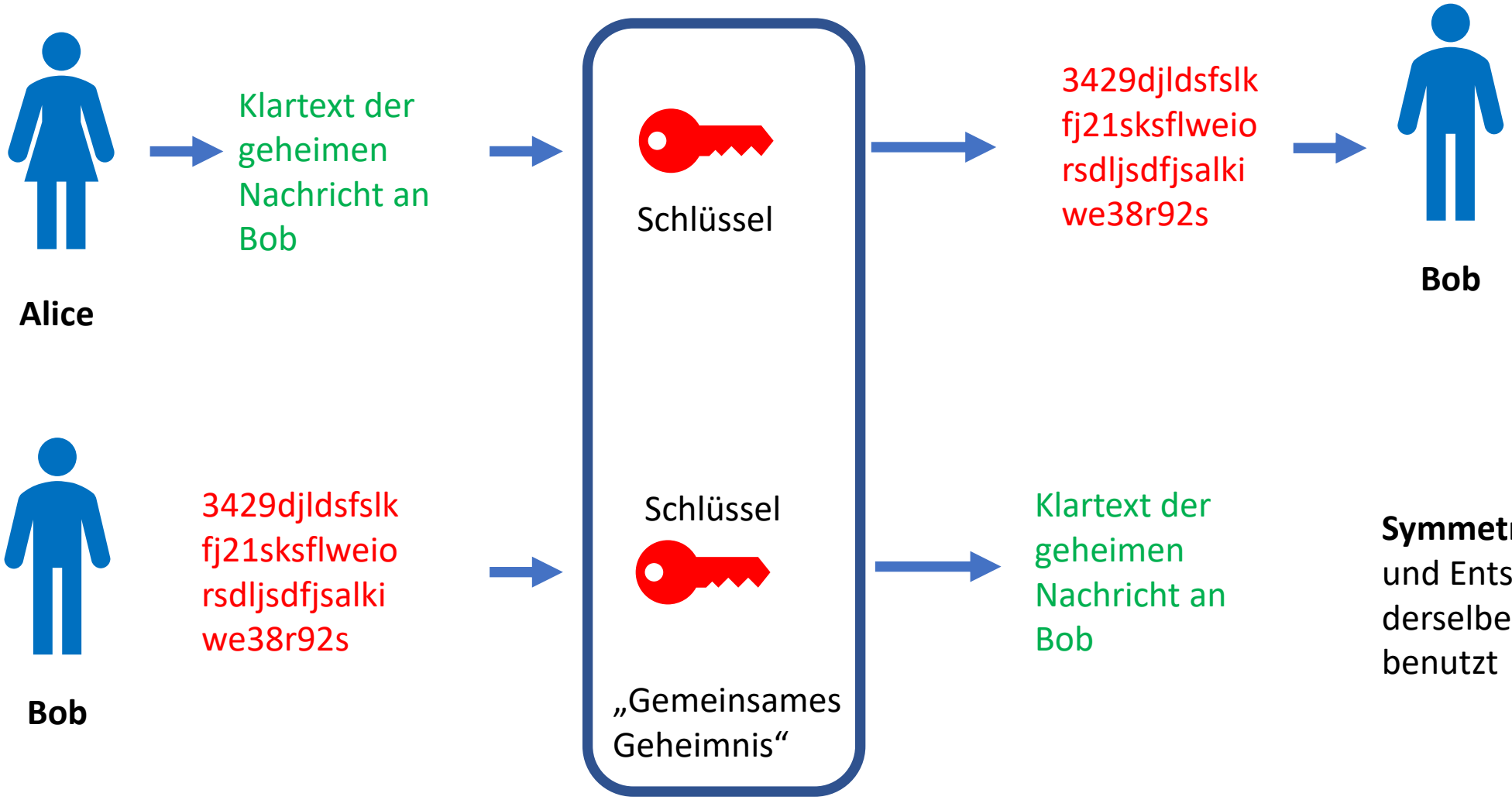
Vorteile

- Einfach (in der Anwendung, im Verständnis, in der Implementation)
- Schnell (basiert im Prinzip auf Bitoperationen, die jede CPU von Haus aus mit maximaler Geschwindigkeit ausführt)

Nachteile

- Der Schlüssel muss sicher getauscht werden („gemeinsames Geheimnis“, „shared secret“, „pre-shared key“)

Symmetrische Verschlüsselung



Symmetrisch: Zum Ver- und Entschlüsseln wird derselbe Schlüssel benutzt

Symmetrische Verfahren (DES, 3DES, AES)

DES (Data Encryption Standard)

- Mitte der 70er Jahre von IBM entwickelt
- 64-Bit-Blöcke, Schlüssellänge: 56 Bit
- Hält einem Brute-Force-Angriff nicht stand
- Wurde im Juli 1998 in 56 Stunden geknackt, Januar 1999 in rd. 23 Stunden

3DES (Triple DES)

- Nachfolger von DES, arbeitet mit zwei 56-Bit-Schlüsseln
- **Klartext** > Key 1 > *Temp 1* > Key 2 > *Temp 2* > Key 1 > **Chiffrat**

AES (Advanced Encryption Standard)

- 128-Bit-Blöcke, variable Schlüssellänge: 128, 192 oder 256 Bit
- AES-256 ist nach heutigem Kenntnisstand in der Praxis nicht zu knacken

Asymmetrische Verschlüsselung

Auch „Public Key Encryption“

Es gibt kein gemeinsames Geheimnis, nicht *den* 1 Schlüssel

Jeder Teilnehmer hat ein *Schlüsselpaar* aus **Private** und **Public** Key.

Der **Public Key** wird öffentlich gemacht, der **Private Key** geheim gehalten (daher die Namen ;-))

Die Schlüssel hängen mathematisch so zusammen, dass Daten, die mit dem *einen* Schlüssel ver- nur mit dem dazugehörigen *anderen* wieder entschlüsselt werden können.

Daher „asymmetrisch“: Zum Ver- und Entschlüsseln werden zwei verschiedene Schlüssel benutzt

Asymmetrische Verschlüsselung

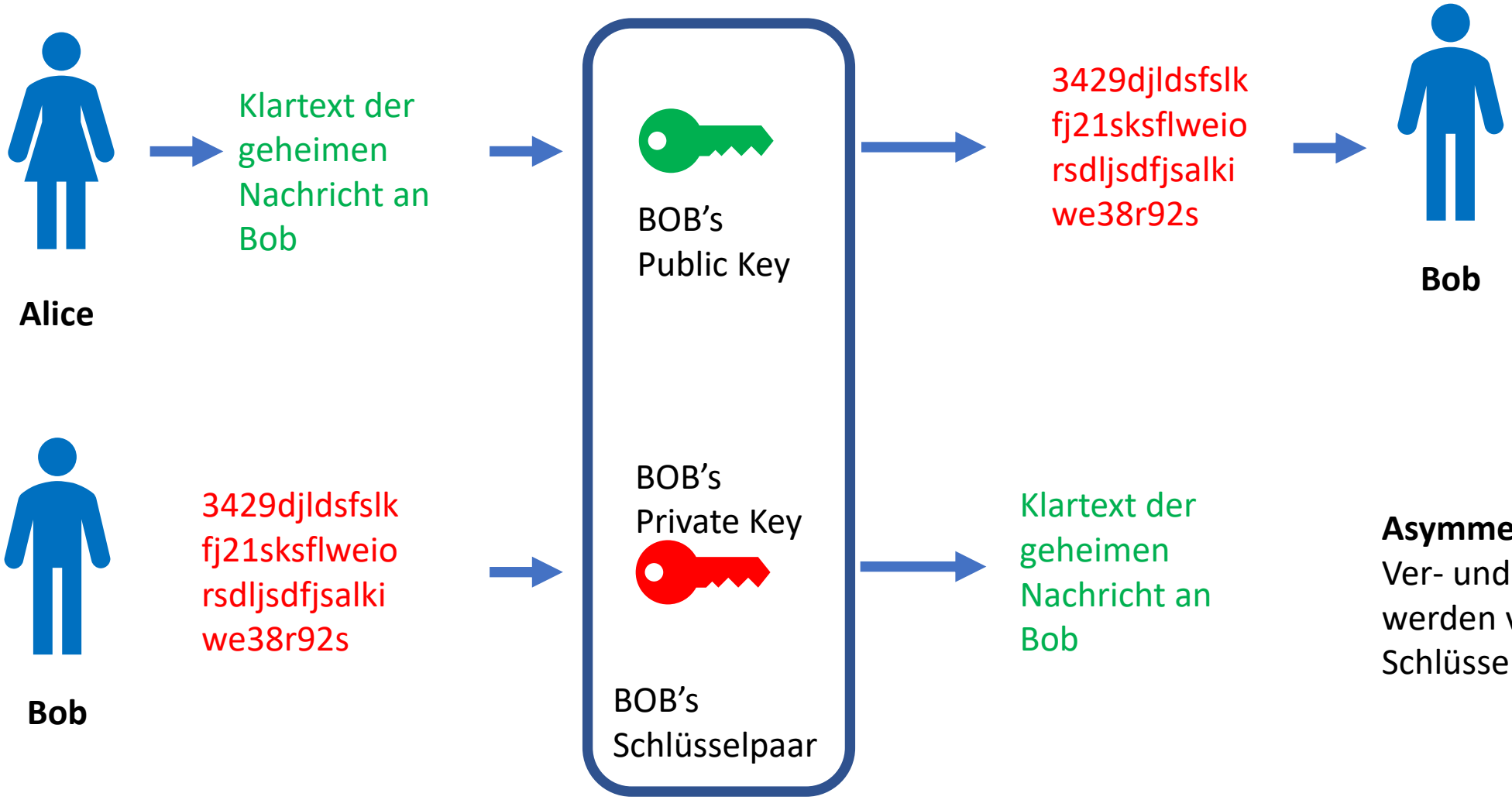
Alice will Bob eine verschlüsselte Nachricht schicken und sicher sein, dass nur Bob diese Nachricht lesen kann

Alice verschlüsselt die Nachricht mit dem **Public Key** von Bob und erzeugt so ein Chiffrat, das nur Bob mit seinem **Private Key** wieder entschlüsseln kann

Alice schickt das Chiffrat über einen unsicheren Kanal an Bob

Bob entschlüsselt das Chiffrat mit seinem **Private Key**.

Asymmetrische Verschlüsselung



Asymmetrisch: Zum Ver- und Entschlüsseln werden verschiedene Schlüssel benutzt

Asymmetrische Verschlüsselung

Vorteil

- Es wird kein gemeinsames Geheimnis benötigt, das Problem des Schlüsseltausches entfällt

Nachteil

- Sehr rechenintensiv (also: langsam)
- Eignet sich *nicht* für große Datenmengen
- Kompliziert im Verständnis, in der Anwendung und in der Implementation

Asymmetrische Verfahren

Es gibt verschiedene Algorithmen zur asymmetrischen Verschlüsselung, es werden vor allem zwei eingesetzt:

RSA (Rivest, Shamir, Adleman)

- Bekanntestes Verfahren, sehr weit verbreitet
- Basiert auf der Multiplikation sehr großer Primzahlen

ECC (Elliptic Curve Cryptographie)

- Neueres Verfahren, wird zunehmend populär
- Schneller und kompakter als RSA

Symmetrisch *vs.* asymmetrisch

Symmetrisch

+ Einfach
+ Schnell
– Gemeinsames Geheimnis

Asymmetrisch

– Kompliziert
– Langsam
+ *Kein* gemeinsames Geheimnis

Ideal wäre ein Verfahren, dass einfach und schnell ist, und trotzdem kein gemeinsames Geheimnis benötigt …

Hybride Verfahren (SSL/TLS)

Kombination aus Symmetrisch / Asymmetrisch

Der eigentliche Datenaustausch erfolgt symmetrisch verschlüsselt

Das gemeinsame Geheimnis wird durch asymmetrische Verfahren etabliert

Wird z.B. bei der Verschlüsselung im Web benutzt (`https`)

Protokolle: **SSL** (Secure Sockets Layer) bzw. heute **TLS** (Transport Layer Security)

Hybride Verfahren (SSL/TLS)

Client kontaktiert Server und fordert eine verschlüsselte Verbindung an

Server schickt seinen Public Key (in Form eines Zertifikats)

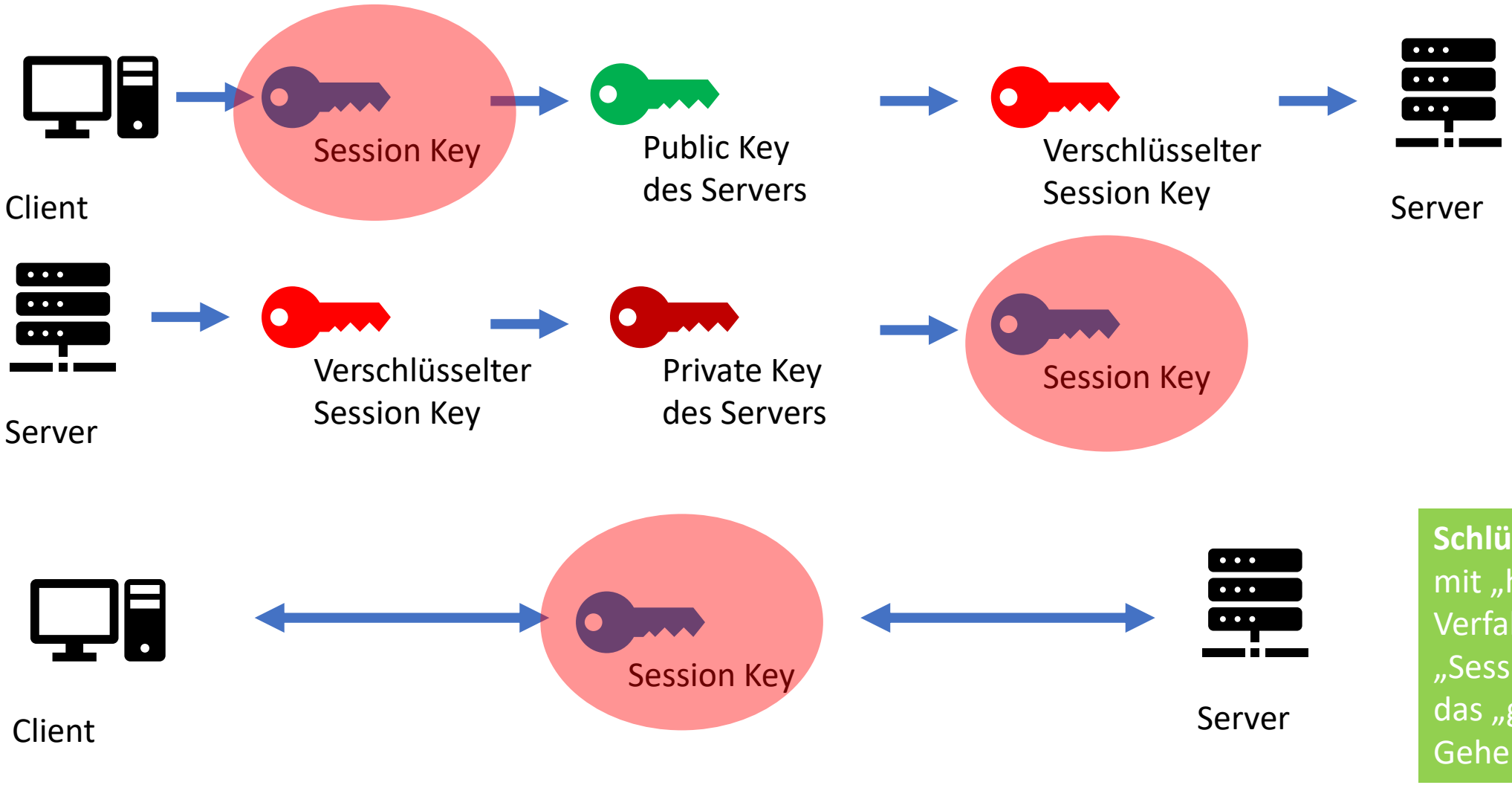
Client erzeugt einen zufälligen **Session Key**, verschlüsselt diesen mit dem **Public Key** des Server und schickt das Chiffrat an den Server

Server entschlüsselt Chiffrat mit seinem **Private Key** und erhält so den vom Client erzeugten **Session Key**

Nun haben Client & Server ein „gemeinsames Geheimnis“ und können ab jetzt symmetrisch verschlüsseln

Der **Session Key** ist sehr klein (z.B. 256 Bit), da fällt der Rechenaufwand der asymmetrischen Verschlüsselung nicht ins Gewicht

Hybride Verfahren (SSL/TLS)



Schlüsseltausch mit „hybridem Verfahren“. Der „Session Key“ ist das „gemeinsame Geheimnis“

Transport- vs. Ende-zu-Ende-Verschlüsselung

Transportverschlüsselung (auch: Punkt-zu-Punkt-Verschlüsselung)

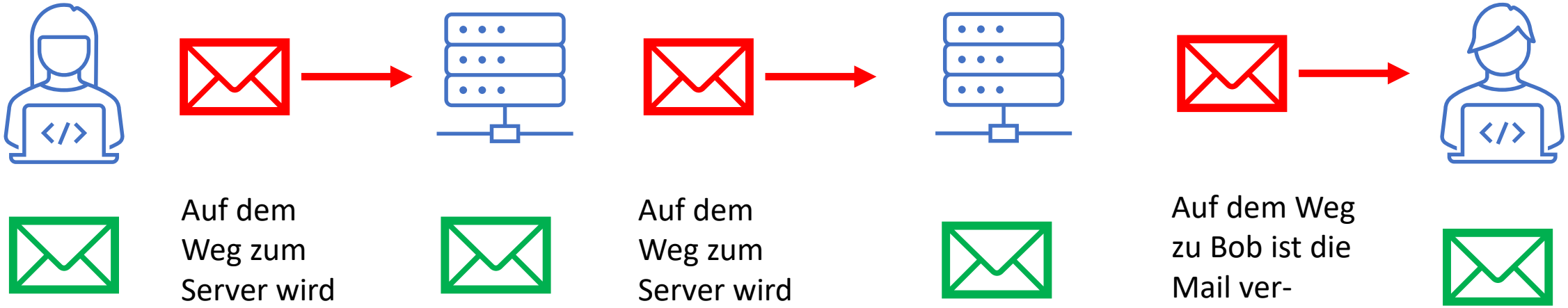
- Die Daten sind während des Transports von Client zu Server, von Server zu Server und von Server zu Client verschlüsselt
- An den jeweiligen Stationen (Punkten) liegen sie unverschlüsselt vor

Ende-zu-Ende-Verschlüsselung

- Die Daten werden direkt auf den jeweiligen Endgeräten ver- und entschlüsselt
- Liegen ausschließlich auf den Endgeräten (Clients) unverschlüsselt vor

Transport-/Punkt-zu-Punkt-Verschlüsselung

Nur zwischen den einzelnen Stationen sind die Daten verschlüsselt



Alice schreibt eine Mail. Die Mail ist auf dem PC unver-schlüsselt

Auf dem Weg zum Server wird die Mail ver-schlüsselt

Auf dem Server ist die Mail unver-schlüsselt

Auf dem Weg zum Server wird die Mail ver-schlüsselt

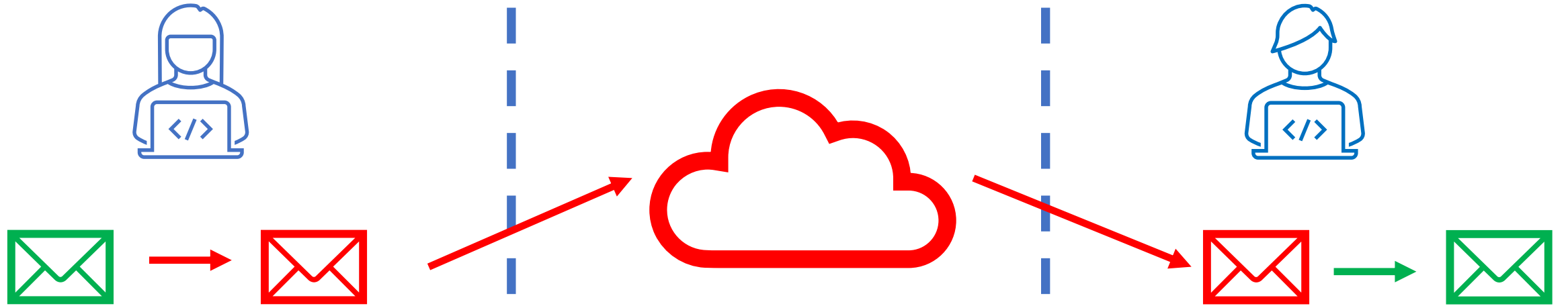
Auf dem Server ist die Mail unver-schlüsselt

Auf dem Weg zu Bob ist die Mail ver-schlüsselt

Auf dem PC von **Bob** ist die Mail unverschlüsselt

Ende-zu-Ende-Verschlüsselung

Die Daten liegen lediglich beim Sender und Empfänger unverschlüsselt vor



Alice schreibt eine Mail. Die Mail ist auf dem PC unver-schlüsselt

Die Mail wird auf dem PC von **Alice** verschlüsselt. Erst dann wird sie via Internet verschickt

Während des gesamten Weg durchs Internet bleibt die Mail verschlüsselt, sie kann an keiner Stelle entschlüsselt werden

Die Mail landet verschlüsselt auf **Bobs** PC

Bob ent-schlüsselt die Mail auf seinem PC

PFS: Perfect Forward Secrecy

Beim hybriden Verfahren wird der Session Key über einen unsicheren Kanal verschickt. Der Session Key ist zwar verschlüsselt, aber potentiell angreifbar:

- Der Angreifer fängt den mit dem Public Key des Empfängers verschlüsselten Session Key ab
- Der Angreifer speichert die gesamte mit dem Session Key verschlüsselte Kommunikation

Damit kann der Angreifer zwar vorerst nichts anfangen …

- … erhält der Angreifer aber Zugriff auf den Private Key des Empfängers, kann er die gesamte Kommunikation nachträglich entschlüsseln

Gesucht wird eine Art der Schlüsselvereinbarung, die auch in Zukunft sicher bleibt, sich der Session Key also nicht rekonstruieren lässt

PFS: Eine perfekte, in die Zukunft gerichtete Verschlüsselung („Folgenlosigkeit“)

Schlüsselvereinbarung nach Diffie-Hellman

Whitfield Diffie und Martin Hellman entwickelten 1976 unter Mitarbeit von Ralph Merkle ein Public-Key-Verfahren, bei dem das „shared secret“ nicht getauscht, sondern berechnet wird

Sender und Empfänger tauschen verschiedene Zahlen öffentlich aus und führen jeweils in Kombination mit einer je eigenen geheimen Zahl Berechnungen durch

Als Ergebnis erhalten beide Seiten ein identisches Ergebnis, das als „shared secret“, also als Schlüssel für symmetrische Verschlüsselung benutzt werden kann

Rechenweg für Diffie-Hellman



Alice

p (Primzahl)
g (Wurzel)

a (Geheimzahl)

schickt p und g an Bob

p (Primzahl)
g (Wurzel)

b (Geheimzahl)



Bob

$A = g^a \bmod p$

schickt A an Bob

A

B

schickt B an Alice

$B = g^b \bmod p$

$Key = B^a \bmod p$

$Key = A^b \bmod p$

Beispiel für Diffie-Hellman



Alice

13 (Primzahl)
2 (Wurzel)

17 (Geheimzahl)

schickt 13 und 2 an Bob

13 (Primzahl)
2 (Wurzel)

4 (Geheimzahl)



Bob

2^{17} **mod** 13 = 6

schickt 6 an Bob

6

schickt 3 an Alice

3

2^{4} **mod** 13 = 3

3^{17} **mod** 13 = 9

6^{4} **mod** 13 = 9