

IT-Sicherheit KI

Grundlagen

Prof. Dr. Tobias Eggendorfer

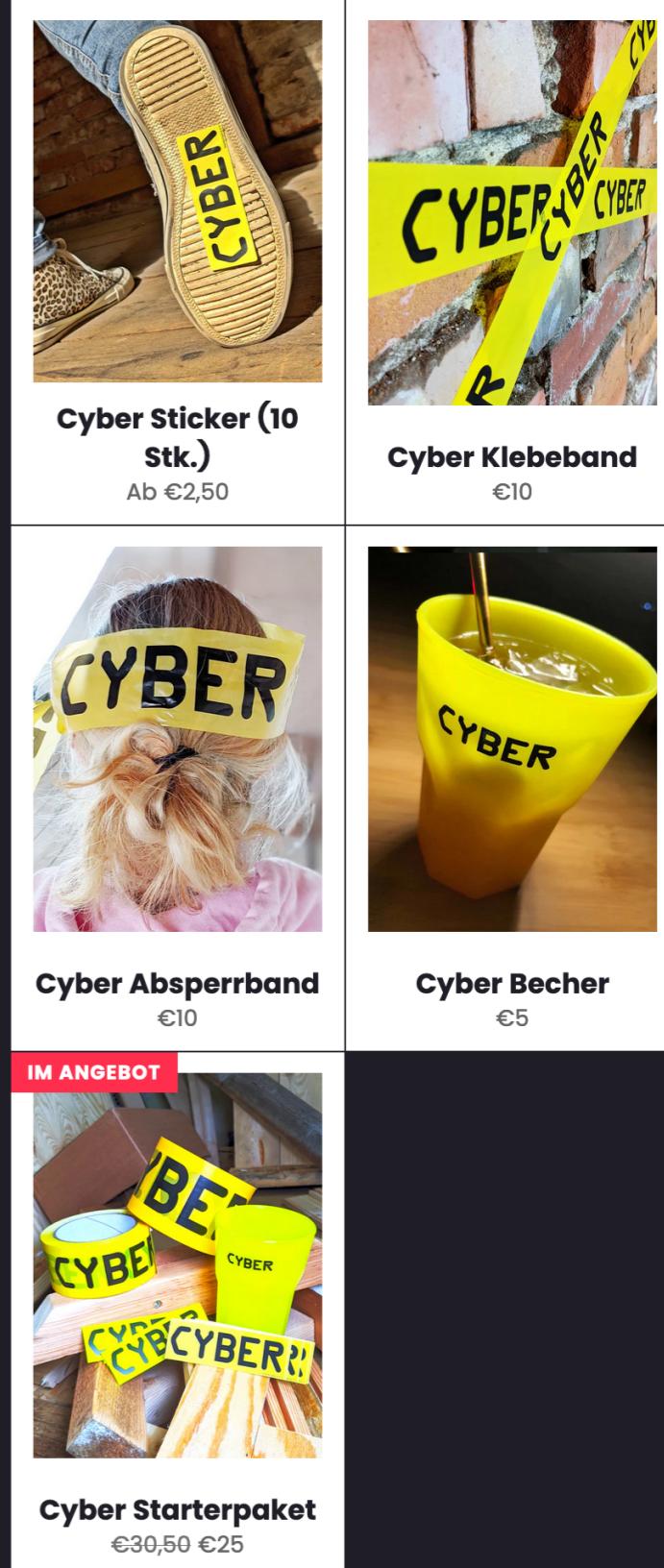


Technische Hochschule
Ingolstadt

Cybercrime & Co.

Cyber-Crime

- Was ist Cyber?
- Was ist Cyber-Crime?
 - Taten im „Cyber“?
 - Taten mit „Cyber“ als Tathilfsmittel?
 - Taten mit ein bißchen „Cyber“?



Wer sind diese Angreifer?

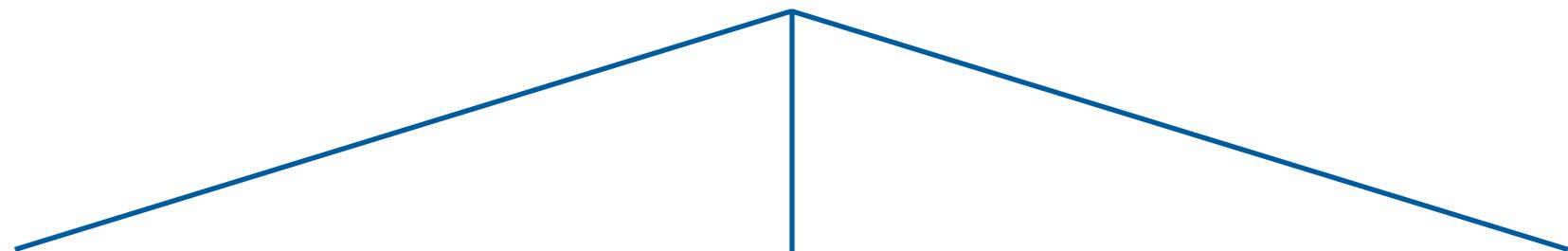
- Script-Kiddie
- Hacker (White-Hat, Grey-Hat, Black-Hat)
- Staatliche Akteure
- Sys-Admin, C*O etc.

Grundziele der IT- Sicherheit

Vertraulichkeit, Integrität und Authentizität

Vertraulichkeit

Kryptologie



Steganographie

Kryptographie

Kryptanalyse

Verdecktes
Schreiben

Geheimes
Schreiben

Knacken von
Chiffren

Steganographie

- Linguistische Steganographie
- Technische Steganographie
- Sonderfall „Covert Channels“

Steganography



There is a
Hospital wide
Information System

Steganography



There is a
Hospital wide
Information System

Memo to the Director:

Subject: Letter of Recommendation

Jane S., a chief sub editor and editor, can always be found hard at work in her cubicle. Jane works independently, without wasting company time talking to colleagues. She never thinks twice about assisting fellow employees, and she always finishes given assignments on time. Often Jane takes extended measures to complete her work, sometimes skipping coffee breaks. She is a dedicated individual who has absolutely no vanity in spite of her high accomplishments and profound knowledge in her field. I firmly believe that Jane can be classed as a high-caliber employee, the type which cannot be dispensed with. Consequently, I duly recommend that Jane be promoted to executive management, and a proposal will be sent away as soon as possible.

Memo to the Director:

Subject: Letter of Recommendation

Jane S., a chief sub editor and editor, can always be found hard at work in her cubicle. Jane works independently, without wasting company time talking to colleagues. She never thinks twice about assisting fellow employees, and she always finishes given assignments on time. Often Jane takes extended measures to complete her work, sometimes skipping coffee breaks. She is a dedicated individual who has absolutely no vanity in spite of her high accomplishments and profound knowledge in her field. I firmly believe that Jane can be classed as a high-caliber employee, the type which cannot be dispensed with. Consequently, I duly recommend that Jane be promoted to executive management, and a proposal will be sent away as soon as possible.

Memo to the Director:

Subject: Letter of Recommendation

Jane S., a chief sub editor and editor, can always be found hard at work in her cubicle. Jane works independently, without wasting company time talking to colleagues. She never thinks twice about assisting fellow employees, and she always finishes given assignments on time. Often Jane takes extended measures to complete her work, sometimes skipping coffee breaks. She is a dedicated individual who has absolutely no vanity in spite of her high accomplishments and profound knowledge in her field. I firmly believe that Jane can be classed as a high-caliber employee, the type which cannot be dispensed with. Consequently, I duly recommend that Jane be promoted to executive management, and a proposal will be sent away as soon as possible.

Never has a man influenced physics so profoundly as Niels Bohr in the early 1900's. Going back to this time period, little was known about atomic structure; Bohr set out to end the obscurity of physics. However, things didn't come easy for Bohr. He had to give up most of his life for physics and research of many hypothesis. But, this is why you and I have even heard of the quantum theory and atomic structures. Bohr came up with his quantum theory while studying at Cambridge. Bohr was a skeptic and he never truly believed in Max Planck's old quantum theory. He put forth the idea that, going from one high-energy orbit to a lower one, an electron could, in fact, be trying to emit a quantum of discrete energy. Bohr was criticized for this idea, but he didn't let up. Soon after, Bohr said his famed quote, "If quantum mechanics hasn't shocked you, you haven't understood it yet." This quote is extremely famous and has gone down as the motto for quantum physicist around the world. Understandably, Bohr never won a Nobel prize outside of physics (of which he only won one). Bohr's still going strong with his theories on atomic structure; he allowed for 100's of scientists to fully experiment with the cell and its many components. Bohr was largely on the run from the Nazi's when he came up with this discovery, which is amazing because around this time, Bohr's home country of Denmark was invaded by the Nazi's. Bohr and Ernest Rutherford are given credit, but it is believed that Rutherford decided to desert Bohr in the middle of their work. Rutherford once, quite famously said that you should never bet against the wonders of science. Niels Bohr's famous career never really kicked off until he was forty years old. Most other major scientists were going all over the world with their ideas by their early twenties. However, in order to preserve the legacy of Niels Bohr, he has his own institution, whose goal is to make many more great strides in the field of physics for years. How did Bohr affect you and me? Without Niels Bohr's more advanced atomic theory, we might as well cry over how little we know of the atoms and their compounds. Physics would have never been such a force in the today's society. However, to this day, research is still going on to improve and update the atomic theory. Although scientists clearly want to improve on Bohr's theory, many famous physicists come out publicly and openly say that Bohr's ideas will never be improved upon, today's society cannot say goodbye to an opportunity to improve our understanding of the sciences. If Bohr never had silenced his critics, we would still be following Planck's theories, and going on incomplete information. Bohr's later life was all occupied when he decided to go back to Denmark and head the Royal Danish Academy. His main goal was to tell the world of the greatness of the Danish Sciences and most likely educate a new crop of scientists. It's funny to think that if Bohr had not been a peace-seeker, Bohr's lie during his stint in Manhattan Project would have probably led to a nuclear explosion and a peace-seeker, Bohr engineered on the Manhattan Project. Though he didn't hurt anyone directly, thousands of people died. Neils Bohr opened up a new world for you and I in the physics world, he will go down as one of the greatest physicists.

THE ULTIMATE RICK ROLL

Never has a man influenced physics so profoundly as Niels Bohr in the early 1900's. Going back to this time period, little was known about atomic structure; Bohr set out to end the obscurity of physics. However, things didn't come easy for Bohr. He had to give up most of his life for physics and research of many hypothesis. But, this is why you and I have even heard of the quantum theory and atomic structures. Bohr came up with his quantum theory while studying at Cambridge. Bohr was a skeptic and he never truly believed in Max Planck's old quantum theory. He put forth the idea that, going from one high-energy orbit to a lower one, an electron could, in fact, be trying to emit a quantum of discrete energy. Bohr was criticized for this idea, but he didn't let up. Soon after, Bohr said his famed quote, "If quantum mechanics hasn't shocked you, you haven't understood it yet." This quote is extremely famous and has gone down as the motto for quantum physicist around the world. Understandably, Bohr never won a Nobel prize outside of physics (of which he only won one). Bohr's still going strong with his theories on atomic structure; he allowed for 100's of scientists to fully experiment with the cell and its many components. Bohr was largely on the run from the Nazi's when he came up with this discovery, which is amazing because around this time, Bohr's home country of Denmark was invaded by the Nazi's. Bohr and Ernest Rutherford are given credit, but it is believed that Rutherford decided to desert Bohr in the middle of their work. Rutherford once, quite famously said that you should never bet against the wonders of science. Niels Bohr's famous career

you should never bet against the wonders of science. Niels Bohr's famous career never really kicked off until he was forty years old. Most other major scientists were going all over the world with their ideas by their early twenties. However, in order to preserve the legacy of Niels Bohr, he has his own institution, whose goal is to make many more great strides in the field of physics for years. How did Bohr affect you and me? Without Niels Bohr's more advanced atomic theory, we might as well cry over how little we know of the atoms and their compounds. Physics would have never been such a force in the todays society. However, to this day, research is still going on to improve and update the atomic theory. Although scientists clearly want to improve on Bohr's theory, many famous physicists come out publicly and openly say that Bohr's ideas will never be improved upon, todays society cannot say goodbye to an opportunity to improve our understanding of the sciences. If Bohr never had silenced his critics, we would still be following Planck's theories, and going on incomplete information. Bohr's later life was all occupied when he decided to go back to Denmark and head the Royal Danish Academy. His main goal was to tell the world of the greatness of the Danish Sciences and most likely educate a new crop of scientists. It's funny to think that if Bohr had not been so successful, we would still be following Planck's theories, and going on incomplete information.

THE ULTIMATE RICK ROLL

and a peace-seeker, Bohr engineered on the Manhattan Project. Though he didn't hurt anyone directly, thousands of people died. Neils Bohr opened up many doors for you and I in the physics world, he will go down as one of the greatest physicists ever.

Technische Steganographie

- Manipulation von
 - Bilddateien
 - Audiodateien
 - Videodateien
- Aber auch
 - Anordnen von Dateisektoren auf der Platte
 - Verstecken weiterer Datei

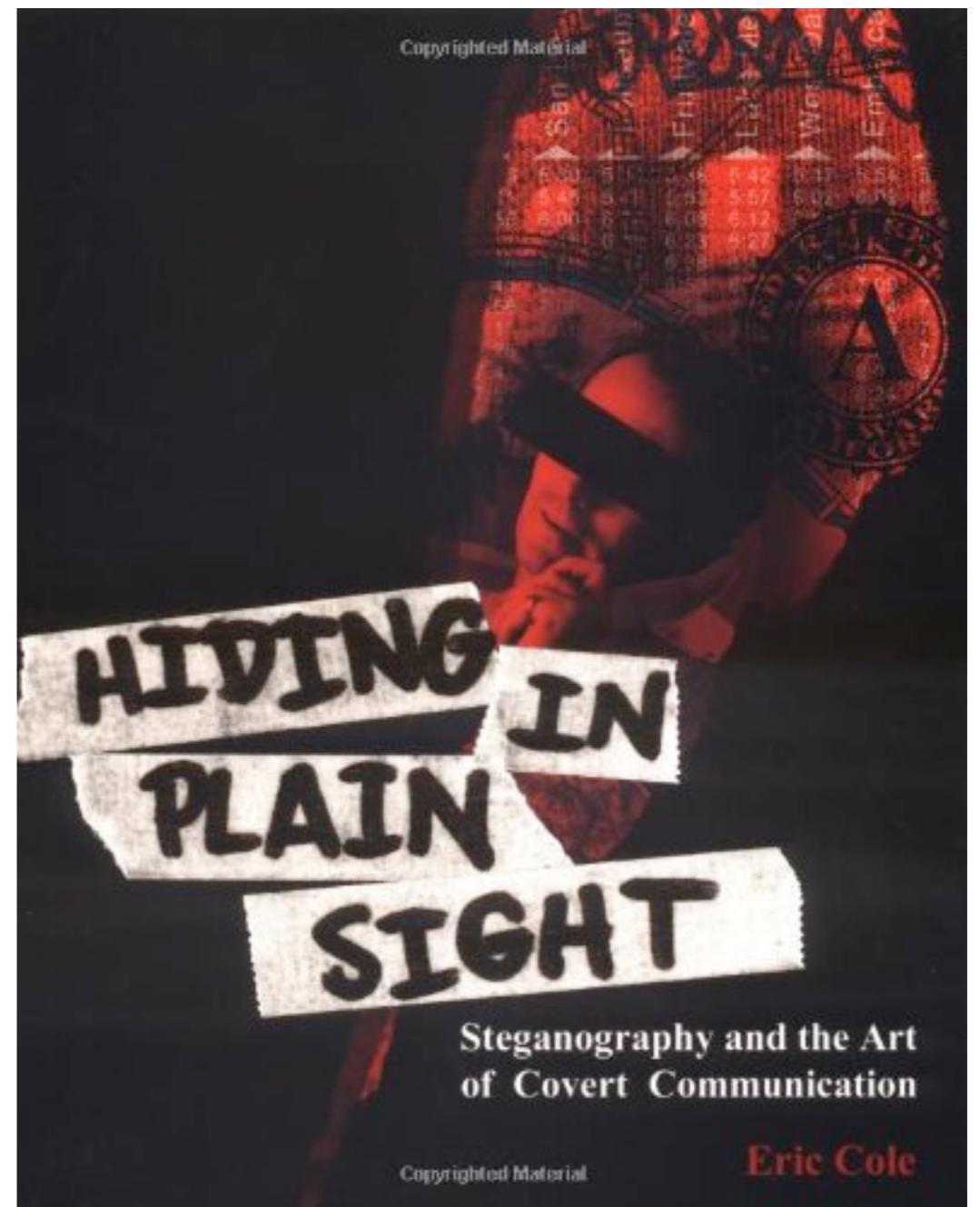
Beispiel Bilddatei

- Niederwertigstes Farb-Bit ist Daten-Bit
- Risiken:
 - Lossy Kompression (z.B. JPEG)
 - Resizing
- Lösung:
 - Kompressionsresistente Verfahren

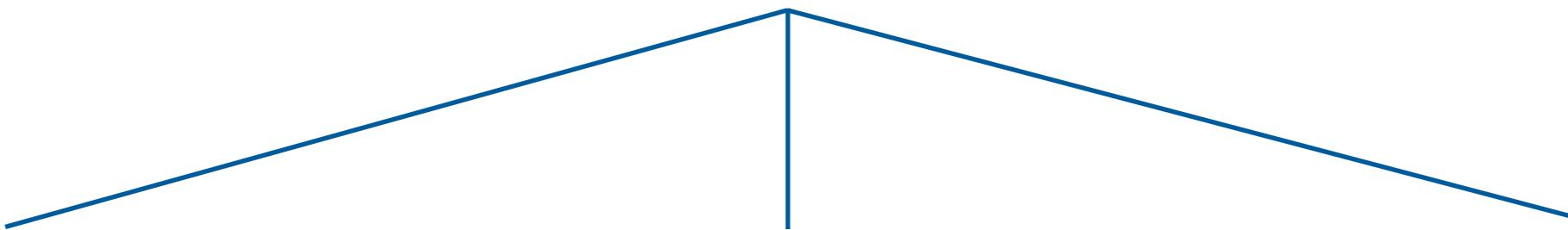
Analog: Zensor
linguistische
Steganographie

Literaturhinweis

- Eric Cole
Hiding in Plain Sight



Kryptographie



- Monoalphabetisch
Cäsar, XOR
 - Polyalphabetisch
 - Stromchiffren
DECT, RC4
 - Blockchiffren
IDEA, DES, AES
- RSA
 - Elliptic Curve

Symmetrische Kryptographie

Symmetrische Kryptographie

- Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
 - Stromchiffren
 - Blockchiffren
- } eher historisch

Monoalphabetische

- Bezeichnungen
 - Monoalphabetische Substitution
 - Monoalphabetische Kryptographie
 - Monoalphabetische Substitutionschiffren
- Von: „Ein Alphabet“
- Beispiele:
 - Cäsar, ROT13 & Co.
 - XOR

Cäsar

Beispiele

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
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

ROT13

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
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

Allgemein

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

Cäsar

Key: 3

spiele

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ROT13

ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Allgemein

ABCDEFGHIJKLMNOPQRSTUVWXYZ
FHINGOLSTADKEYBCJMPQRUVWXZ

Cäsar

Beispiele

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
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

ROT13

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
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

Allgemein

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

Beispiele

Cäsar

ROT13

Allgemein

Key konstant: 13

Vorteil: $\text{ROT13}(\text{ROT13}(T))=T$

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
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
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

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

Cäsar

Beispiele

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
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

ROT13

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
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

Allgemein

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

Cäsar

Beispiele

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ROT13

Key: „FHINGOLSTADKEY“

Allgemein

ABCDEFGHIJKLMNOPQRSTUVWXYZ
FHINGOLSTADKEYBCJMPQRUVWXZ

Cäsar

Beispiele

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
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

ROT13

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
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

Allgemein

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

Cäsar-Schiebealgorithmus



ABCDEFGHIJKLMNOPQRSTUVWXYZ

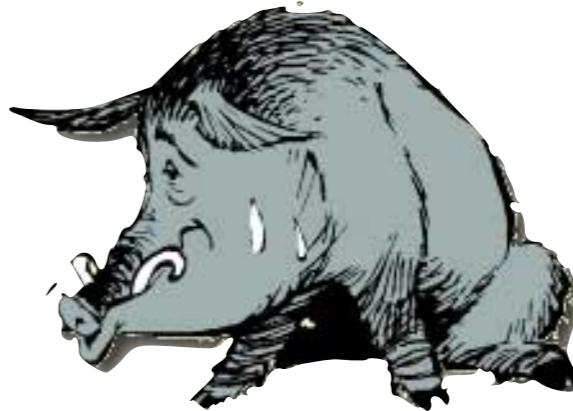
Cäsar-Schiebealgorithmus



ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar-Schiebealgorithmus

Wildschwein

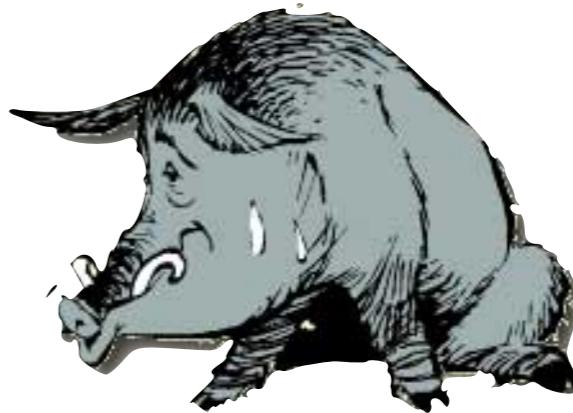


ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar-Schiebealgorithmus

Wildschwein

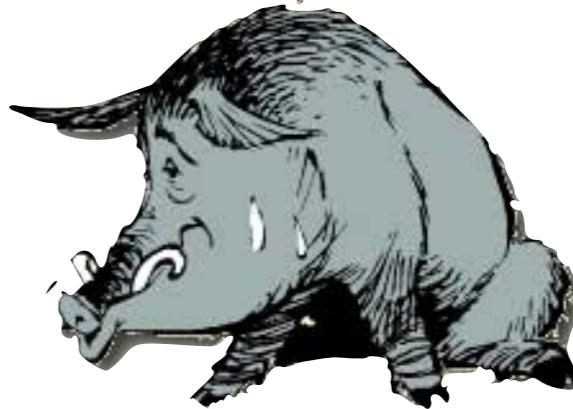
T



ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar-Schiebealgorithmus

Wildschwein
Tf



ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar-Schiebealgorithmus

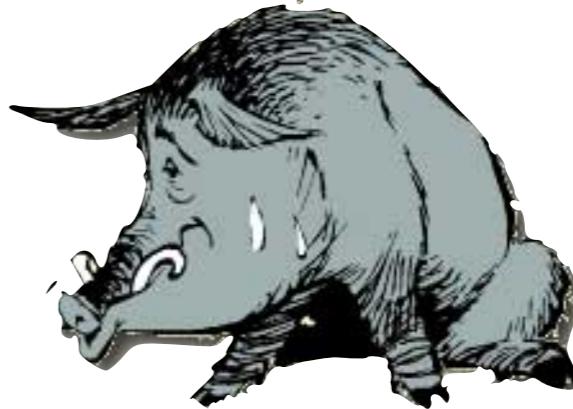
Wildschwein
Tfi



ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar-Schiebealgorithmus

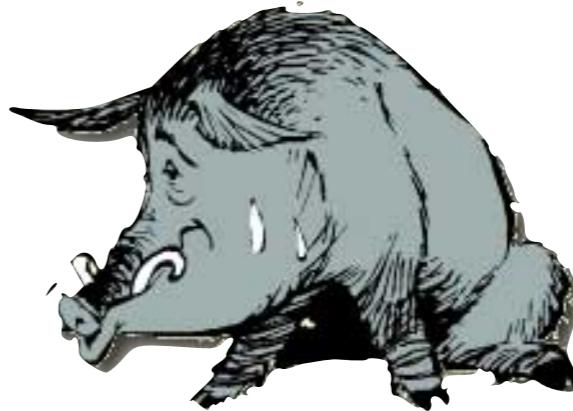
Wildschwein
Tfia



ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar-Schiebealgorithmus

Wildschwein
Tfiapzetbfk

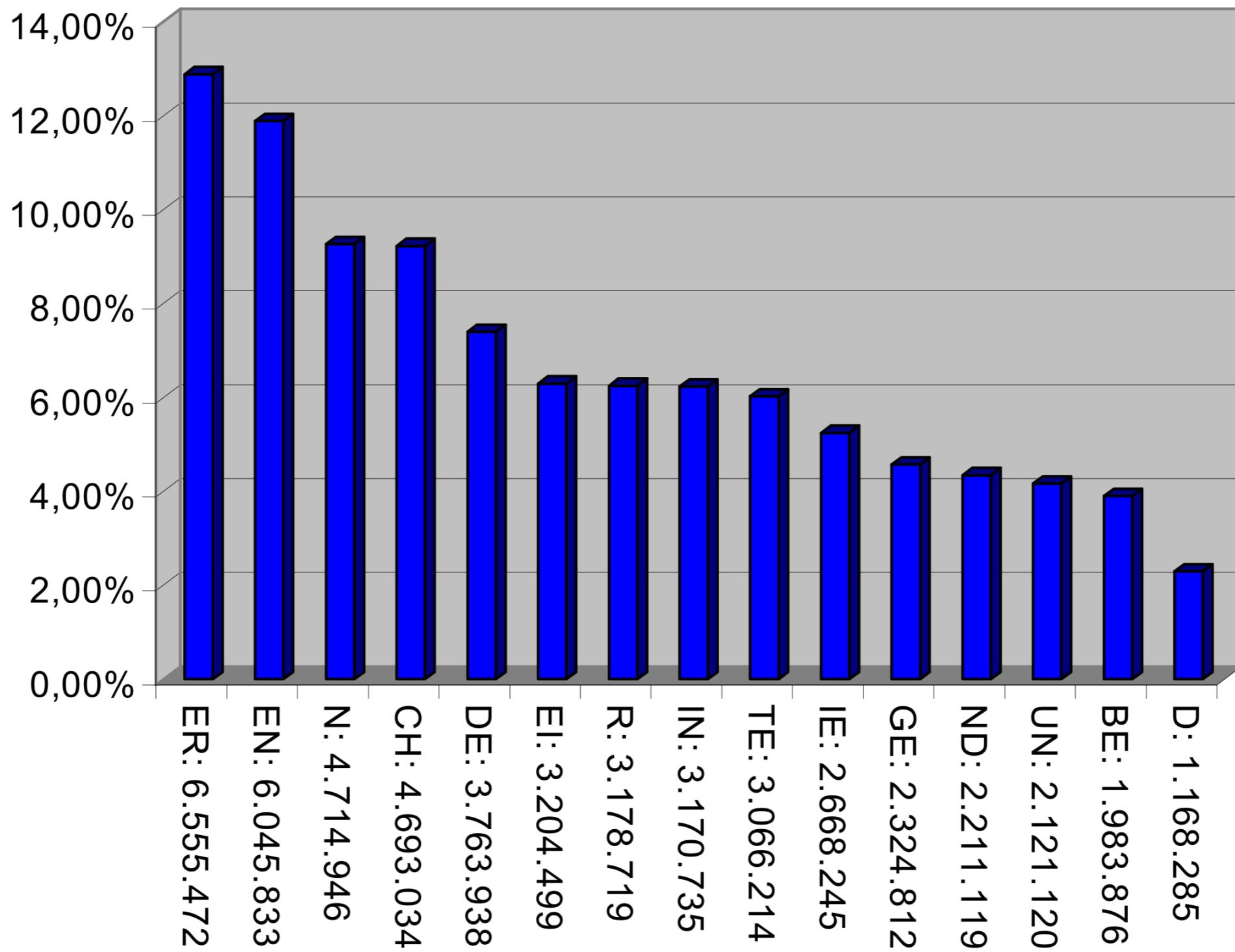


ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

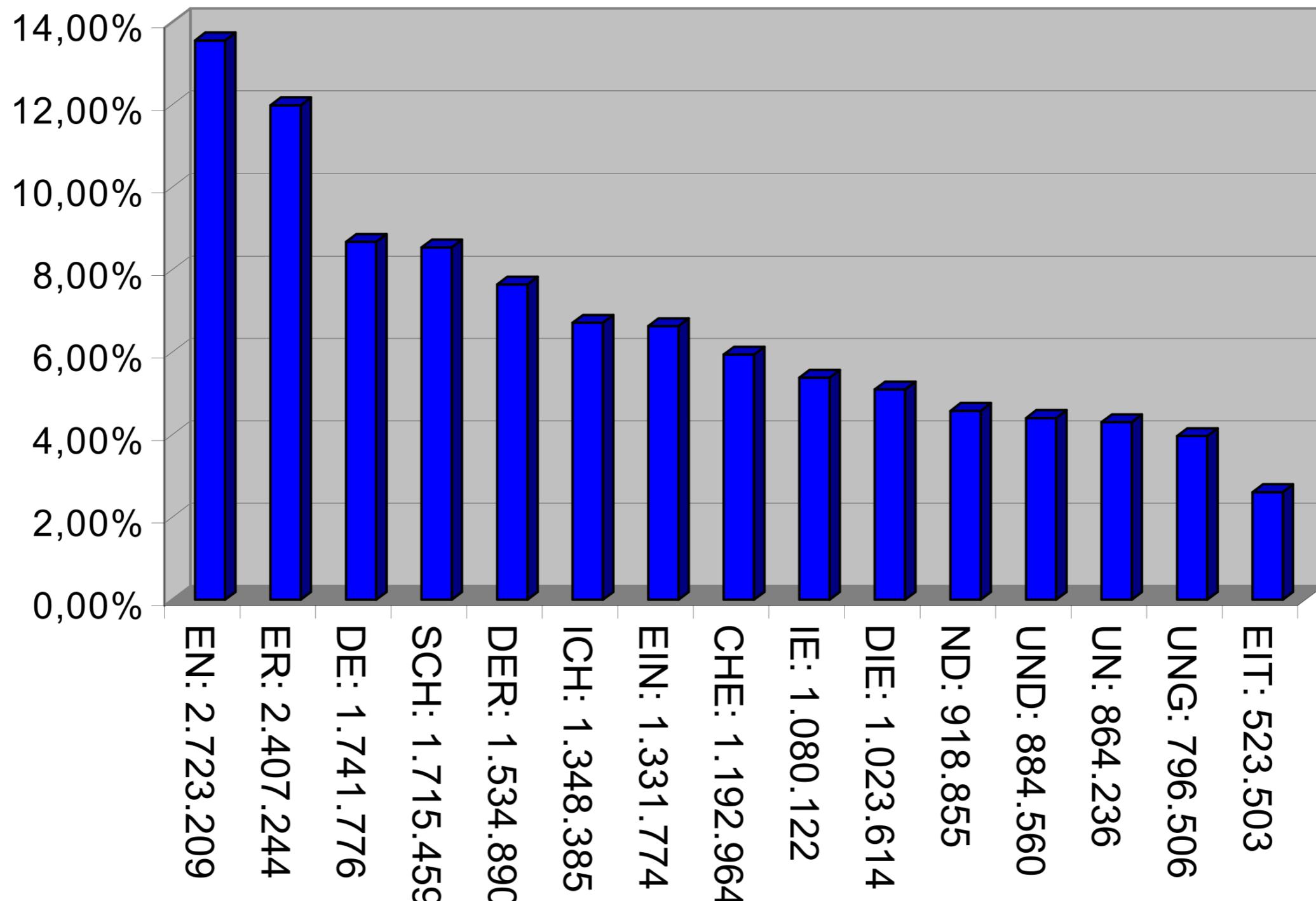
Kryptanalyse

- Häufig durch Häufigkeitsanalysen
 - Monogramme
 - Allgemein: E > N > I > S > R
 - Wortanfang: D > E > I > S > W
 - Wortende: N > E > R > T > S
 - Bigramme
 - Trigramme
- Notfalls: Brute Force

Bigramme



Trigramme



Quelle & weitere Sprachen

<https://de.wikipedia.org/wiki/Buchstaben%C3%A4ufigkeit>

Known-Plaintext

- Teil / Kompletter Klartext bekannt
- Ansatz:
 - Pattern wiederkennen
- Beispiel:
 - Hello World ROT 13 → Uryyb Jbeyq
 - II => yy

„Verbesserungen“

- Ähnliche Zeichen gleich setzen, z.B.
 - I=J
 - U=V
- Entfernen von Satz- und Sonderzeichen, Wortlängen:
 - Gdv lvw hlq Ehlvslho. („Aristocrat“)
 - GDVL VWHL QEHL VSLH O („Patristocrat“)

XOR

- Idee: $(A \text{ XOR } B) \text{ XOR } B = A$
- Problem:
 - $1 \leq B \leq 255 \rightarrow$ Brute-Forcing simpel

Polyalphabetische

- Beispiel: Vigenère-Verschlüsselung

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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext

THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext



Resultat:

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext

THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext

Resultat:

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext



Resultat:

Klartext-Alphabet



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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	Q	
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	
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	
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	
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	
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	
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	
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	
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
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
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	
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	
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	
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	
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	

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext



Resultat:

W

Klartext-Alphabet



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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	Q	
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	
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	
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	
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	
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	
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	
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	
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
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
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	
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	
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	
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	
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	

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext



Resultat:

W

Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN

Das ist ein Geheimtext



Resultat:

Wh



H



Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN



Resultat:

Wha



Klartext-Alphabet



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
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
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
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
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
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
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
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
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
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
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
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	Q
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Verschlüsseln von:

Das ist ein Geheimtext



THI NGO LST ADTKEYTHIN



Das ist ein Geheimtext



Resultat:

Wha vyh pag Ghrigfamkz

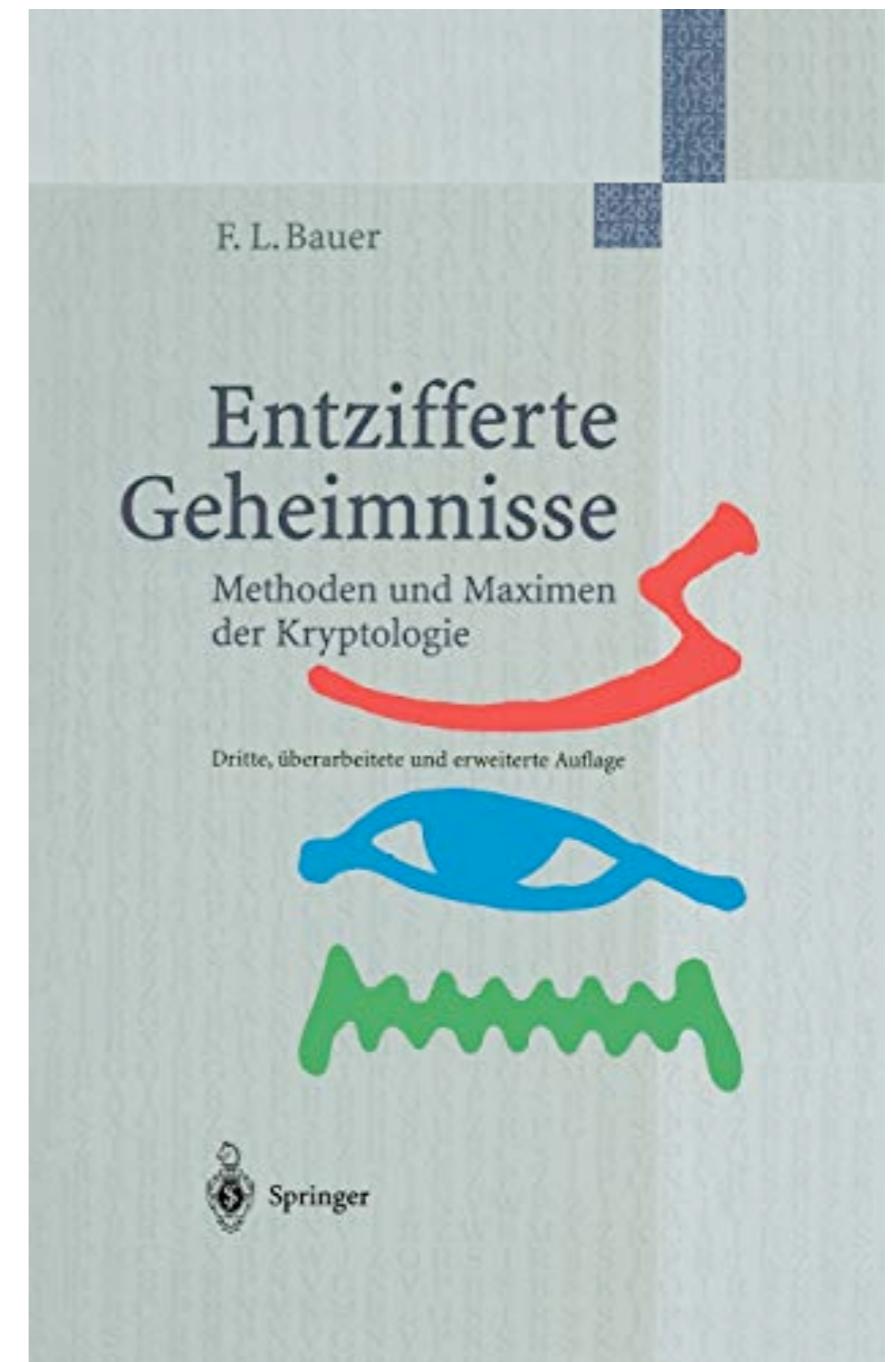


Gut und schlecht

- Keylänge entscheidend:
 - $\text{Len}(K) = 1 \rightarrow$ Cäsar
 - $\text{Len}(K) \ll \text{Len}(\text{Text}) \rightarrow$ Mehrere Cäsar-Chiffren
 - Frequenzanalyse für Bi- und Trigramme
 - $\text{Len}(K) = \text{Len}(\text{Text})$ und Key ist zufällig
 - One-Time-Pad
 - Echte Zufälligkeit?

Literaturhinweis

- Friedrich Ludwig Bauer
Entzifferte Geheimnisse
Methoden und Maximen der
Kryptologie



Stromchiffren

- Ansatz: Byte-weise verschlüsseln
- Beispiel: RC4

RC4

- S-Box mit 256 Werten, initialisiert mit Key
- $\text{crypt}(\text{Eingabe}_i) = \text{Eingabe}_i \text{ XOR } S[i]$
- Jeder Schritt verändert S-Box
→ Pseudo-Zufallszahlenfolge
- Gleiche Pseudo-Zufallszahlenfolge bei Absender und Empfänger → Gleiches Ergebnis

RC4 Initialisieren (I)

- K: array [255] of byte;

Wenn Key kürzer 256 Byte, dann wiederholen in K

- S: array [255] of byte;

```
for i = 0 to 255  
    S[i] = i  
next i
```

RC4 Initialisieren (II)

```
unsigned int j=0;  
for (i=0; i<255; i++)  
{  
    j=(j+S[i]+key[i mod KEYLENGTH]) mod 256;  
    swap(S[i],S[j]);  
}
```

RC4 Anwenden

```
i=0  
j=0  
while input  
{  
    i = (i + 1) mod 256  
    j = (j + S[i]) mod 256  
    swap (S[i], S[j])  
    K = S[ (S[i] + S[j]) mod 256 ]  
    input = input XOR K  
}
```

}

Pseudozufallsfolge

Verschlüsseln

Risiken

- Ist der Key bekannt, ist Pseudozufallsfolge vorhersagbar
- FehlendeNonce
 - Gleicher Key für lange Zeit → Leichter Knackbar
 - Lösung:
 - key = hash(Passphrase, Nonce)
 - Nonce = Zufallswert
 - Problem: Nonce tauschen

Blockchiffren

- Konzept
 - Blockweise verschlüsseln, z.B. 64 Bit
 - Ggf. Padding für $n \cdot 64$ -Bit
- Beispiele
 - DES / 3DES
 - IDEA
 - AES

Blockchiffren - Kernkonzepte

- Betriebsmodus:
Umgang mit Zerlegung für Nachrichten > n Bit
 - Electronic Code Book Mode
 - Cipher Block Chaining Mode
 - Cipher Feedback Mode
 - (und weitere, hier nicht relevante)

Electronic Code Book Mode

- Jeder Block unabhängig verschlüsselt
- Pro:
 - Fehler beeinflusst nur jeweiligen Block
- Contra:
 - Vertauschen von verschlüsselten Blöcken
 - Blöcke entschlüsselt vertauscht
 - Gleiche Blöcke gleich verschlüsselt

Cipher Block Chaining Mode

$$\text{Block}_{i+1} = \text{Encrypt}(\text{Input}_{i+1} \text{ XOR } \text{Block}_i, \text{Key})$$
$$\text{Block}_0 = \text{Encrypt}(\text{Input}_0 \text{ XOR IV}, \text{Key})$$

Cipher Block Chaining Mode

- Pro:
 - Fehler wirken sich nur auf beide nachfolgende Blöcke aus
 - Gleicher Input-Block → anderer Output-Block
 - Reihenfolge ändern → „Vermüllt“ Dechiffrat
- Contra:
 - Nicht parallelisierbar
(Block_i muß für Block_{i+1} bekannt sein)

Cooler Angriff

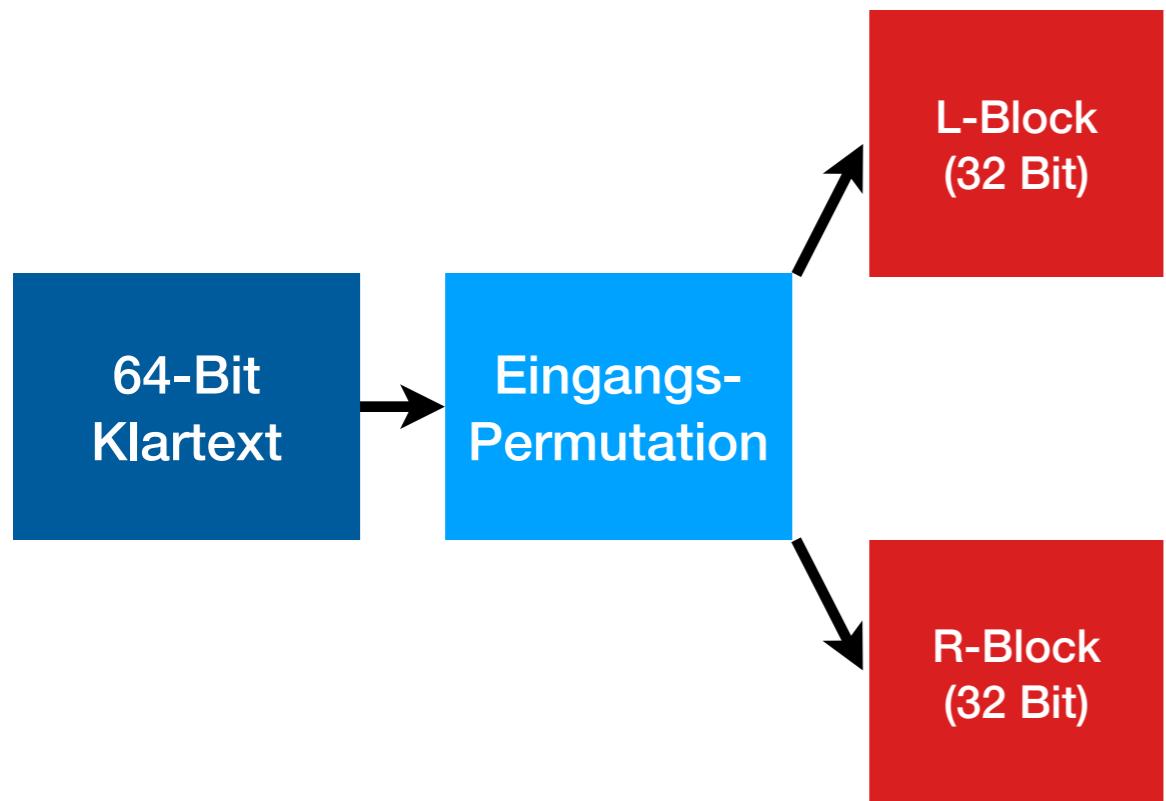
- Shell-Code-Injection in encrypted disks
- Grundidee:
 - 16 Byte Shell-Code
 - JMP am Ende
 - 16 Byte „Garbage“
- <https://www.jakoblell.com/blog/2013/12/22/practical-malleability-attack-against-cbc-encrypted-luks-partitions/>

Cipher Feedback Mode

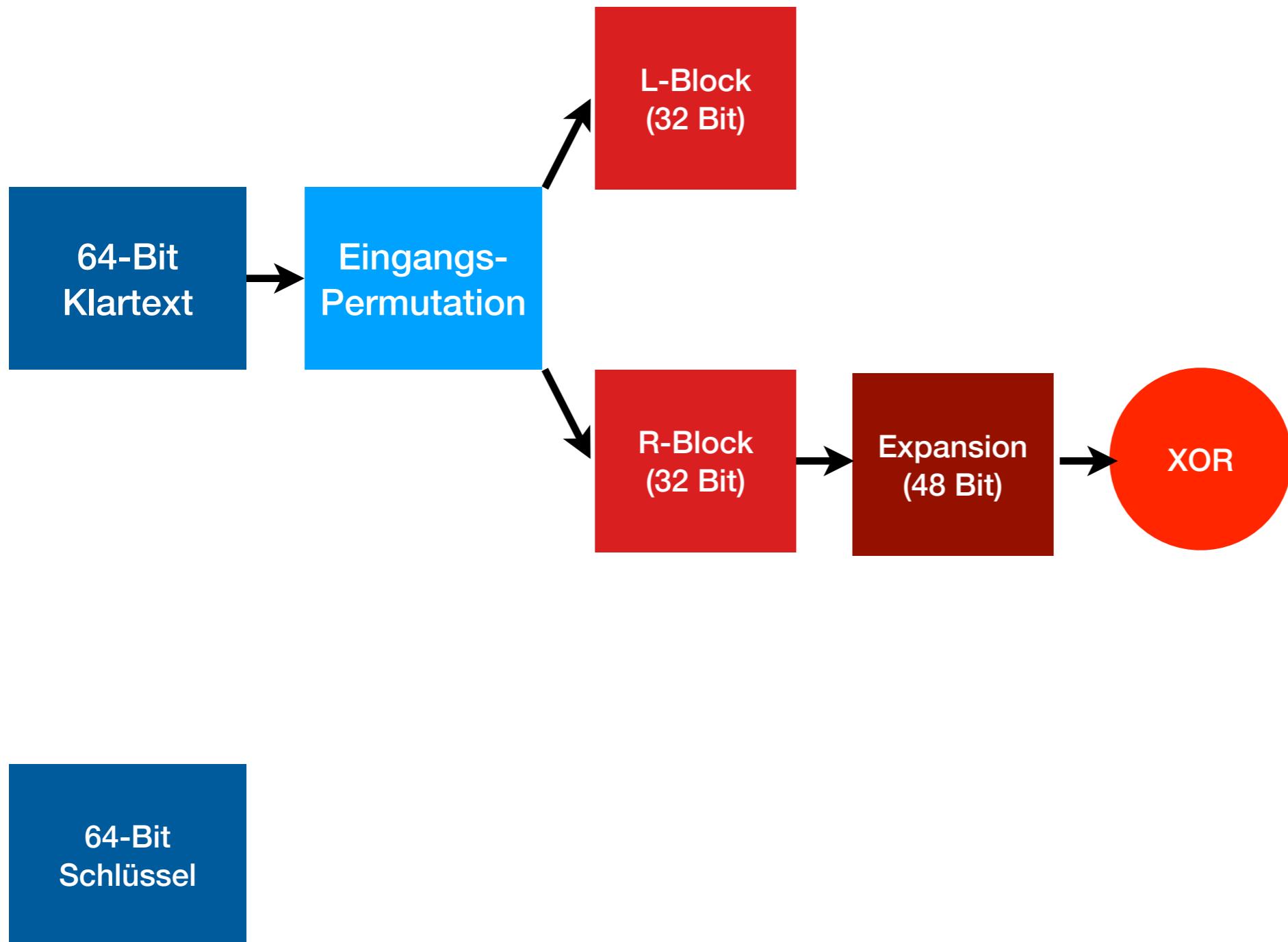
- Analog Cipher Block Chaining Mode, aber
 - n bit aus dem Input-Strom ersetzen n bit aus Key
 - Kein Padding
- Dadurch Verwendung von Block-Chiffre als Strom-Chiffre

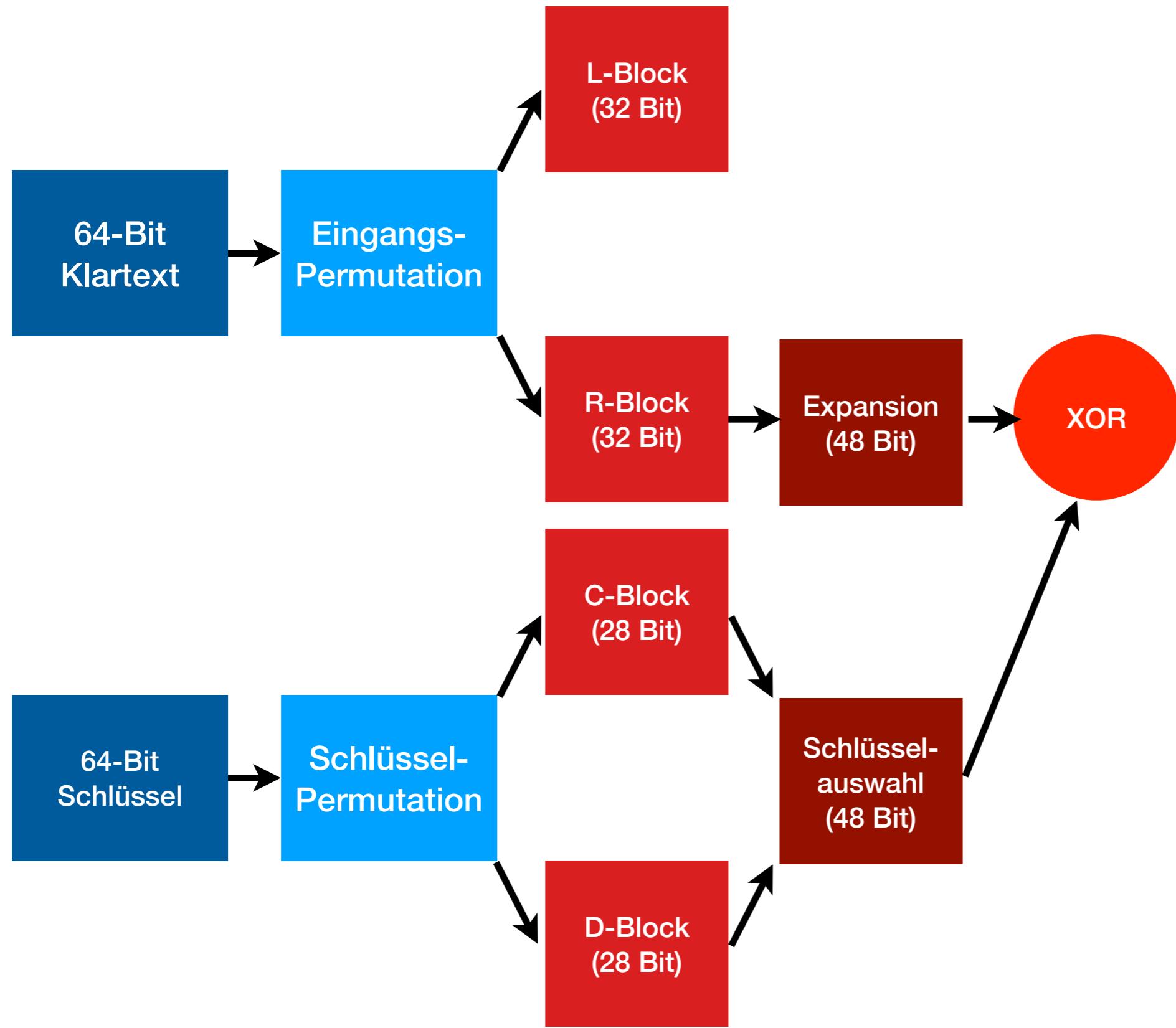
DES

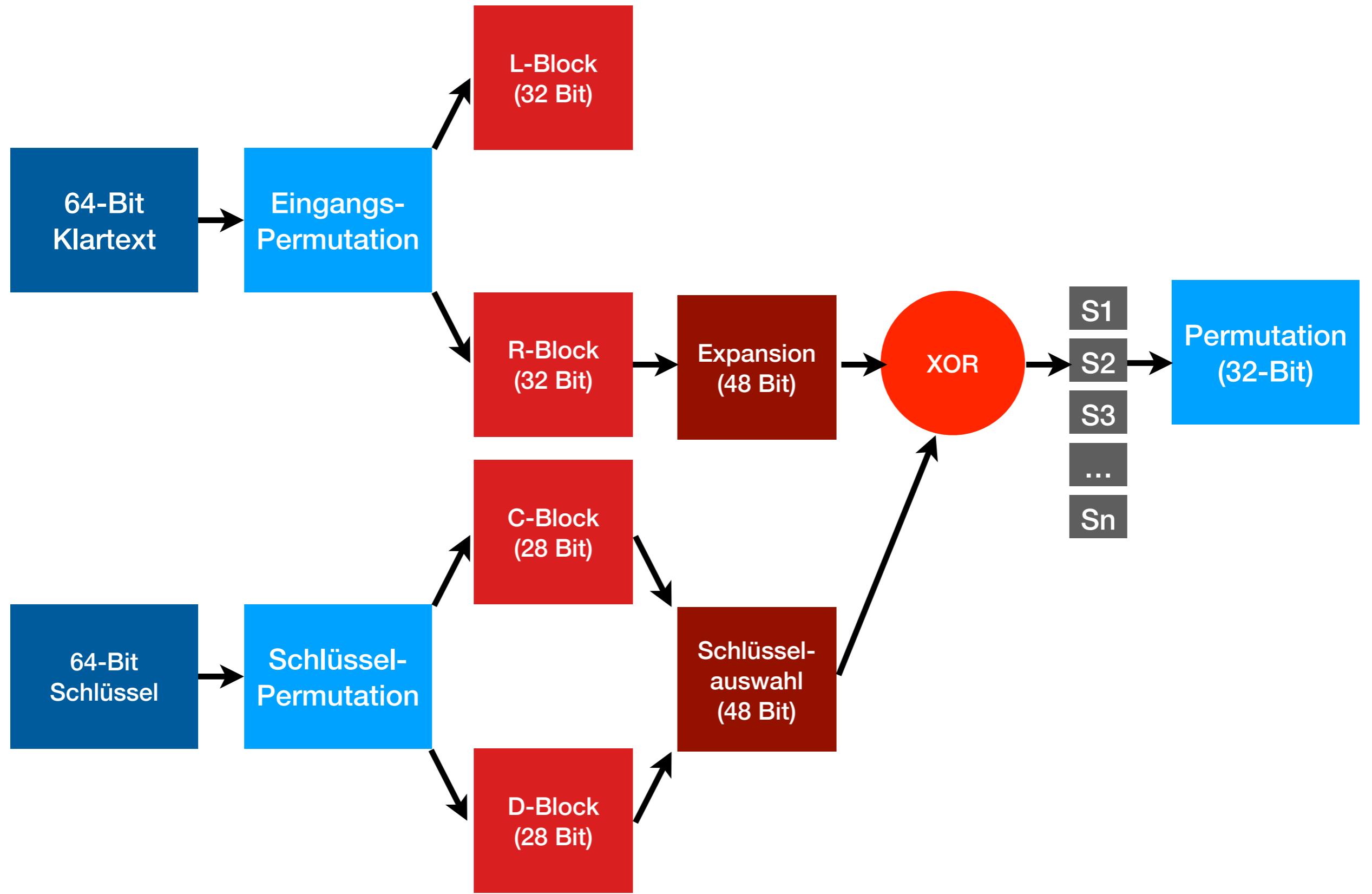
- „Data Encryption Standard“ (USA, 1977)
- Schlüssellänge DES:
64 Bit = 56 Bit User gewählt + 8 Bit Parität
- Mehrere Schritte zur Verschlüsselung
 - Permutation
 - Halbieren
 - Mehrere Runden
 - Zusammenführen
 - Permutation

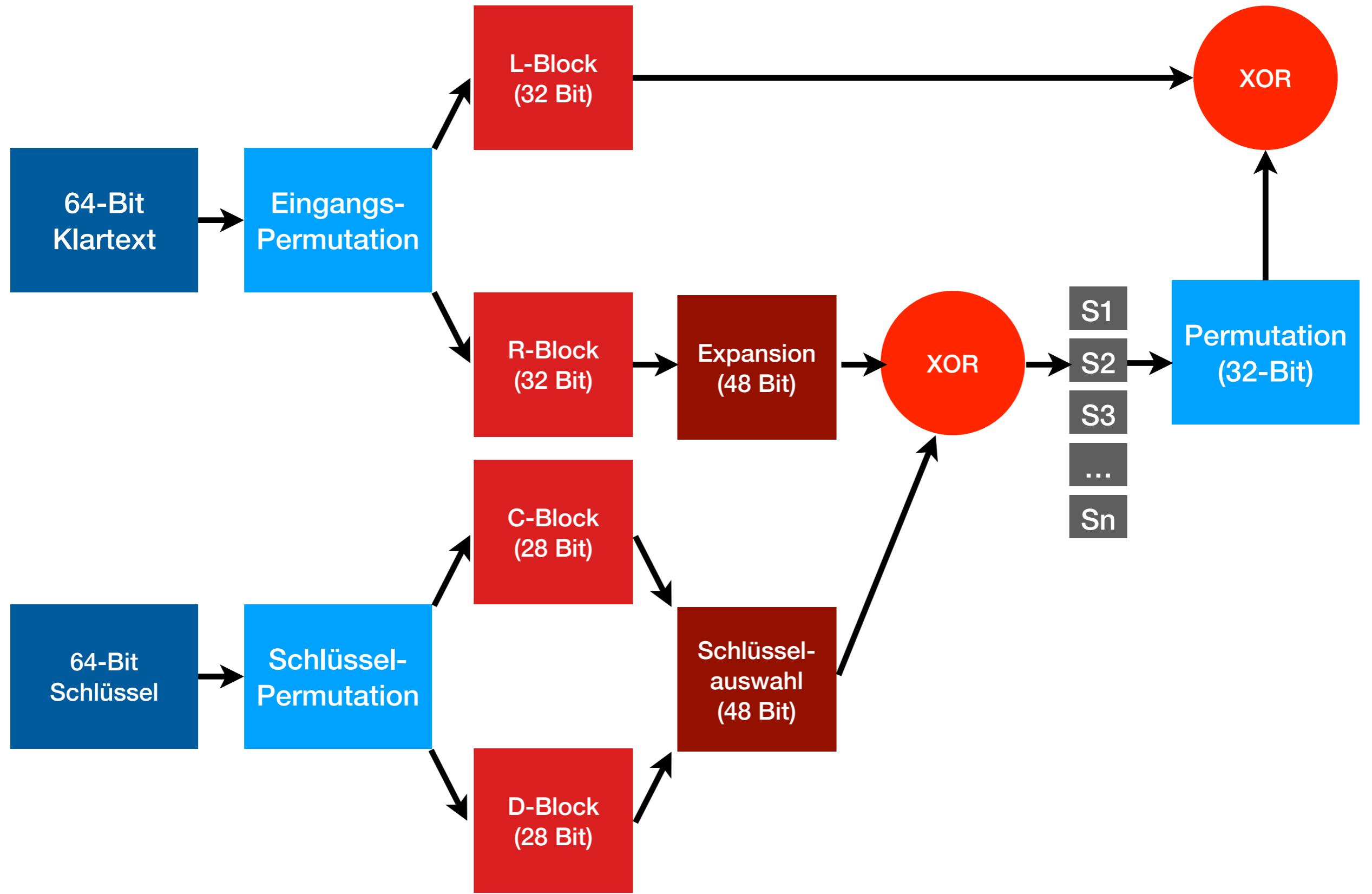


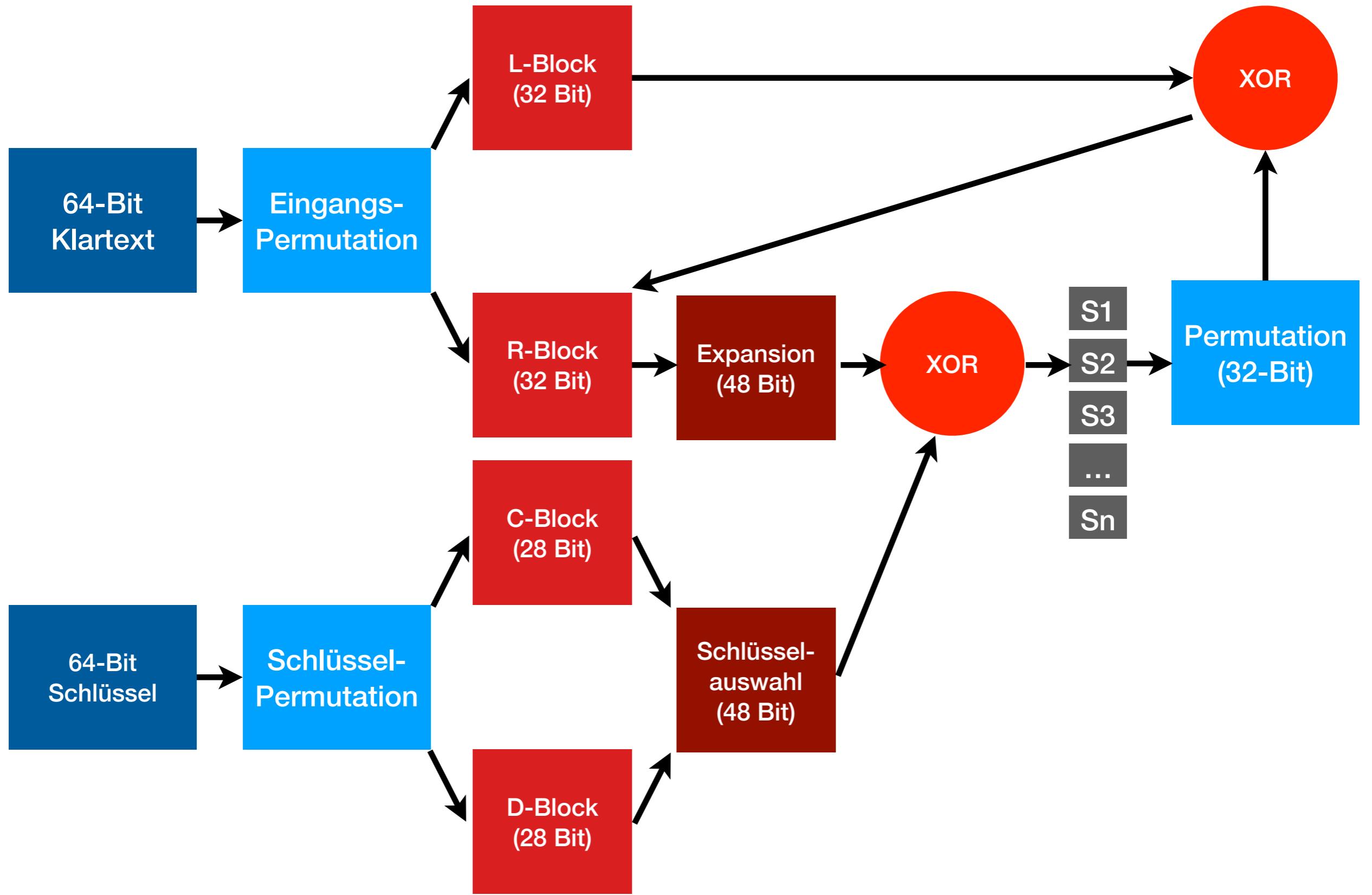
64-Bit
Schlüssel

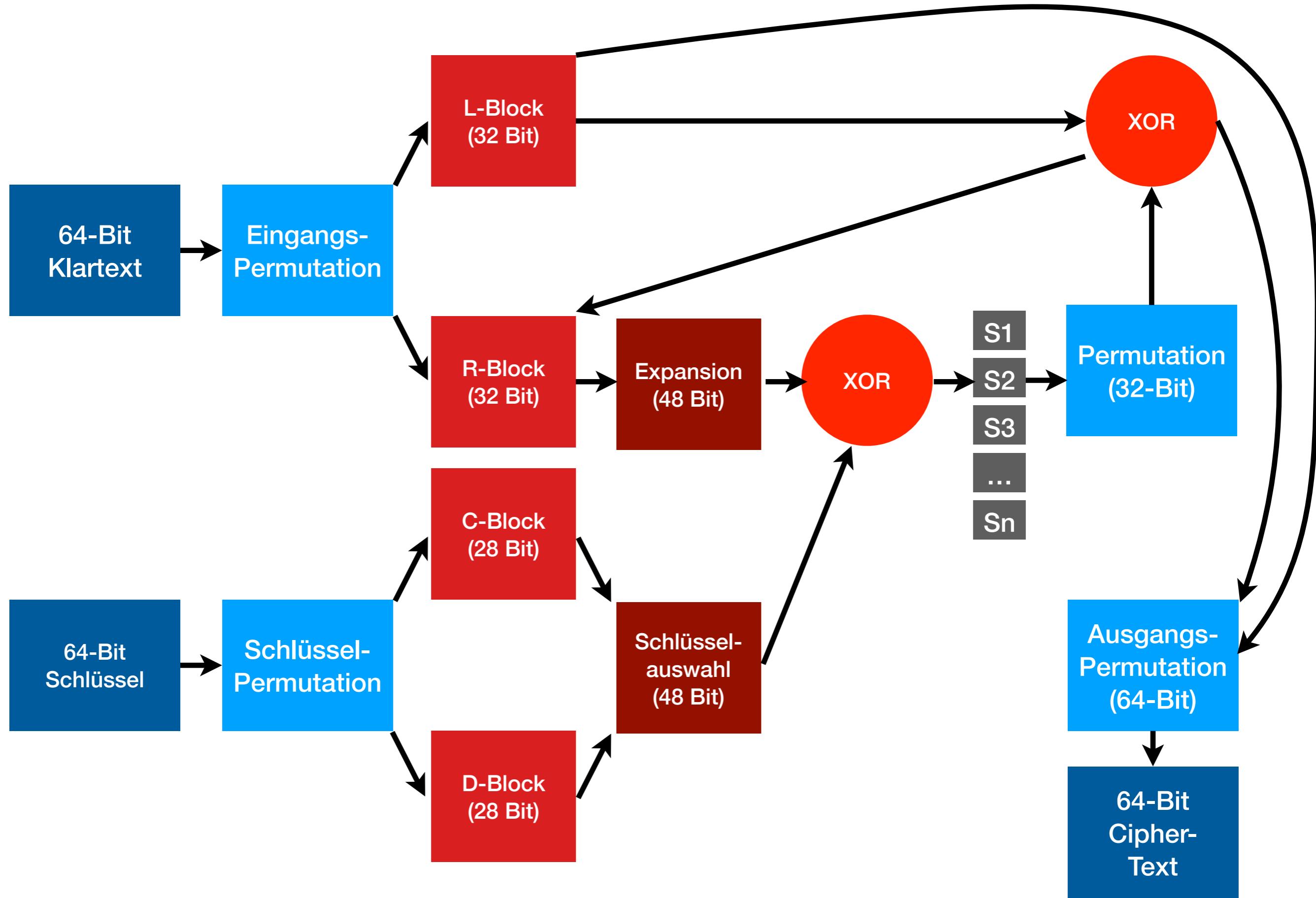












3DES

- 3DES / TripleDES / TDES / DESede, 1981

$$\begin{aligned} \text{3DES(Msg, } &K_1, K_2, K_3) = \\ \text{enc(dec(enc(Msg, } &K_1) , K_2) , K_3) } \end{aligned}$$

Further Reading

- <https://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm>
- Weitere Links in Moodle

IDEA

- Entstanden 1990 ETH Zürich und Ascom Systec AG
- Patentiert bis 2011
- 128-Bit Schlüssel
- 64-Bit Blöcke
- 8 Runden + 1/2 Ausgaberunde

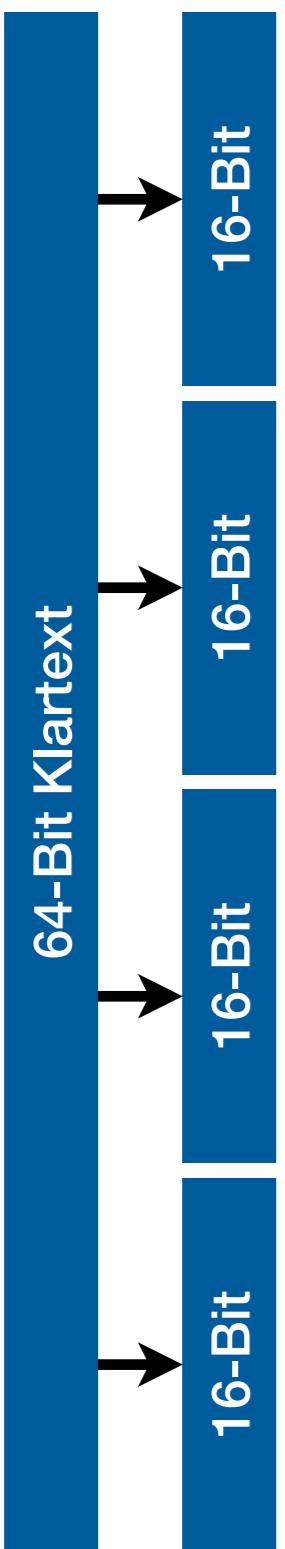
IDEA - Key-Erzeugung

- Jede Runde nutzt 6 16-Bit-Teilschlüssel } $8 \cdot 6 + 4$
- Ausgaberunde 4 16-Bit-Teilschlüssel
- Key-Erzeugung:
 - 128-Bit Schlüssel in 8 16-Bit Teilkeys $T_1 - T_8$ zerlegen
 - $T_1 - T_6$: Rundenschlüssel
 - $T_1 - T_4$: Ausgabenrundenschlüssel
 - Pro Runde: Rotiere Key 25 Bit nach links

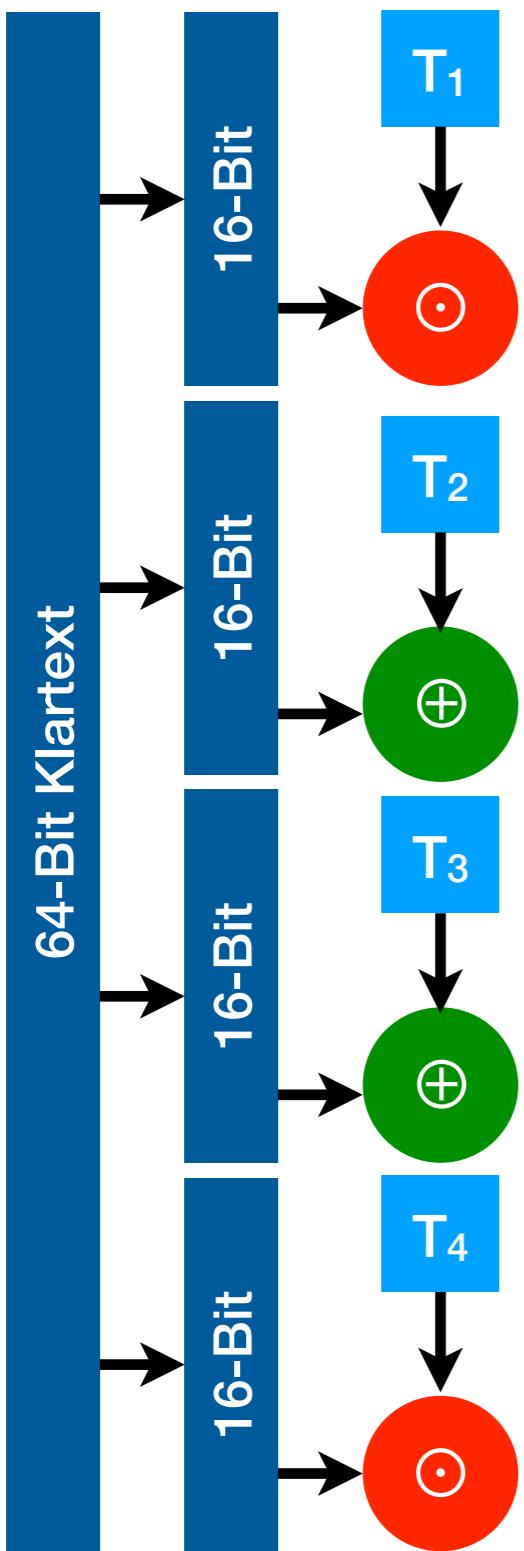
IDEA - Operationen

- XOR
- Addition mod $2^{16} \oplus$ (16-Bit-Wert)
- Multiplikation mod $2^{16}+1 \odot$
 - Besonderheit: Ergebnis 0000 wird FFFF (hex)
Ergo: 16-Bit-Wert, Wertebereich 0001 - FFFF (hex)

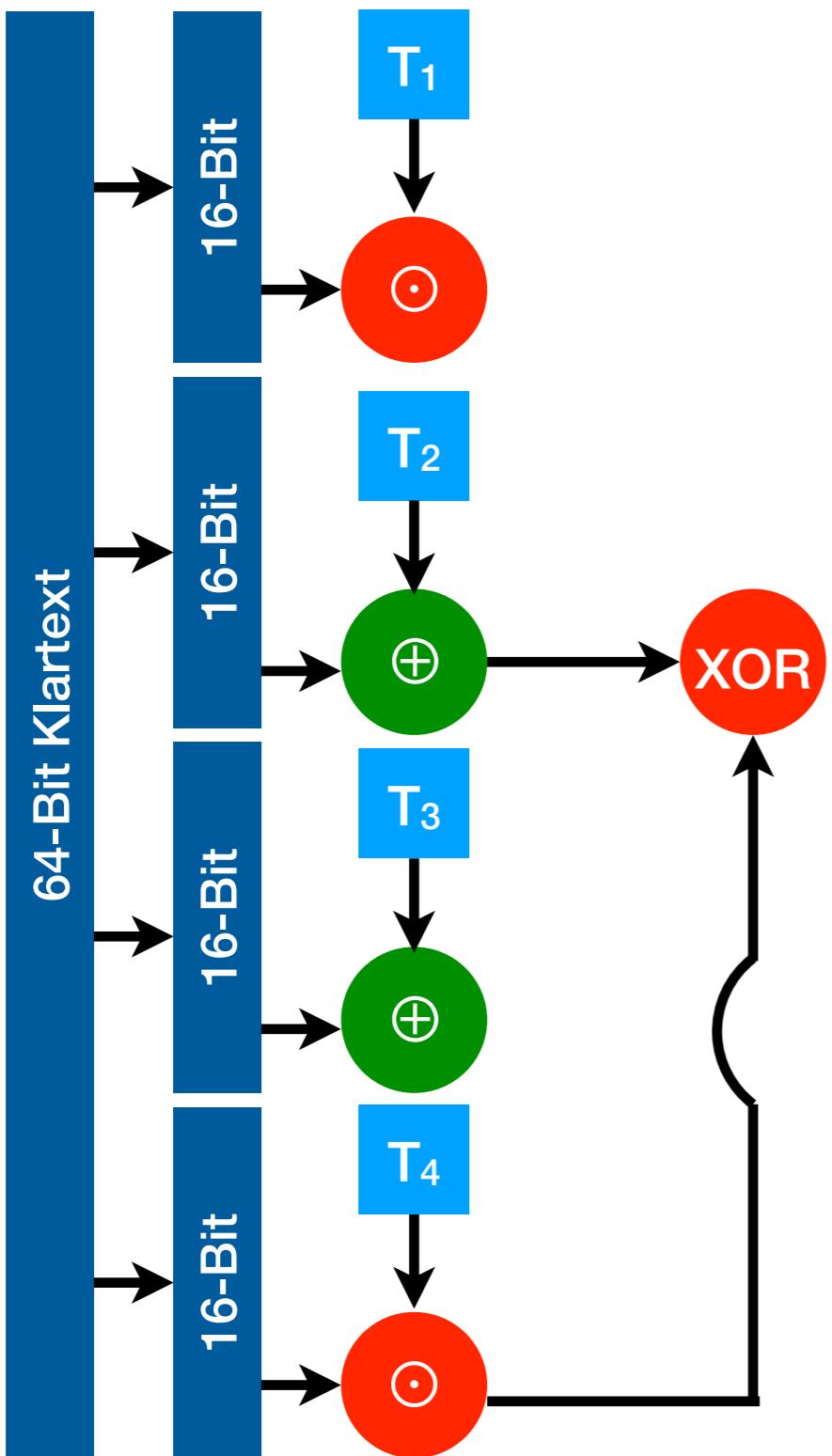
IDEA: Eine Runde



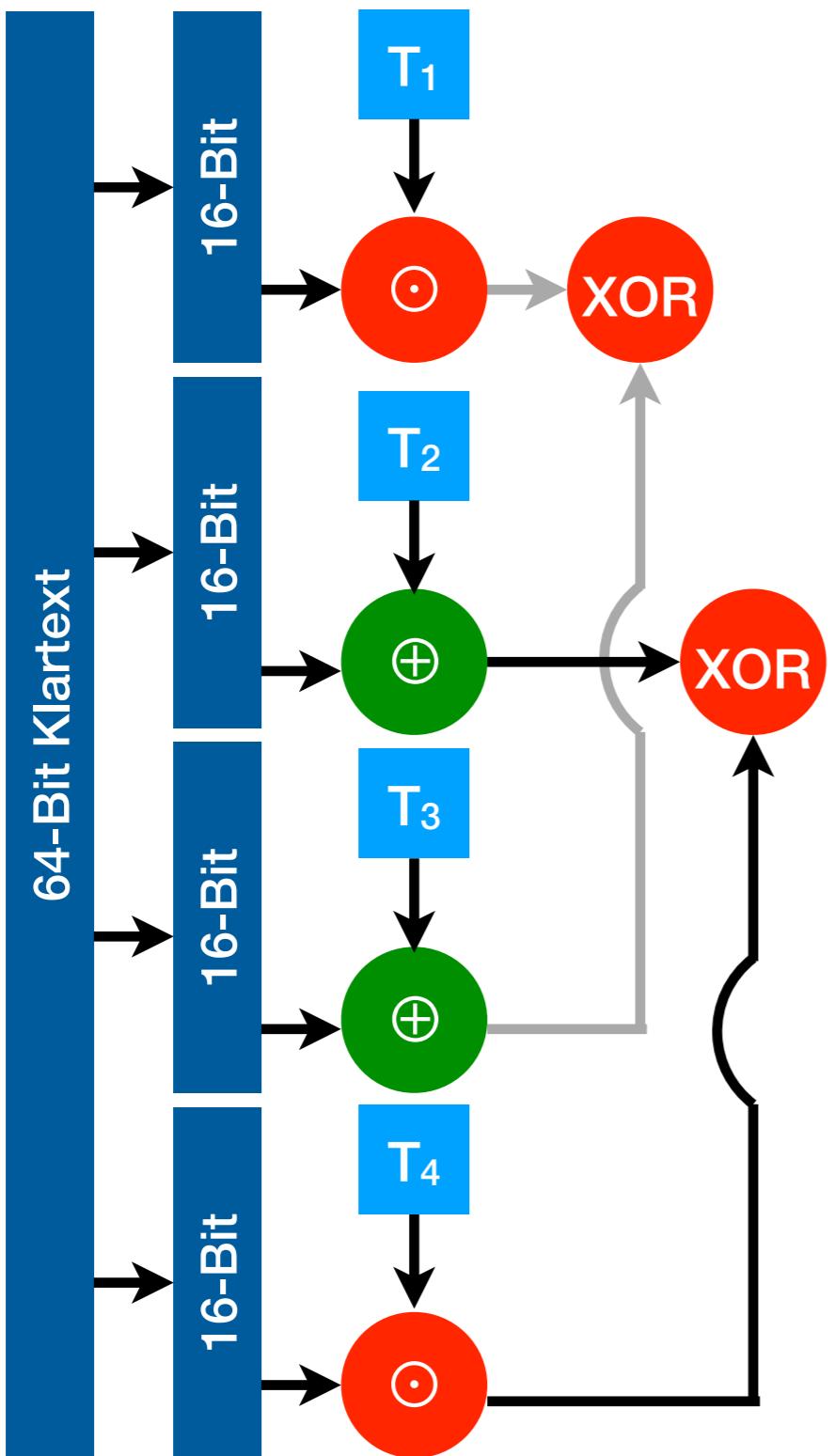
IDEA: Eine Runde



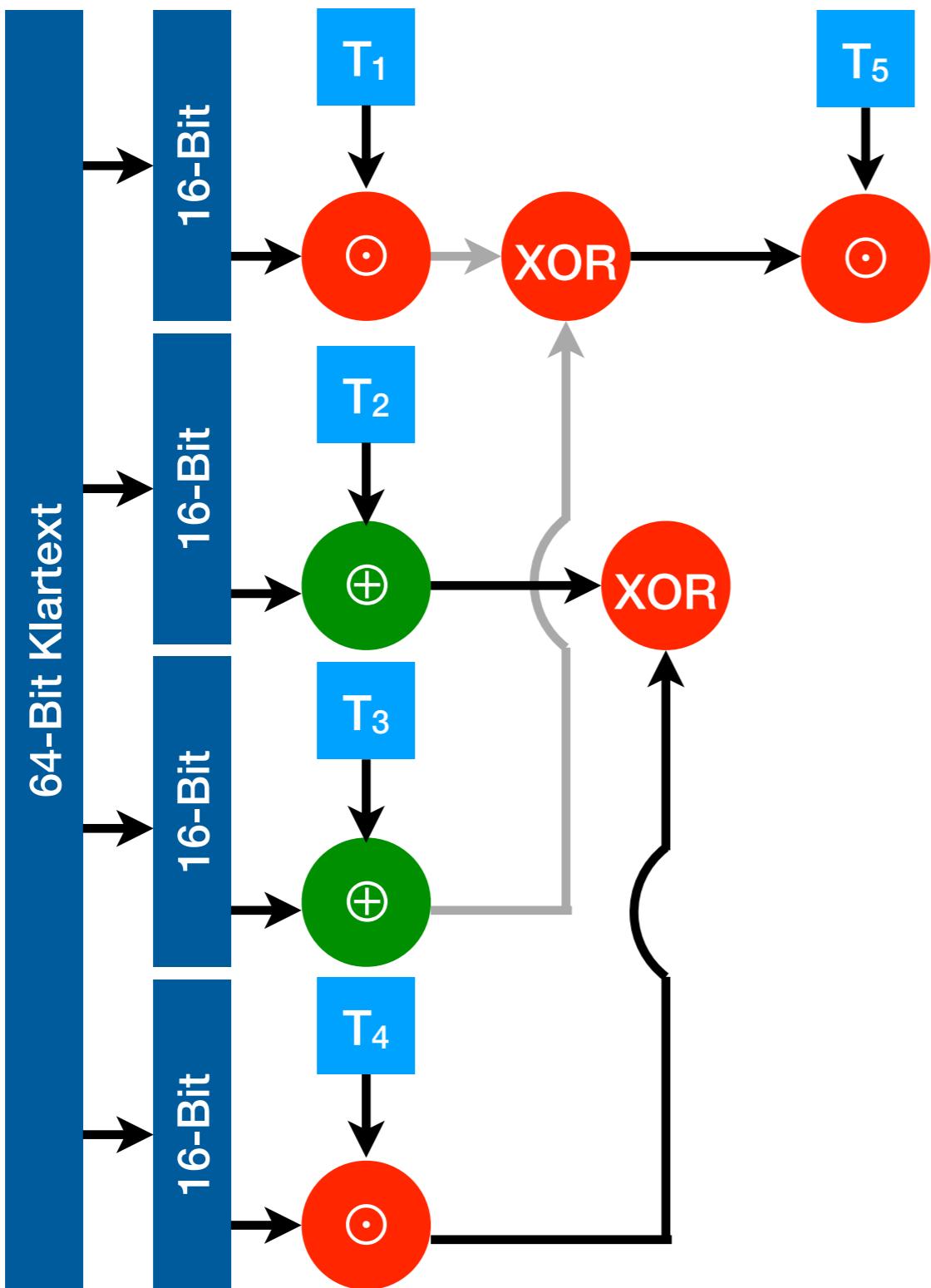
IDEA: Eine Runde



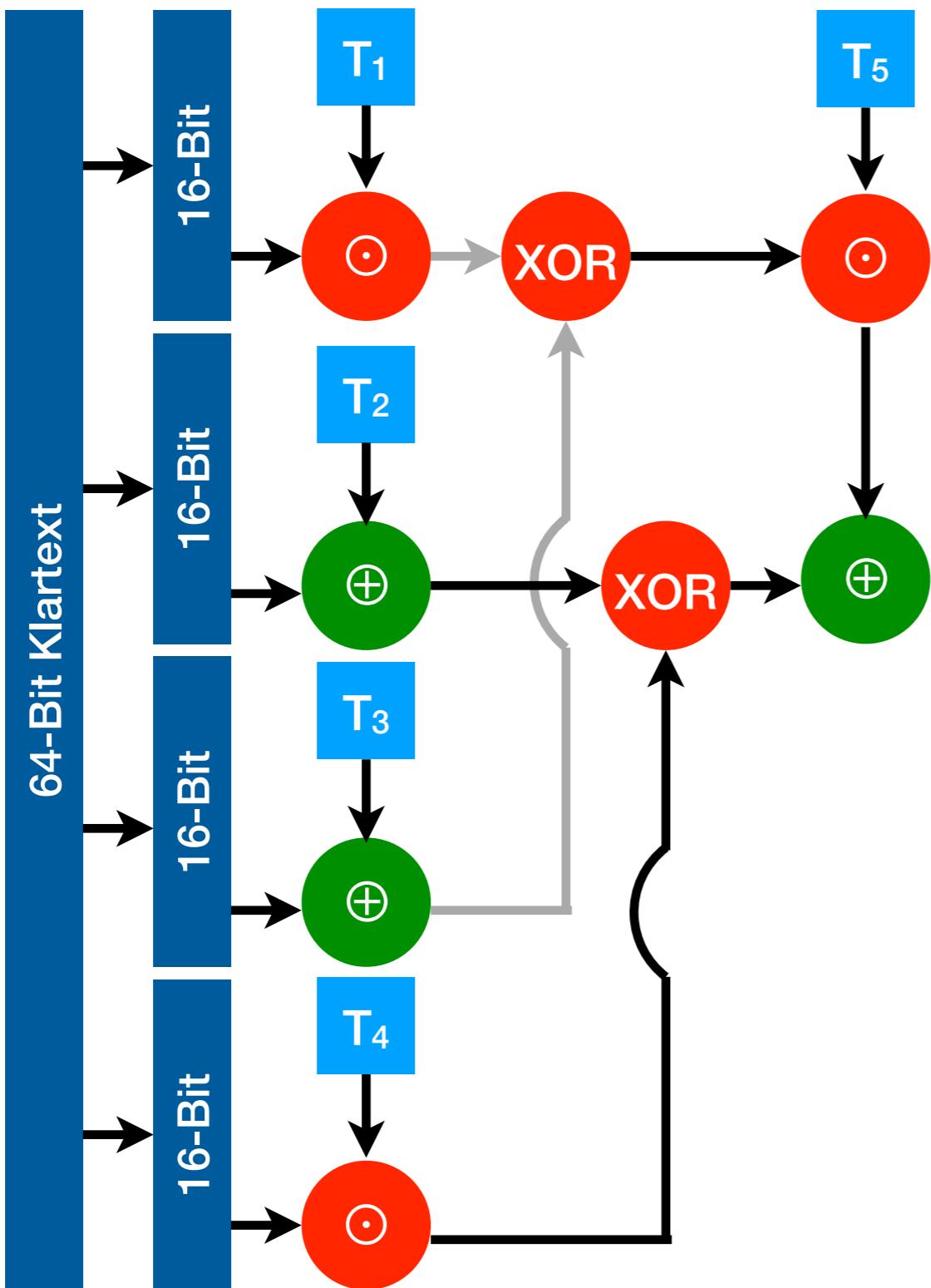
IDEA: Eine Runde



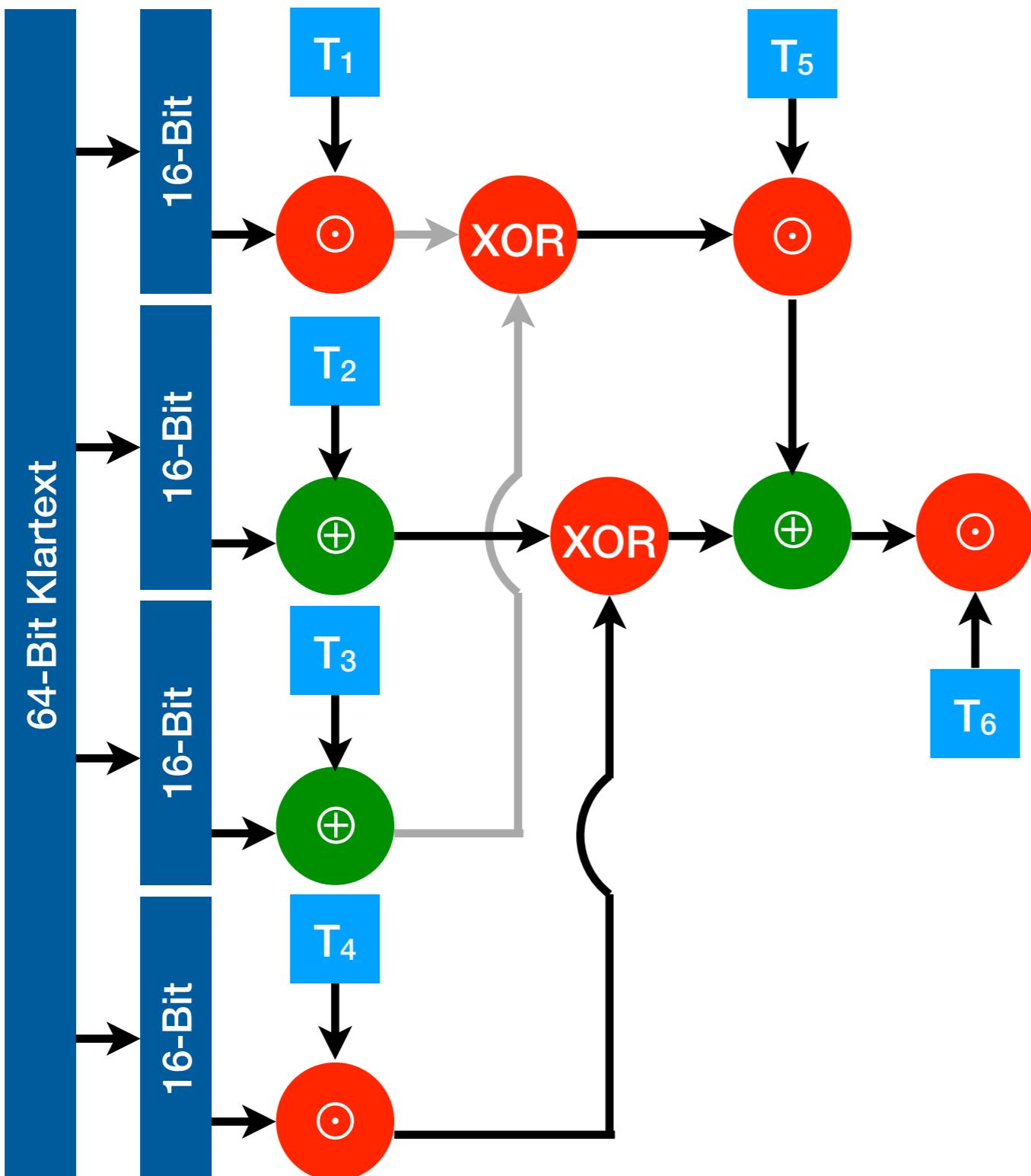
IDEA: Eine Runde



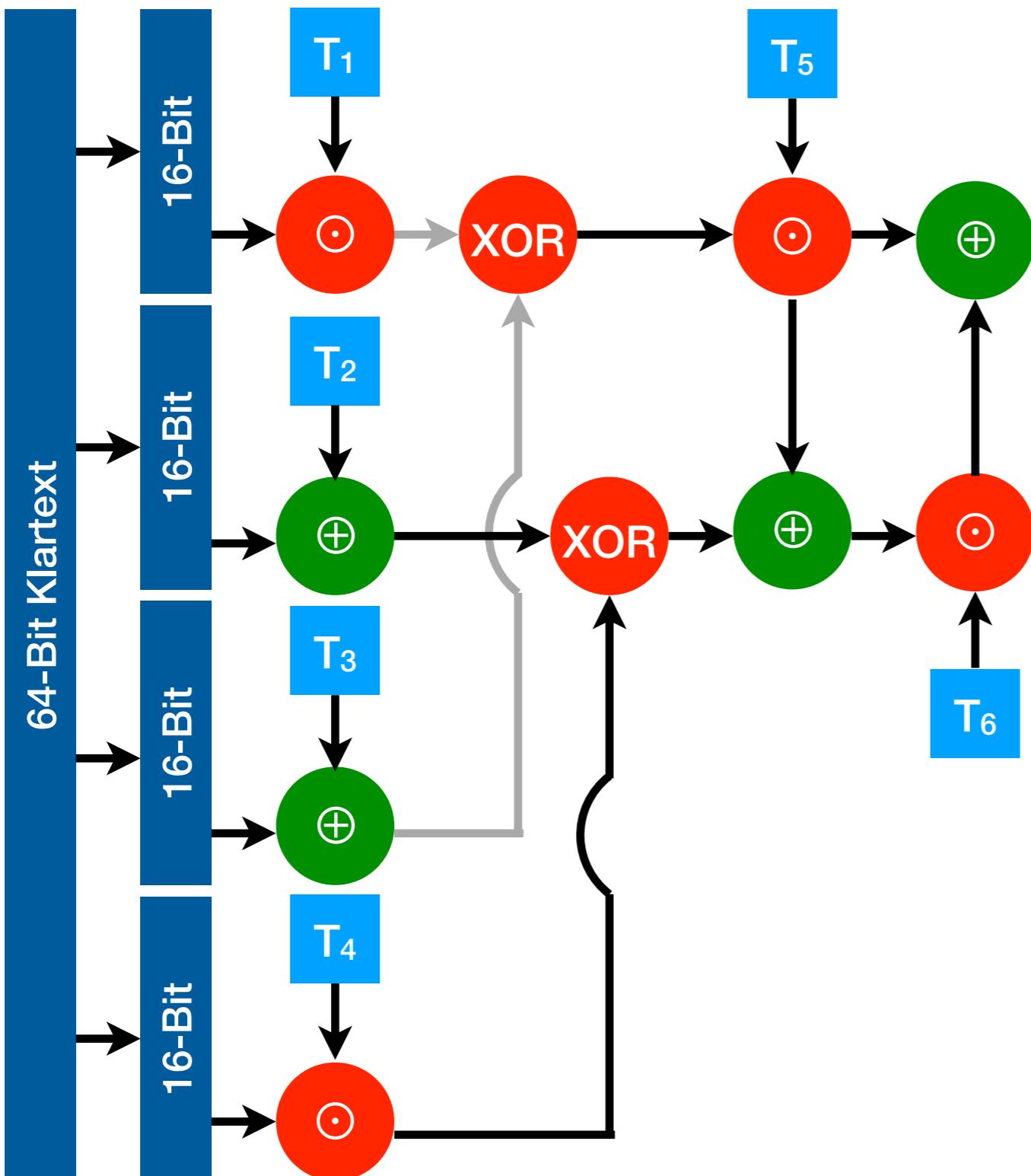
IDEA: Eine Runde



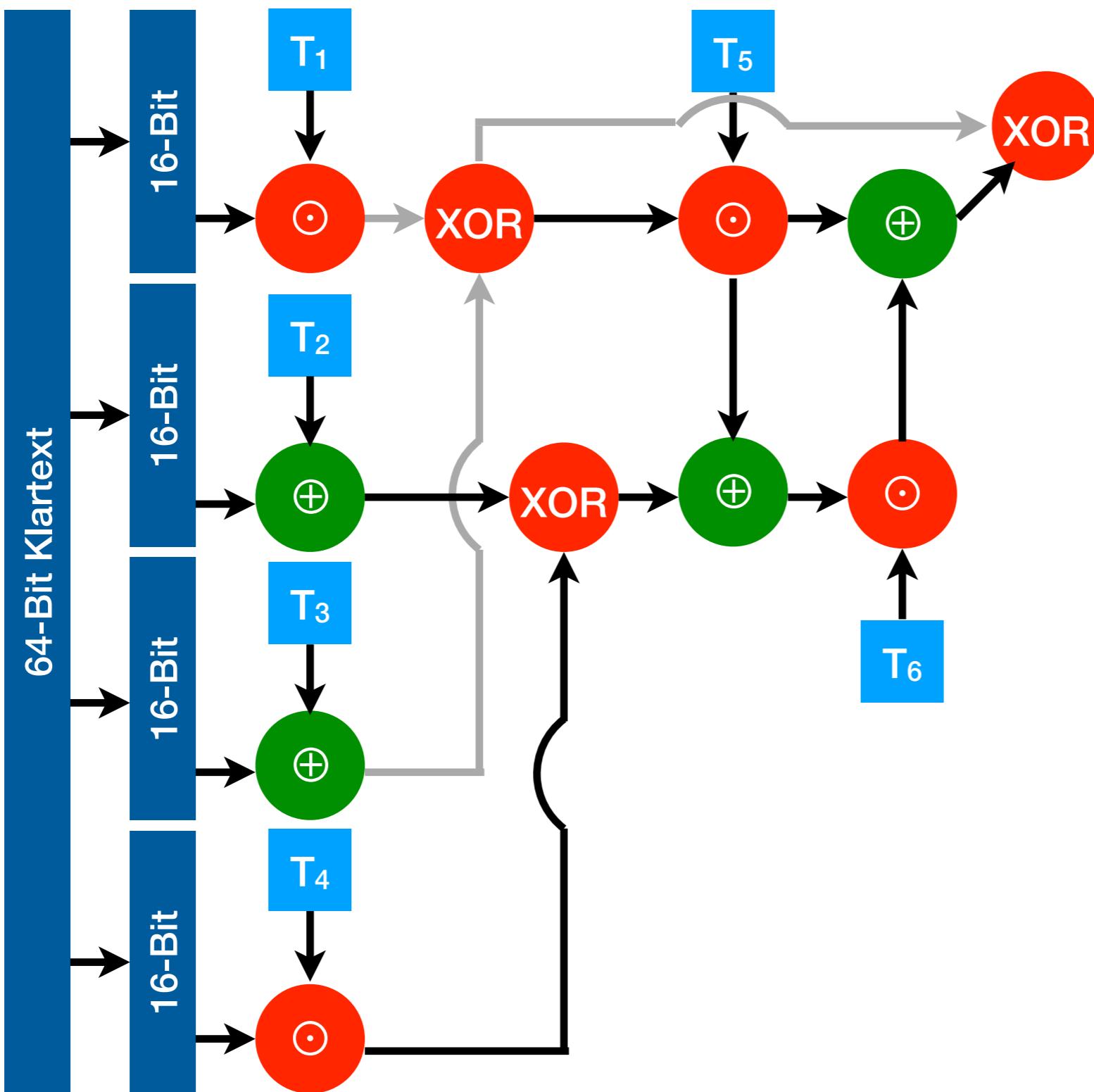
IDEA: Eine Runde



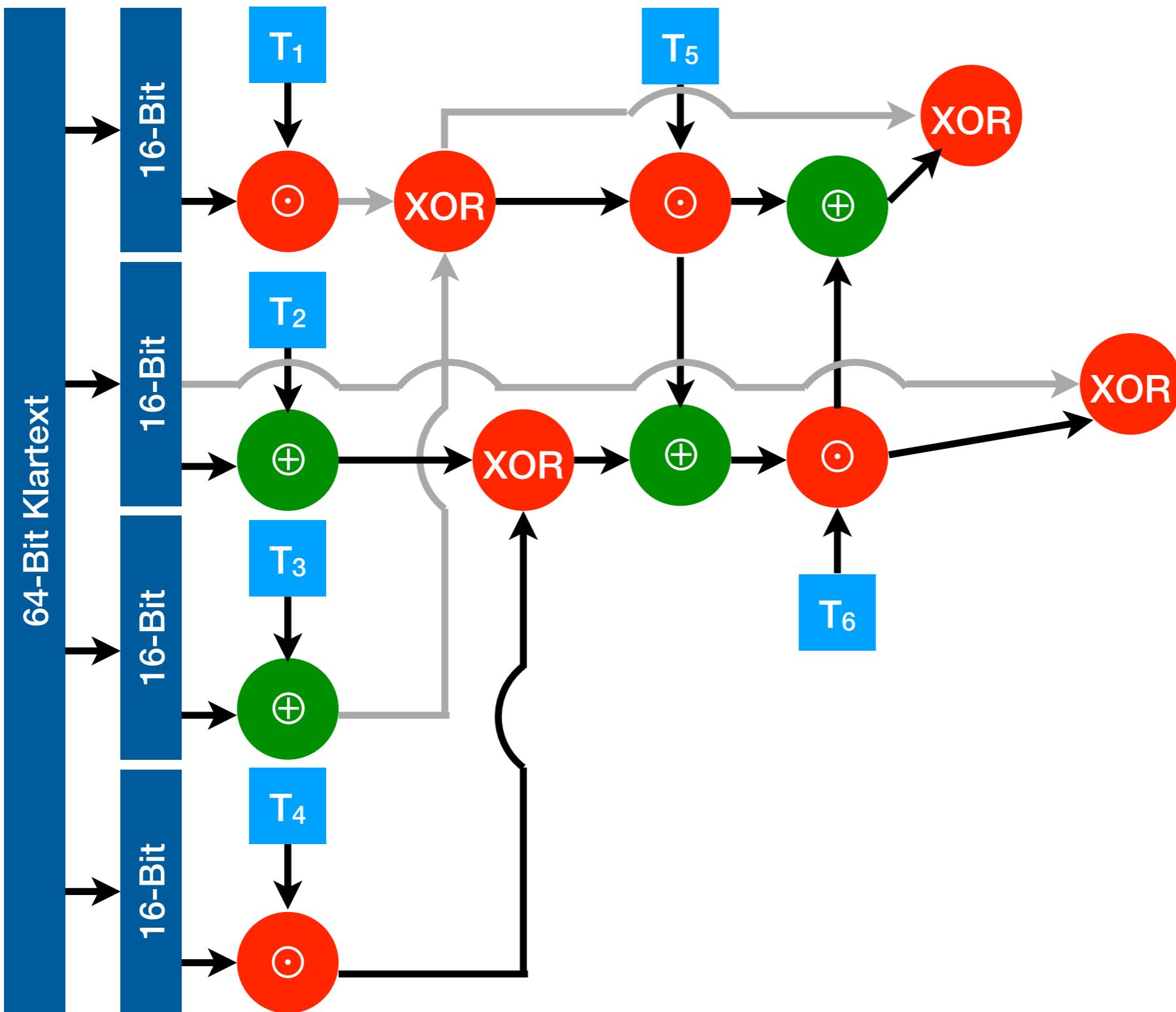
IDEA: Eine Runde



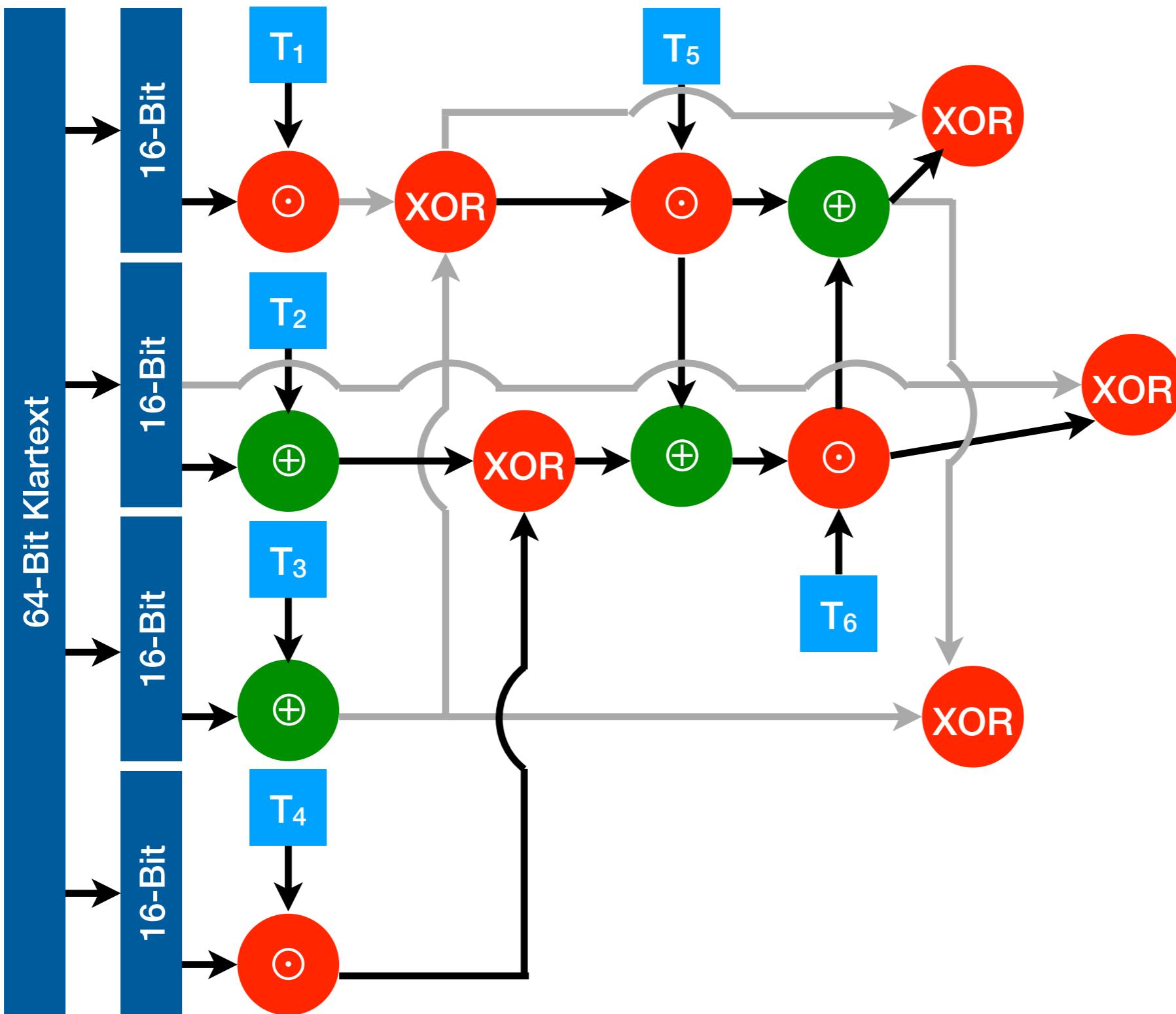
IDEA: Eine Runde



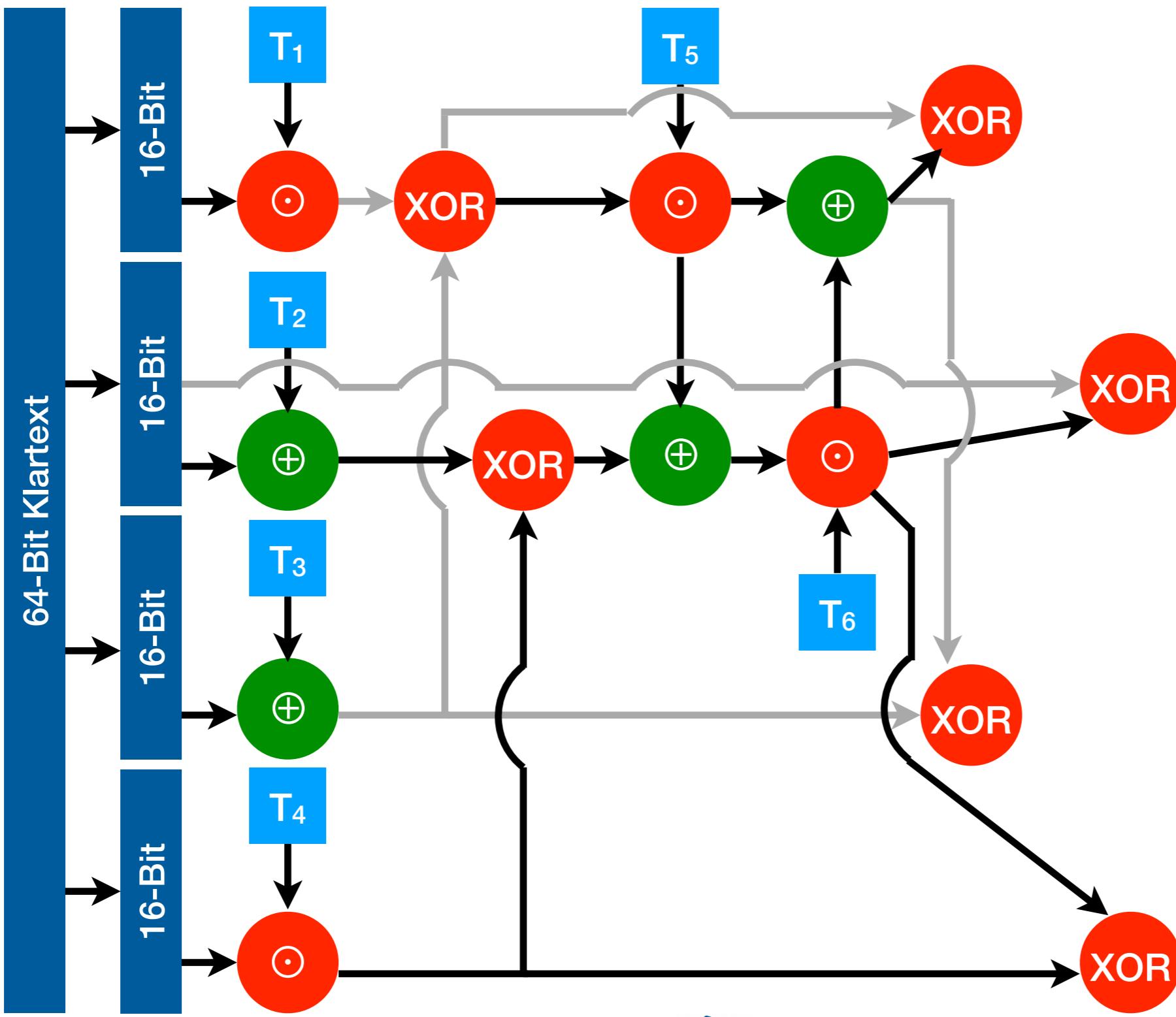
IDEA: Eine Runde



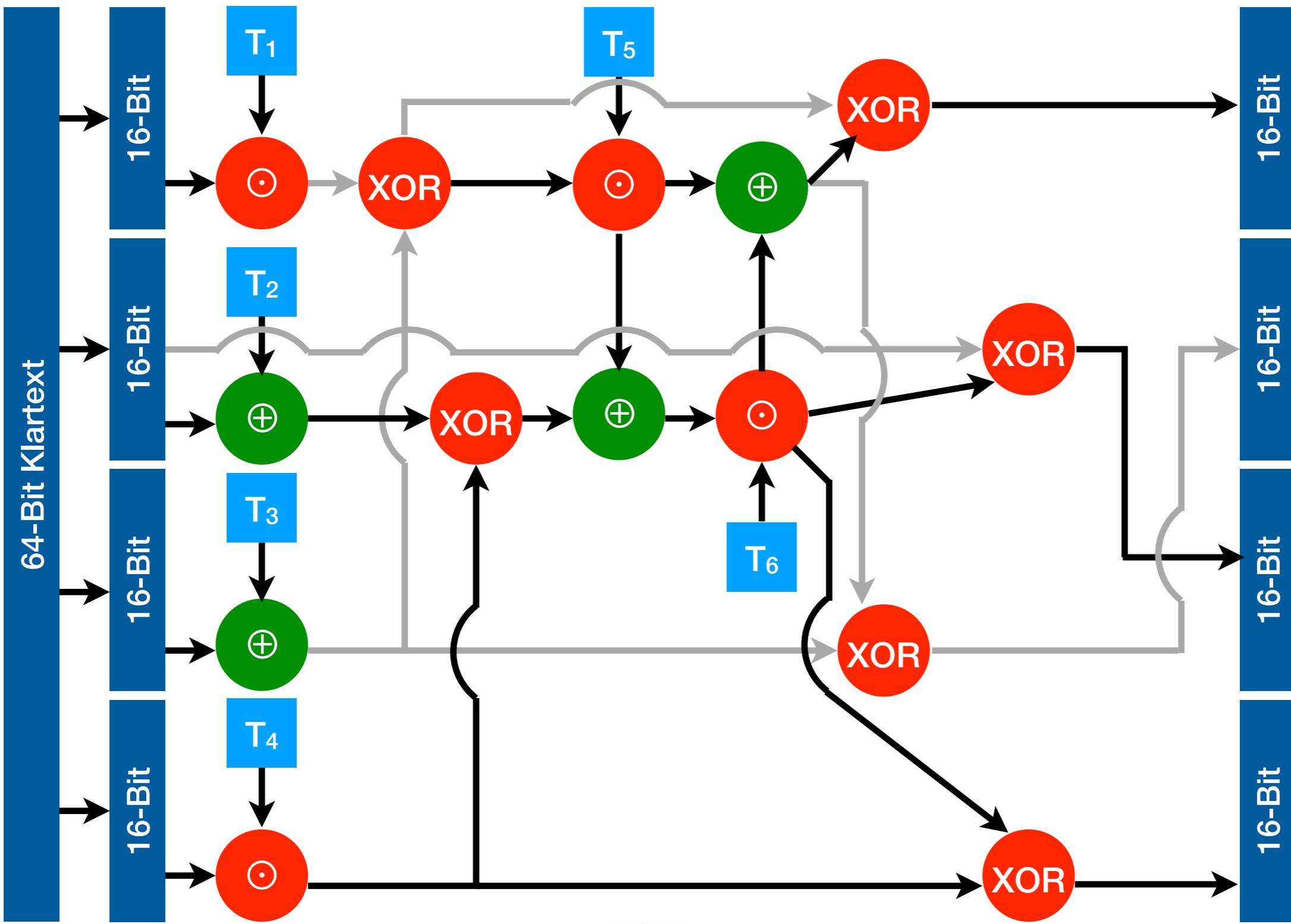
IDEA: Eine Runde



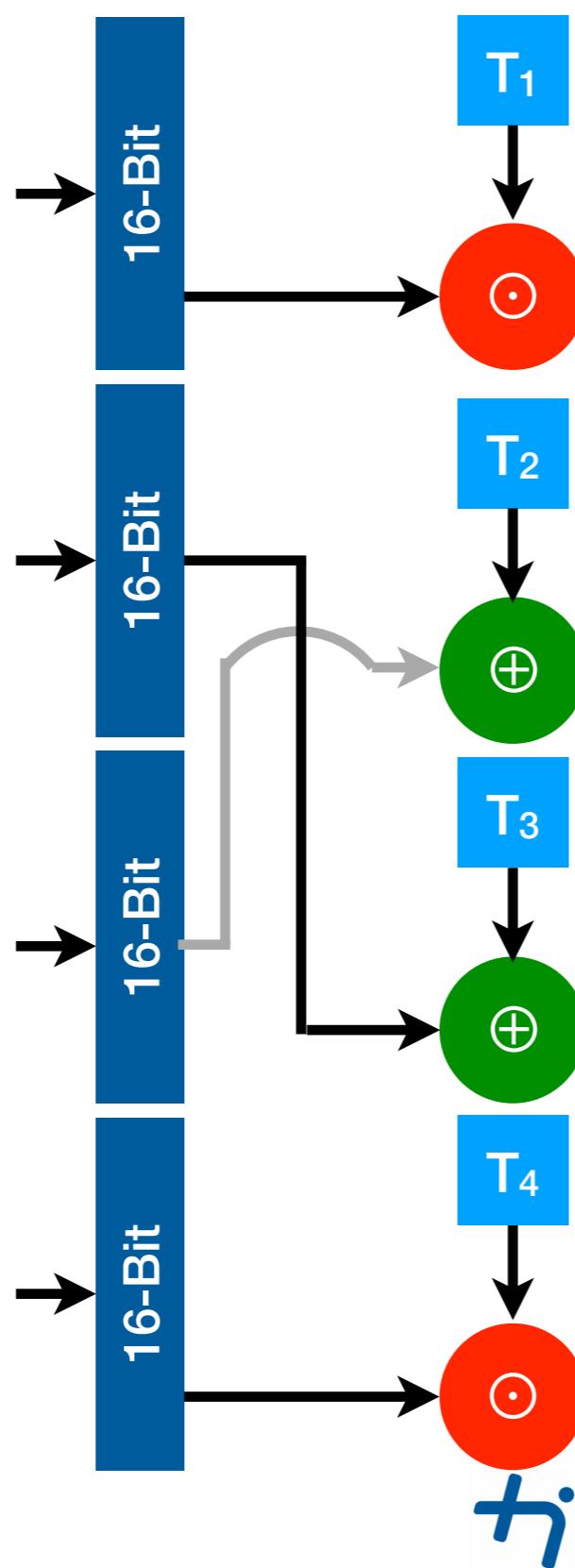
IDEA: Eine Runde



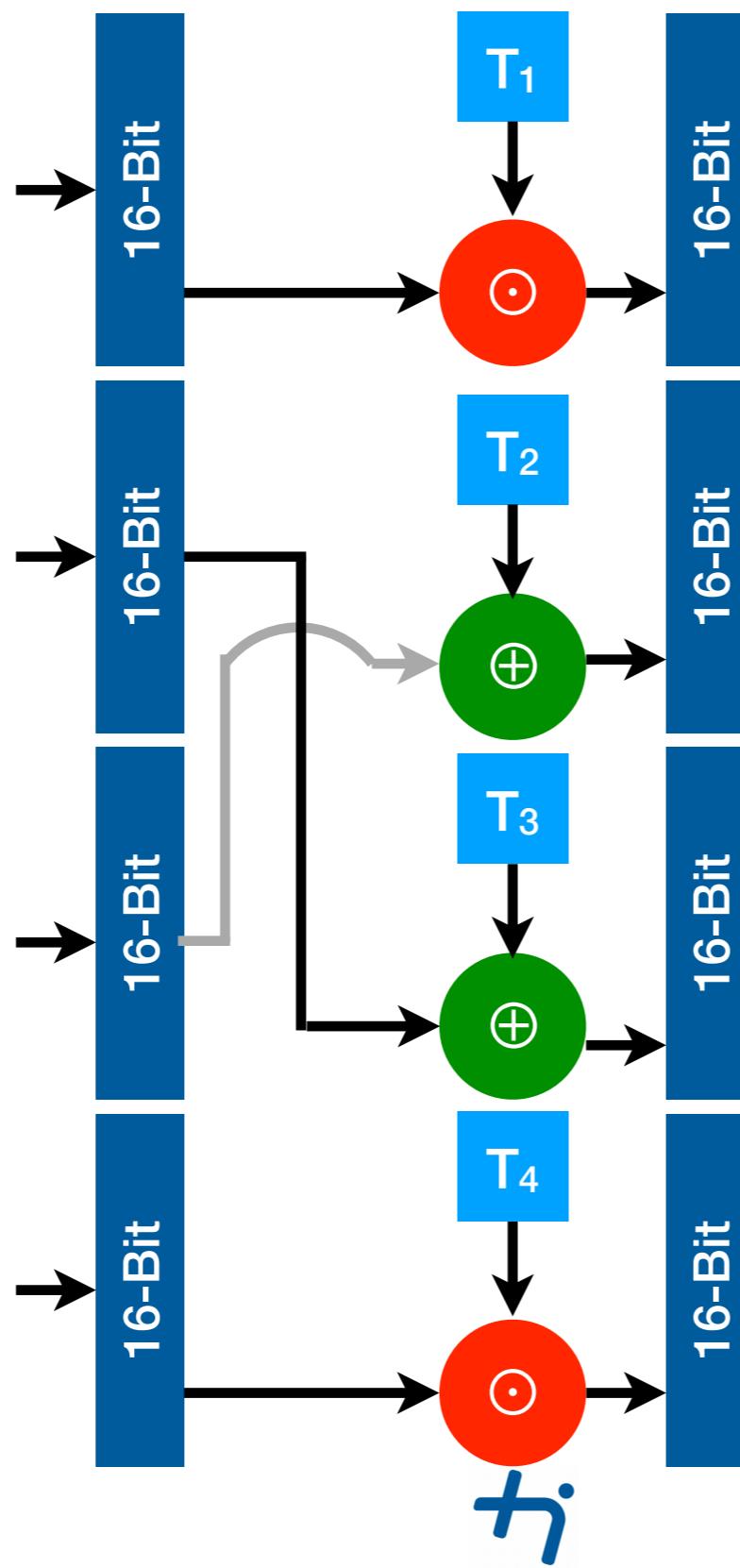
IDEA: Eine Runde



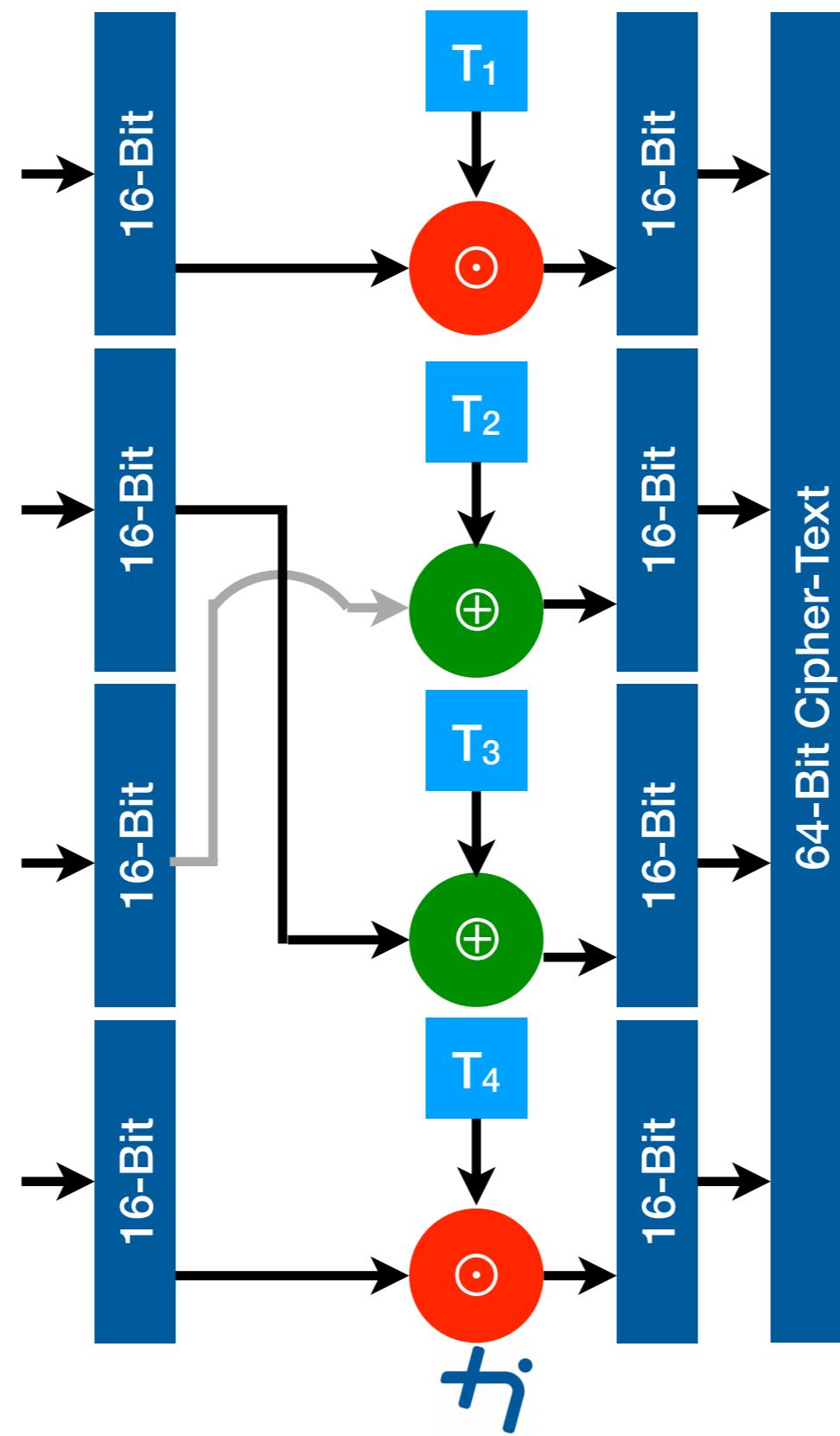
IDEA: Abschluß-Runde



IDEA: Abschluß-Runde



IDEA: Abschluß-Runde



Further Reading

- IDEA-Paper in Moodle

AES

- Advanced Encryption Standard
- 2000 „in Dienst gestellt“
- 128-Bit Blöcke
- Schlüssellänge 128, 160, 192, 224, 256 Bit
(orange: zugelassen in US für TOP SECRET)
- Hardware-Support gut möglich

Theoretisch gebrochen

- Bedingung:
Aufwand zum Entschlüsseln < Key Brute-Force
- Praxis: unrealistisch hoher Aufwand
 - AES 128 $2^{126,1} = 9 \cdot 10^{37}$ Schritte
 - AES 192 $2^{189,7} = 10^{57}$ Schritte
 - AES 256 $2^{254,4} = 3 \cdot 10^{76}$ Schritte
- Damit: Praktisch sicher

Ablauf

- Schlüssel-Expansion
- Rundenschlüssel erzeugen
- Verschlüsselungsrunden (nach Schlüssellänge)
 - Substitute-Bytes (SubBytes)
 - ShiftRows
 - MixColumns
 - Rundenschlüssel erzeugen
- Schlussrunde
 - SubBytes
 - ShiftRows
 - Rundenschlüssel erzeugen

Anzahl der Runden

Schlüssel-länge	AES-128	AES-160	AES-192	AES-224	AES-256
Runden	10	11	12	13	14

Beispiel

- Key: TE@TH-INGOLSTADT
Hex: 54 45 40 54 48 2D 49 4E 47 4F 4C 53 54 41 44 54
- Nachricht: Krypto-Einführung
Hex: 4B 72 79 70 74 6F 2D 45 69 6E 66 C3 BC 68 72 75 6E 67
- Geheimtext ist dann:
DA 41 83 EB 4D A0 AC 8F EC C8 F7 62 74 24 19 60 1B 11 37 BF 2C FC 10 4B FE A7 02 95 A5 A2 4D 22

Beispiel

- Key: TE@TH-INGOLSTADT
Hex: 54 45 40 54 48 2D 49 4E 47 4F 4C 53 5A
- Nachricht: Krypto-Einführung
Hex: 4B 72 79 70 74 6F 2D 45 69 6E 66
6E 67
- Geheimtext ist dann:
DA 41 83 EB 4D A0 AC 8F EC C8 F7 62 74 24 19 60
1B 11 37 BF 2C FC 10 4B FE A7 02 95 A5 A2 4D 22

Padding ersichtlich

Beispiel

- Key: TE@TH-INGOLSTADT
Hex: 54 45 40 54 48 2D 49 4E 47 4F 4C 53 54 41 44 54
- Nachricht: Krypto-Einführung
Hex: 4B 72 79 70 74 6F 2D 45 69 6E 66 C3 BC 68 72 75 6E 67
- Geheimtext ist dann:
DA 41 83 EB 4D A0 AC 8F EC C8 F7 62 74 24 19 60 1B 11 37 BF 2C FC 10 4B FE A7 02 95 A5 A2 4D 22

Eingangsdaten

Nachricht (Erste 128 Bit)

Key (128 Bit)

Eingangsdaten

Nachricht (Erste 128 Bit)

Key (128 Bit)

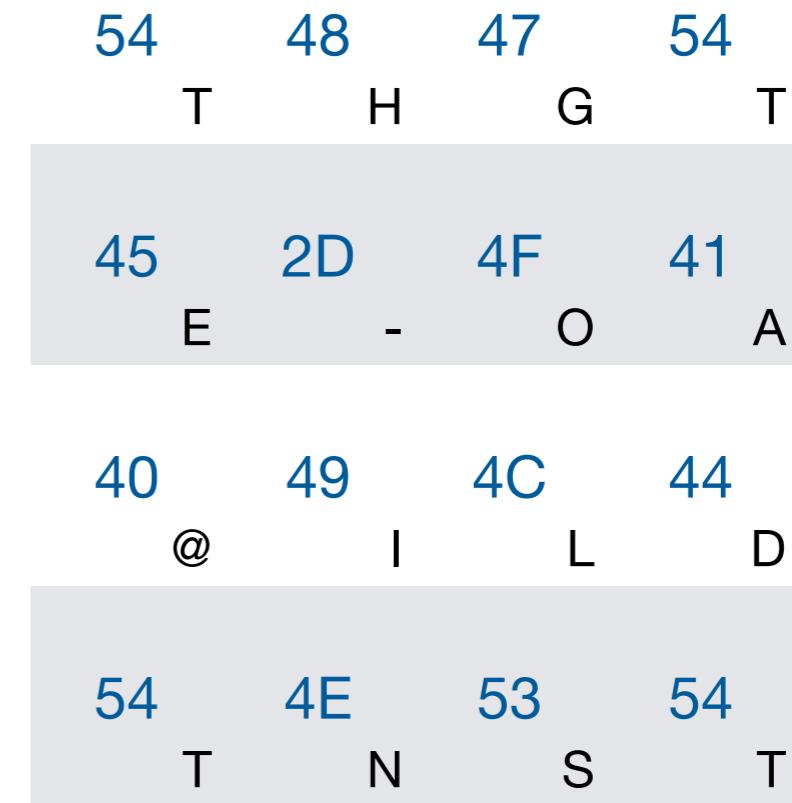


Eingangsdaten

Nachricht (Erste 128 Bit)



Key (128 Bit)



Substitute-Bytes

- Nimm Zellwert des Klartextes als Index in S-Box
- x: linkes Halbbyte, y: rechtes Halbbyte

		y																
		hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
		0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
		1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
		2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
		3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
		4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
		5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
		6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
		7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
		8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
		9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
		A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
		B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
		C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
		D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
		E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
		F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Substitute-Bytes

- Nimm Zellwert des Klartextes als Index in S-Box
- x: linkes Halbbyte, y: rechtes Halbbyte

hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Substitute-Bytes

- Nimm Zellwert des Klartextes als Index in S-Box
- x: linkes Halbbyte, y: rechtes Halbbyte

hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Substitute-Bytes

- Nimm Zellwert des Klartextes als Index in S-Box
- x: linkes Halbbyte, y: rechtes Halbbyte

hex	y															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

x

B3 92 F9 65 →
 40 A8 9F 45 →
 B6 D8 33 40 →
 51 6E 2E 9D →

Shift-Rows

B3 92 F9 65

40 A8 9F 45

B6 D8 33 40

51 6E 2E 9D

Shift-Rows

B3 92 F9 65

Rotation um 0 Byte

40 A8 9F 45

B6 D8 33 40

51 6E 2E 9D

Shift-Rows

B3 92 F9 65

Rotation um 0 Byte

A8 9F 45 40

Rotation um 1 Byte

B6 D8 33 40

51 6E 2E 9D

Shift-Rows

B3 92 F9 65

Rotation um 0 Byte

A8 9F 45 40

Rotation um 1 Byte

33 40 B6 D8

Rotation um 2 Byte

51 6E 2E 9D

Shift-Rows

B3 92 F9 65

Rotation um 0 Byte

A8 9F 45 40

Rotation um 1 Byte

33 40 B6 D8

Rotation um 2 Byte

9D 51 6E 2E

Rotation um 3 Byte

Mix-Columns

AES-Galois-Feld			
B3	92	F9	65
A8	9F	45	40
33	40	B6	D8
9D	51	6E	2E

Mix-Columns

AES-Galois-Feld

92 F9 65		02 03 01 01 B3
9F 45 40		01 02 03 01 A8
40 B6 D8		01 01 02 03 33
51 6E 2E		03 01 01 02 9D

\times =

Mix-Columns

AES-Galois-Feld		
92	F9	65
9F	45	40
40	B6	D8
51	6E	2E
02	03	01
01	02	03
01	01	02
03	01	01
B3		E5
A8		98
33		65
9D		4B

Reminder: Matrix \times Vektor

$$\begin{array}{cccc|c|c} 02 & 03 & 01 & 01 & \text{B3} & \text{E5} \\ \hline 01 & 02 & 03 & 01 & \text{A8} & 98 \\ 01 & 01 & 02 & 03 & 33 & 65 \\ 03 & 01 & 01 & 02 & 9D & 4B \end{array}$$

The diagram illustrates the multiplication of a 4x4 matrix by a 4x1 column vector. The matrix has columns labeled B3, A8, 33, and 9D. The column vector has entries E5, 98, 65, and 4B. The result of the multiplication is shown as a single value in each row.

Reminder: Matrix \times Vektor

Jedes Element der Zeile 1, also $m_{1,i}$

$$\begin{matrix} & \boxed{02} & 03 & 01 & 01 \\ \begin{matrix} 01 & 02 & 03 & 01 \end{matrix} & \times & \begin{matrix} B3 \\ A8 \end{matrix} & = & \begin{matrix} E5 \\ 98 \end{matrix} \\ & 01 & 01 & 02 & 03 \\ & 03 & 01 & 01 & 02 \end{matrix} \quad \begin{matrix} 33 \\ 9D \end{matrix} \quad \begin{matrix} 65 \\ 4B \end{matrix}$$

Reminder: Matrix \times Vektor

Jedes Element der Zeile 1, also $m_{1,i}$

multipliziert mit dem Wert in Zeile 1

$$\begin{array}{cccc} 02 & 03 & 01 & 01 \end{array} \boxed{\quad} \begin{array}{c} B3 \\ A8 \\ 33 \\ 9D \end{array} \times \begin{array}{c} E5 \\ = \\ 65 \\ 4B \end{array}$$

The diagram illustrates the calculation of a scalar product. It shows a row vector (matrix row) with elements 02, 03, 01, 01, followed by a box containing the label "B3". Below this is another row vector with elements 01, 02, 03, 01, followed by a box containing the label "A8". To the right of these is a multiplication symbol "x". Further to the right is an equals sign "=" followed by a box containing the label "E5". Below the first row vector is another row vector with elements 01, 01, 02, 03, followed by a box containing the label "33". Below the second row vector is another row vector with elements 03, 01, 01, 02, followed by a box containing the label "9D". To the right of the multiplication symbol is a box containing the label "65". To the right of the equals sign is a box containing the label "4B".

Reminder: Matrix \times Vektor

Jedes Element der Zeile 1, also $m_{1,i}$

multipliziert mit dem Wert in Zeile 1

darüber die Summe.

$$\begin{array}{cccc} 02 & 03 & 01 & 01 \end{array} \boxed{\quad} \begin{array}{c} B3 \\ \times \\ A8 \end{array} = \begin{array}{c} E5 \\ 98 \\ 65 \\ 4B \end{array}$$
$$\begin{array}{cccc} 01 & 02 & 03 & 01 \end{array}$$
$$\begin{array}{cccc} 01 & 01 & 02 & 03 \end{array}$$
$$\begin{array}{cccc} 03 & 01 & 01 & 02 \end{array}$$

Reminder: Matrix \times Vektor

Jedes Element der Zeile 1, also $m_{1,i}$

multipliziert mit dem Wert in Zeile 1

darüber die Summe.

$$\begin{matrix} \boxed{02} & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{matrix} \times \begin{matrix} B3 \\ A8 \\ 33 \\ 9D \end{matrix} = \begin{matrix} E5 \\ 98 \\ 65 \\ 4B \end{matrix}$$

Weil es AES ist,
modulo 256

Reminder: Matrix \times Vektor

$$\begin{array}{c} \boxed{02 \quad 03 \quad 01 \quad 01} \\ \begin{array}{cccc} 01 & 02 & 03 & 01 \end{array} \\ \begin{array}{cccc} 01 & 01 & 02 & 03 \end{array} \\ \begin{array}{cccc} 03 & 01 & 01 & 02 \end{array} \end{array} \times \begin{array}{c} \text{B3} \\ \text{A8} \\ 33 \\ 9D \end{array} = \begin{array}{c} \text{E5} \\ 98 \\ 65 \\ 4B \end{array}$$

$$\sum_{i=1}^4 (m_{1,i} * v_1) \bmod 256$$

Zurück zu: Mix-Columns

AES-Galois-Feld

92 F9 65		02 03 01 01		B3	E5
9F 45 40		01 02 03 01		A8	98
40 B6 D8		01 01 02 03		x	=
51 6E 2E		03 01 01 02		33	65
				9D	4B

Zurück zu: Mix-Columns

AES-Galois-Feld			
E5	92	F9	65
98	9F	45	40
65	40	B6	D8
4B	51	6E	2E
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

× =

Zurück zu: Mix-Columns

AES-Galois-Feld		
E5	F9 65	02 03 01 01 92 FE
98	45 40	01 02 03 01 9F = 59
65	B6 D8	01 01 02 03 40 C0
4B	6E 2E	03 01 01 02 51 37

Zurück zu: Mix-Columns

AES-Galois-Feld			
E5	FE	F9	65
98	59	45	40
65	C0	B6	D8
4B	37	6E	2E

\times =

Zurück zu: Mix-Columns

AES-Galois-Feld

E5	FE	65	
98	59	40	
65	C0	D8	
4B	37	2E	

× =

02	03	01	01	F9	CF
01	02	03	01	45	E3
01	01	02	03	B6	FA
03	01	01	02	6E	2

Zurück zu: Mix-Columns

AES-Galois-Feld			
E5	FE	CF	65
98	59	E3	40
65	C0	FA	D8
4B	37	2	2E
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02
		x	=

Zurück zu: Mix-Columns

AES-Galois-Feld		
E5	FE	CF
98	59	E3
65	C0	FA
4B	37	2
02	03	01
01	02	03
01	01	02
03	01	01
65	40	C3
01	02	01
01	01	03
03	01	02
x		=
D8	2E	E8
		42

Zurück zu: Mix-Columns

AES-Galois-Feld			
E5	FE	CF	C3
98	59	E3	C0
65	C0	FA	E8
4B	37	2	42
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02
		x	=

Add Round Key

Neuer Rundenschlüssel

=

Aktuelle Verschlüsselungsmatrix

XOR

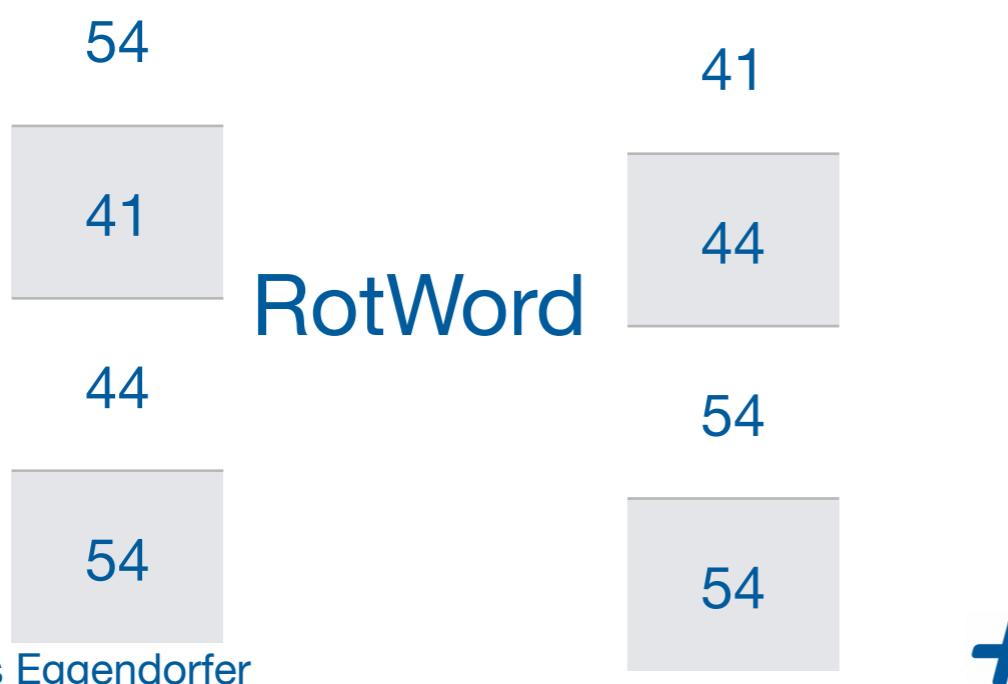
aktueller Rundenschlüssel

Schlüsselextension

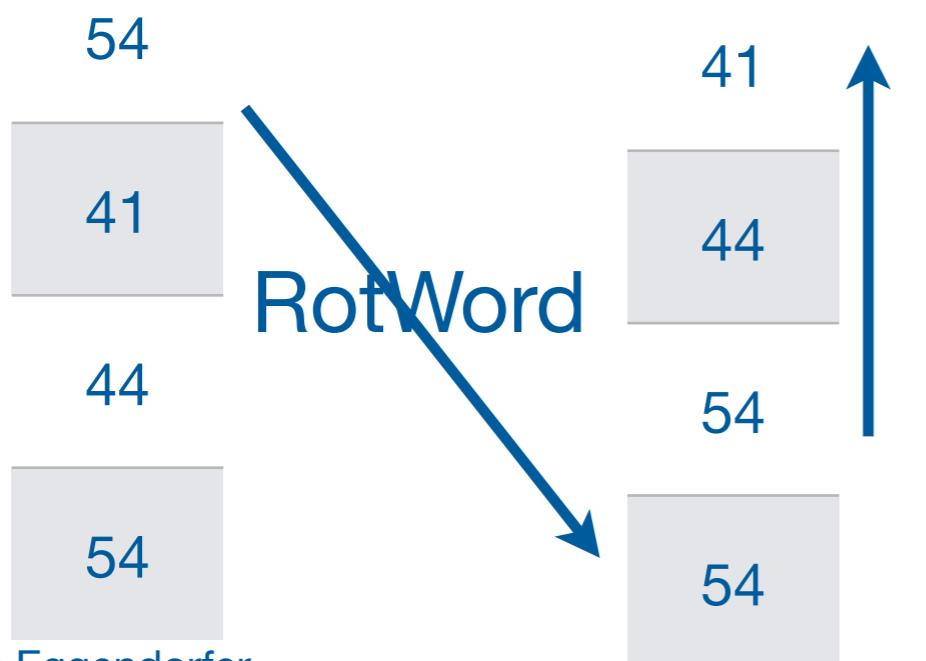
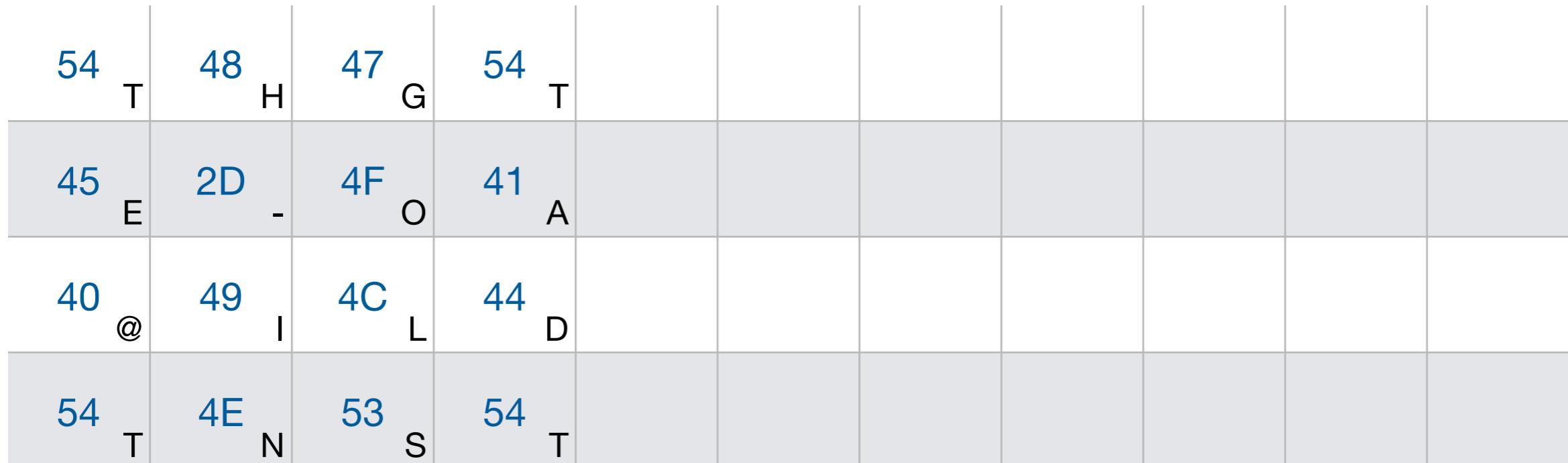
54	T	48	H	47	G	54	T
45	E	2D	-	4F	O	41	A
40	@	49	I	4C	L	44	D
54	T	4E	N	53	S	54	T

Schlüsselexpansion

54	T	48	H	47	G	54	T
45	E	2D	-	4F	O	41	A
40	@	49	I	4C	L	44	D
54	T	4E	N	53	S	54	T

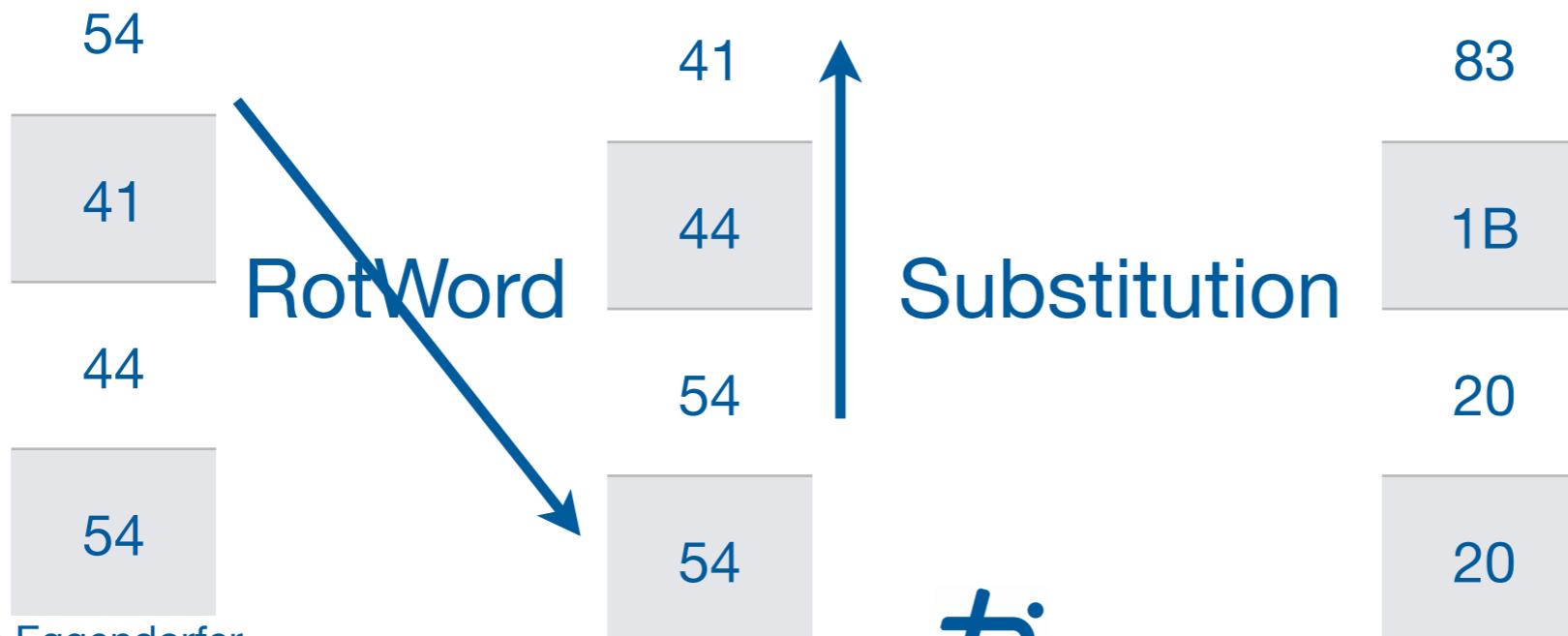


Schlüsselextension



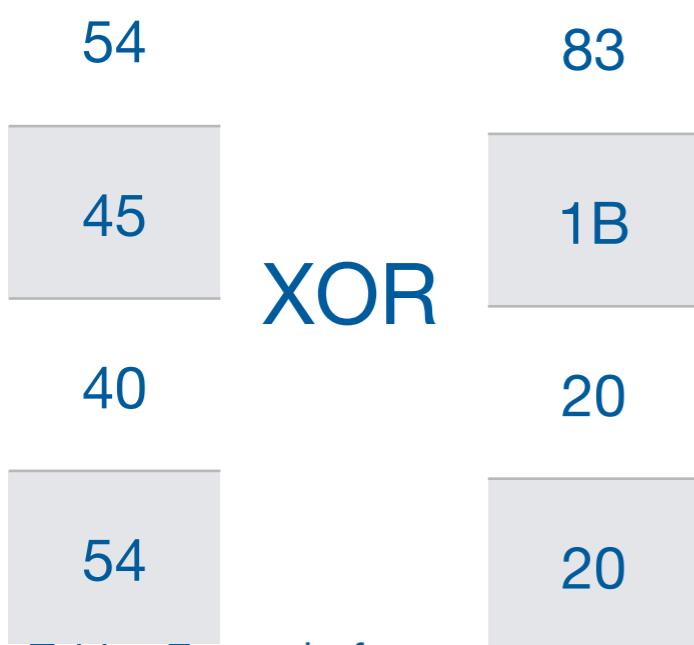
Schlüsselexpandion

T	48	H	47	G	54	T
E	2D	-	4F	O	41	A
@	49	I	4C	L	44	D
T	4E	N	53	S	54	T



Schlüsselexpansion

54	T	48	H	47	G	54	T
45	E	2D	-	4F	O	41	A
40	@	49	I	4C	L	44	D
54	T	4E	N	53	S	54	T



Schlüsselexpansion

54	T	48	H	47	G	54	T
45	E	2D	-	4F	O	41	A
40	@	49	I	4C	L	44	D
54	T	4E	N	53	S	54	T



Schlüsselextension

54	T	48	H	47	G	54	T
45	E	2D	-	4F	O	41	A
40	@	49	I	4C	L	44	D
54	T	4E	N	53	S	54	T



Schlüsselexpansion

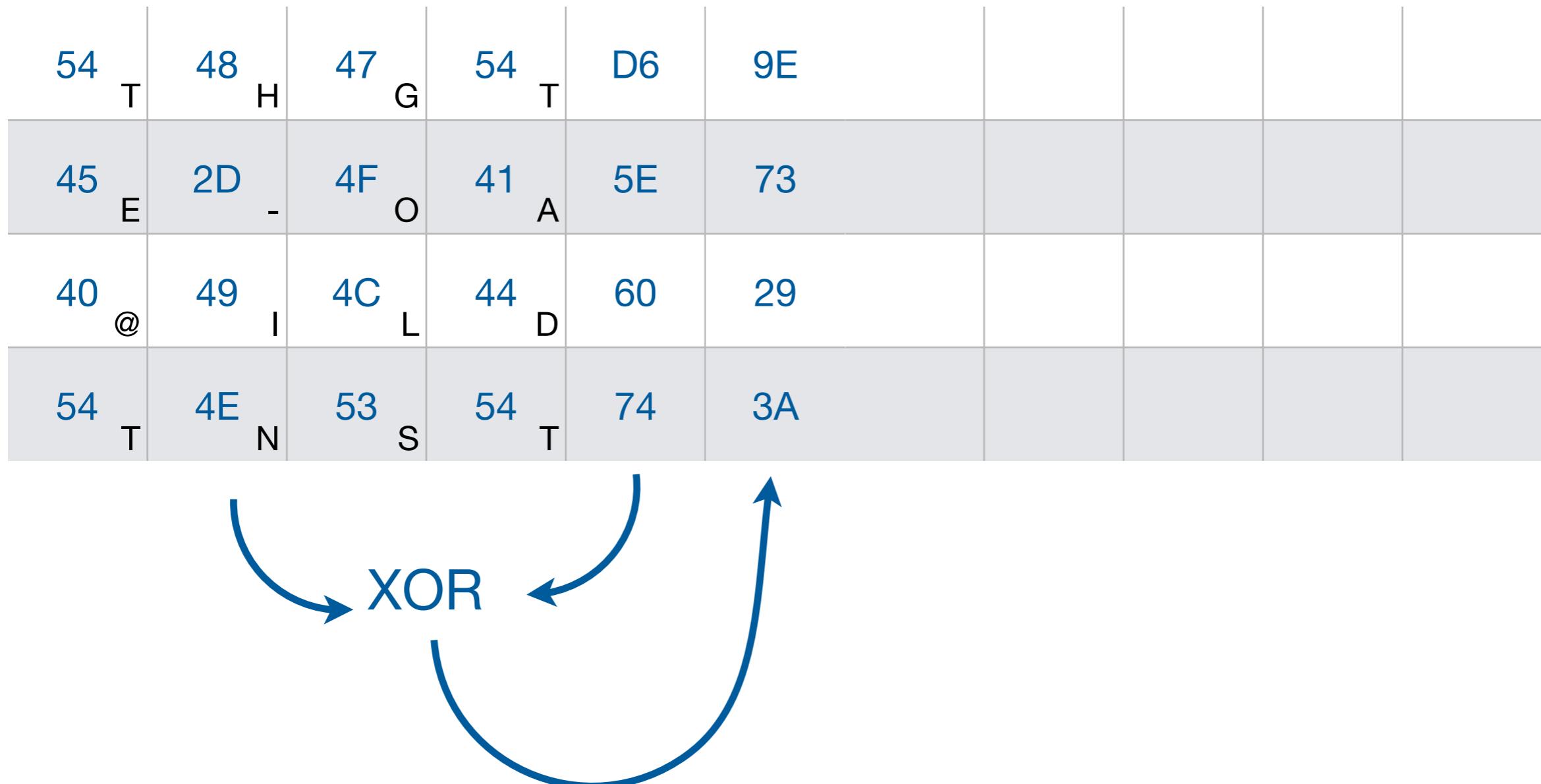
54	T	48	H	47	G	54	T	D6
45	E	2D	-	4F	O	41	A	5E
40	@	49	I	4C	L	44	D	60
54	T	4E	N	53	S	54	T	74



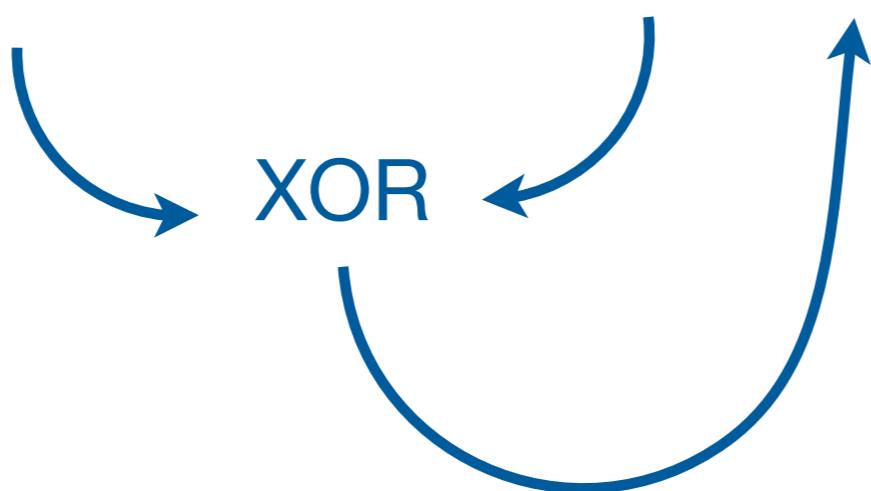
Schlüsselexpansion

54	T	48	H	47	G	54	T	D6
45	E	2D	-	4F	O	41	A	5E
40	@	49	I	4C	L	44	D	60
54	T	4E	N	53	S	54	T	74

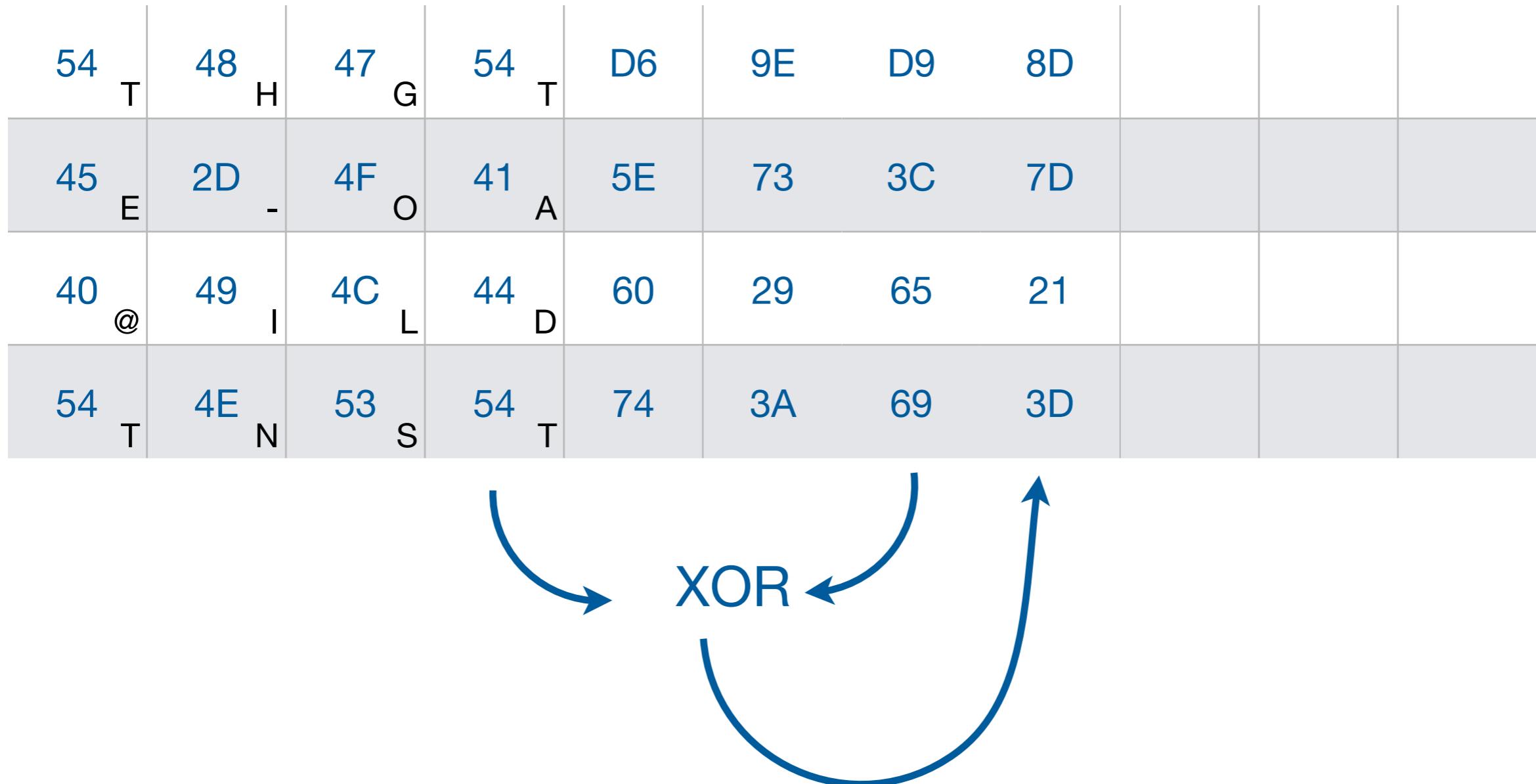
Schlüsselexpansion



Schlüsselexpansion



Schlüsselexpansion



Schlüsselexpansion

54	T	48	H	47	G	54	T	D6	9E	D9	8D	2B	
45	E	2D	-	4F	O	41	A	5E	73	3C	7D	A3	
40	@	49	I	4C	L	44	D	60	29	65	21	47	
54	T	4E	N	53	S	54	T	74	3A	69	3D	29	

↑

Wieder:

- RotWord
- Substitution
- XOR

Schlüsselexpansion

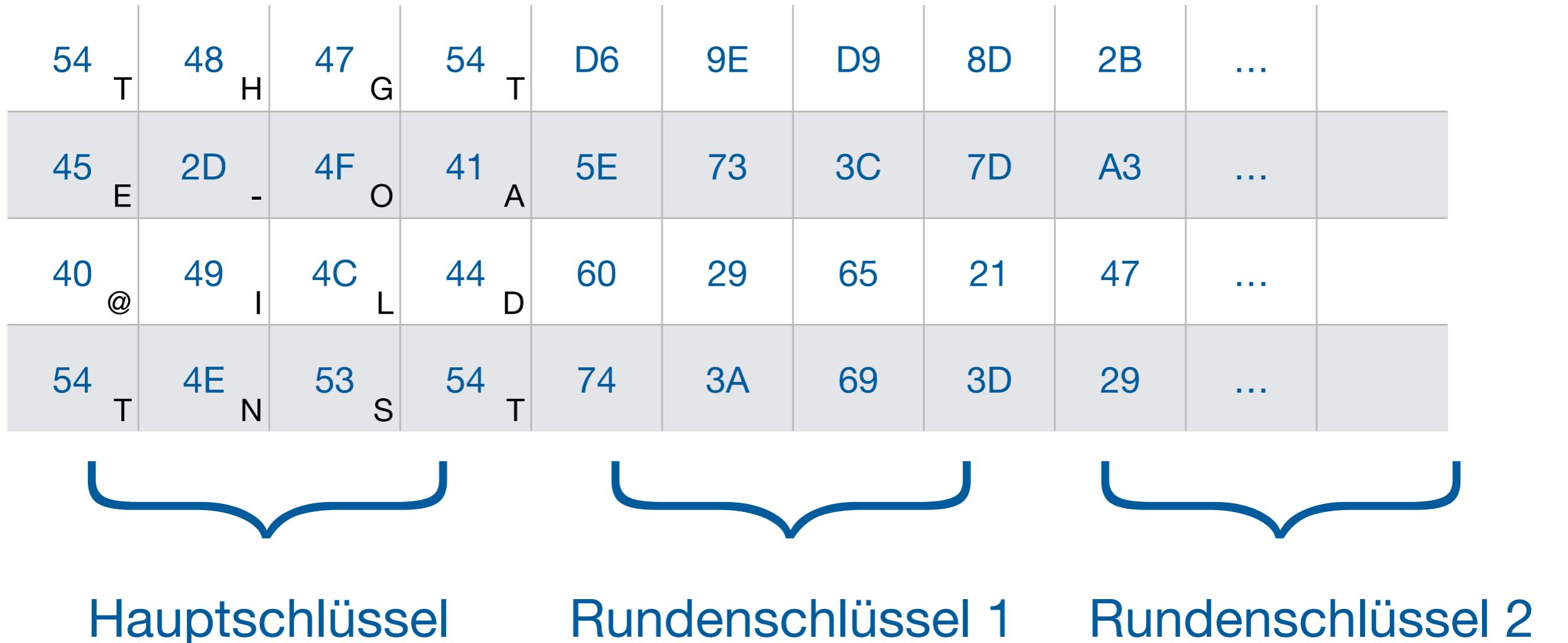
54	T	48	H	47	G	54	T	D6	9E	D9	8D	2B	
45	E	2D	-	4F	O	41	A	5E	73	3C	7D	A3	Wieder
40	@	49	I	4C	L	44	D	60	29	65	21	47	dreimal
54	T	4E	N	53	S	54	T	74	3A	69	3D	29	XOR

↑

Wieder:

- RotWord
- Substitution
- XOR

Schlüsselextension



Further Reading zu AES

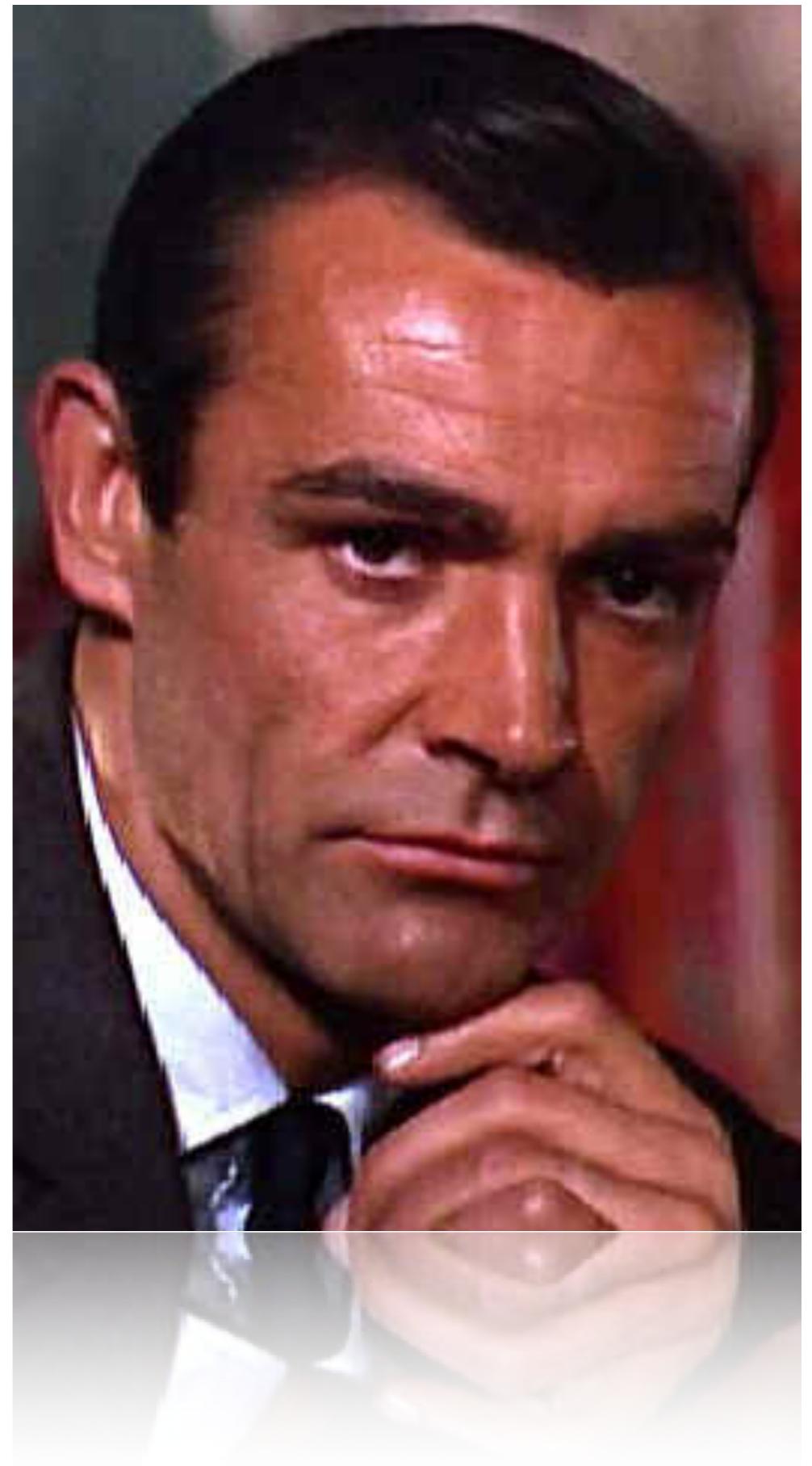
- <https://www.cryptool.org/de/cto/aes-animation>
- <https://www.cryptool.org/de/cto/aes-step-by-step>

Vorteile symmetrischer Verfahren

- Schnelle Verfahren
 - Hardware-Unterstützung möglich
- Moderne Verfahren sind sehr sicher

Nachteile

- Schlüsselübertragung



Lösungsidee

Schlüsselübertragung

- Diffie-Hellmann
- oder Verzicht auf Übertragung:
→ asymmetrische Kryptographie

Sicherer Schlüsseltausch: Diffie Hellmann

Diffie-Hellmann

- Client und Server wählen
 - Primzahl p
 - Primitivwurzel g modulo p
 $1 < g < p - 1$

Formale Definition Modulo

Definitionen - Grundlagen

- Eine Menge M besteht aus 0 bis n Elementen.
 $M = \{m_1, \dots, m_n\}$
- \mathbb{N} ist die Menge der natürlichen Zahlen inkl. 0
- a teilt m für $a, b \in \mathbb{N}$, wenn $\exists b \in \mathbb{N}$ mit $a^*b=m$
 a ist Divisor von m , m Vielfaches von a

Modulo-Arithmetik

- $a, b \in \mathbb{N}$, dann $\exists q, r \in \mathbb{N}$ mit $a = q * b + r$
- $r = a - b * q$ heißt Rest
 $r = a \bmod b$
- $c, d \in \mathbb{N}$ heißen kongruent modulo m , wenn
 $c \bmod m = r = d \bmod m$

Diskrete Exponentialfunktion

- auch: Modulare Exponentiation, Modulares Potenzieren
- $a^x \bmod n$
- Umkehrfunktion: Diskreter Logarithmus
nicht effizient berechenbar

Binäre Exponentiation

- $y = x^k$
- Idee:
 - $x^9 = x \cdot (x^8) = x \cdot x^2 \cdot x^2 \cdot x^2 = x \cdot (x^2)^3$
 - Exponentiation also durch mehrere Multiplikationen und Potenzen darstellbar
- Umwandlung von k in binär
 - 1001
 - Aus 1 mache: Quadrieren und Multiplizieren
 - Aus 0 mache: Quadrieren

Binäre Exponentiation

- Die Binärdarstellung beginnt immer mit 1, als mit Quadriere und Multipliziere, also $1^2 * x = x$
- Daher streichen des ersten „Quadriere und Multipliziere“ und ersetzen durch x
- Beispiel: 7^{23}
- $23_{\text{dez}} = 10111_{\text{bin}}$
- Also: Q&M, Q, Q&M, Q&M, Q&M
Streichen des ersten: x, Q, Q&M, Q&M, Q&M
Ergo:

$$x \xrightarrow{Q} x^2 \xrightarrow{Q} x^4 \xrightarrow{M} x^5 \xrightarrow{Q} x^{10} \xrightarrow{M} x^{11} \xrightarrow{Q} x^{22} \xrightarrow{M} x^{23}$$

Mit Modulo

- Nach jedem Schritt Modulo
→ kleinere Zahlen
- Beispiel: $7^{18} \text{ mod } 256 = 177$
 $18_{\text{bin}} = 10010$
Also: x, Q, Q, Q&M, Q

Schritt		mod 256
x		7
Q		49
Q	2401	97
Q	9409	193
M	1351	71
Q	5041	177

Definition: Primitivwurzel

- Primzahl innerhalb einer Modulo-Gruppe, aus der alle Zahlen der Gruppe als Potenz dargestellt werden können.
- Beispiel:
 - Primzahl 3
 - $G=\{0, 1, 2, 3, 4, 5, 6\}$
ergo: Modulo 7

$3^1 = 3$	$3^1 \bmod 7 = 3$
$3^2 = 9$	$3^2 \bmod 7 = 2$
$3^3 = 27$	$3^3 \bmod 7 = 6$
$3^4 = 81$	$3^4 \bmod 7 = 4$
$3^5 = 243$	$3^5 \bmod 7 = 5$
$3^6 = 729$	$3^6 \bmod 7 = 1$

Diffie-Hellmann (II)

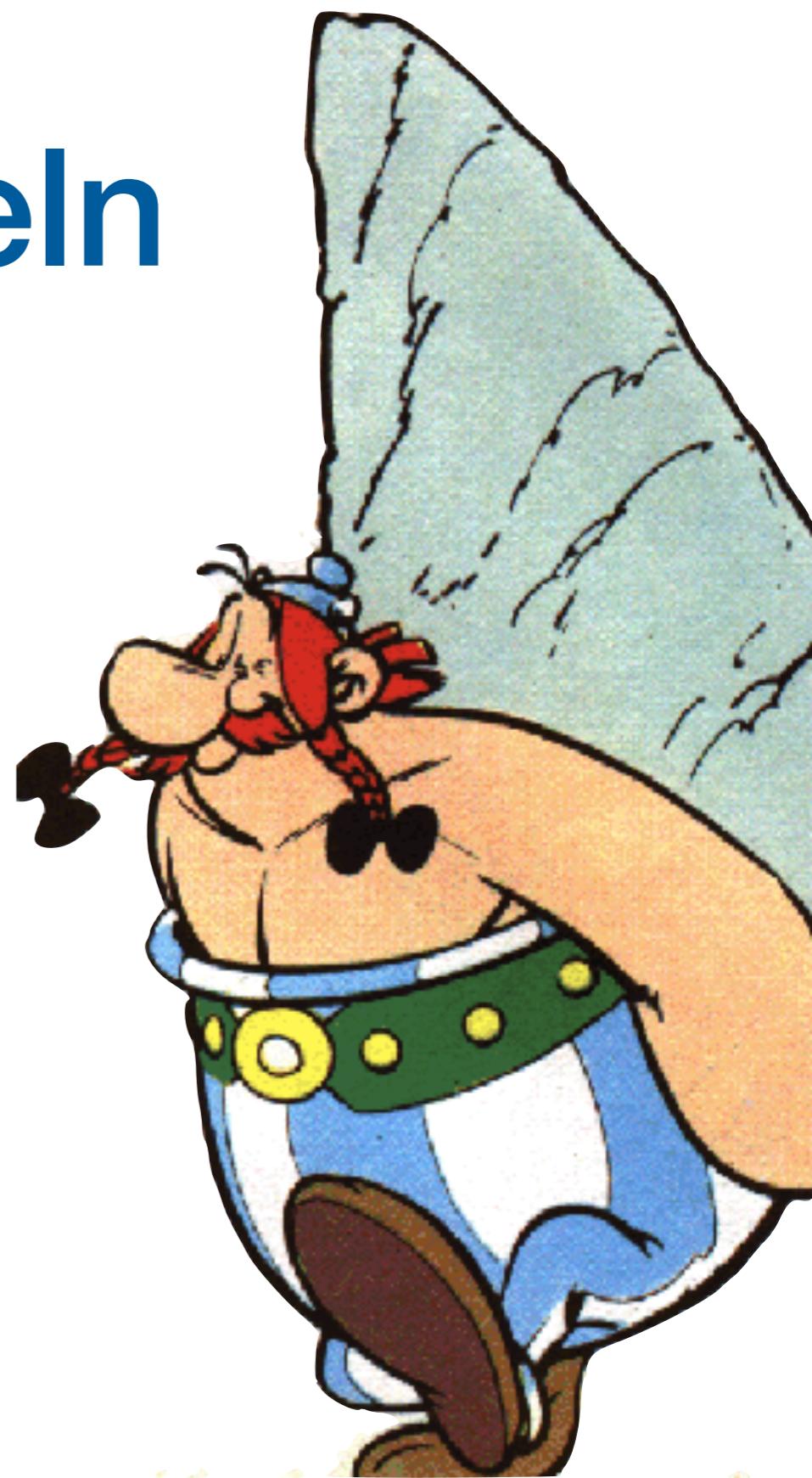
- Geheime Zufallszahlen a, b
- Client wählt Zufallszahl $a, 1 \leq a < p-1$
und berechnet: $A = g^a \text{ mod } p$
- Server wählt Zufallszahl $b, 1 \leq b < p-1$
und berechnet: $B = g^b \text{ mod } p$
- Gegenseitiges Zusenden von A und B

Diffie-Hellmann (III)

- Client berechnet $K = B^a \text{ mod } p$
- Server berechnet $K = A^b \text{ mod } p$
- Beide K gleich, weil:
 $B^a \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = g^{ba} \text{ mod } p$
 $A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p$
- K ist Schlüssel

Asymmetrische Kryptographie

Verschlüsseln



Verschlüsseln



Verschlüsseln



Public Key



Verschlüsseln



Public Key



Private Key

Verschlüsseln

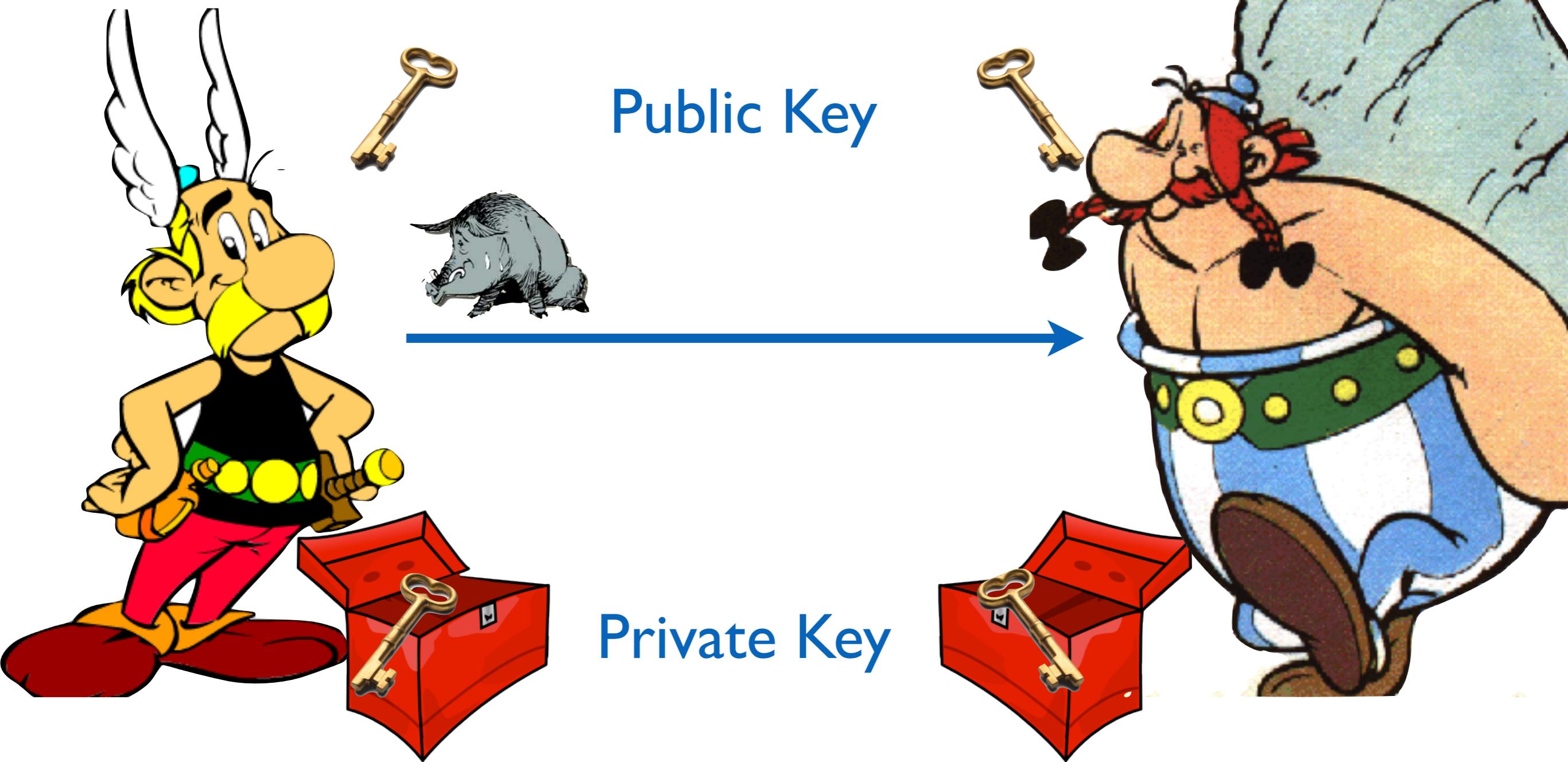


Public Key

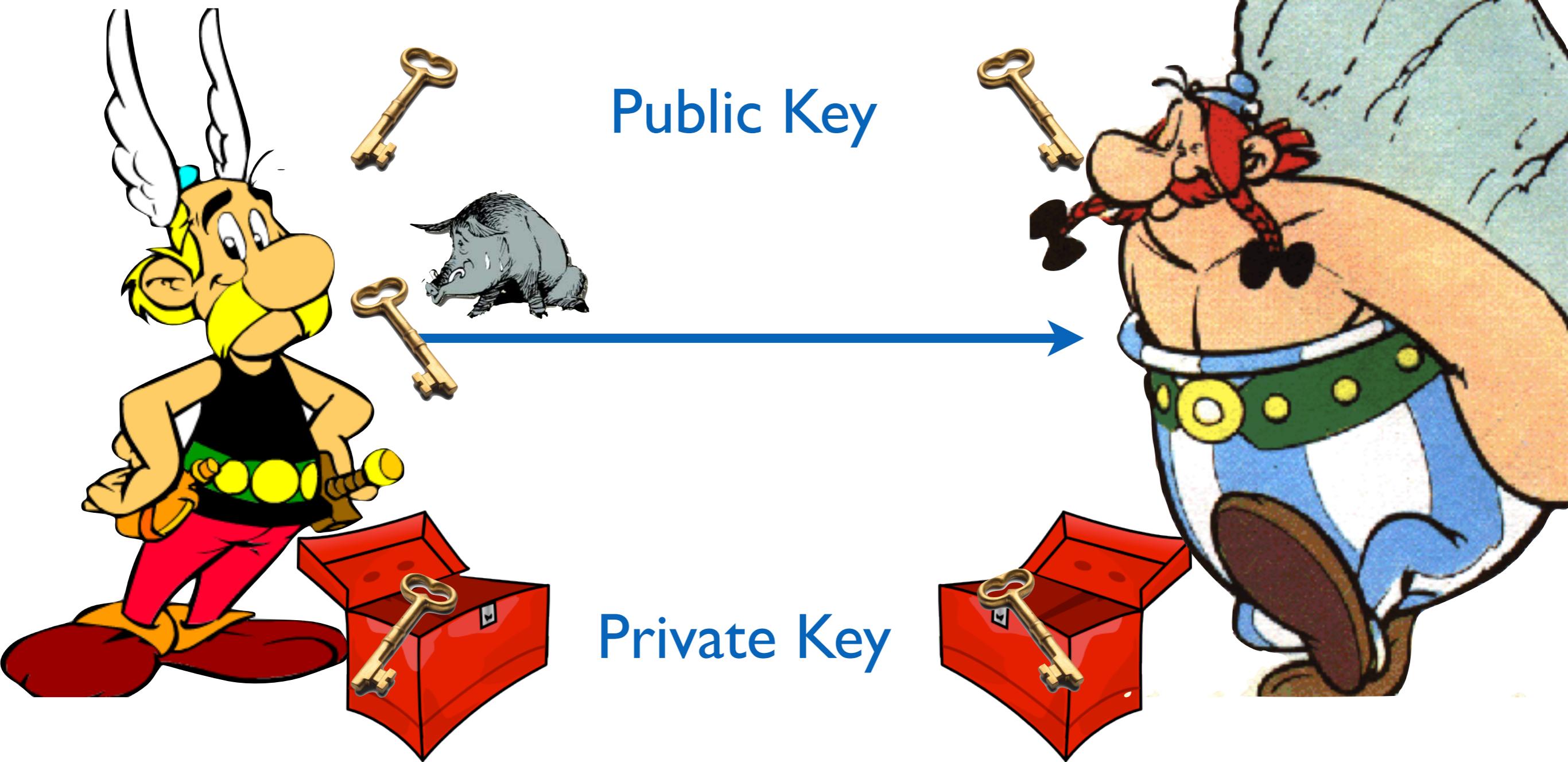
Private Key



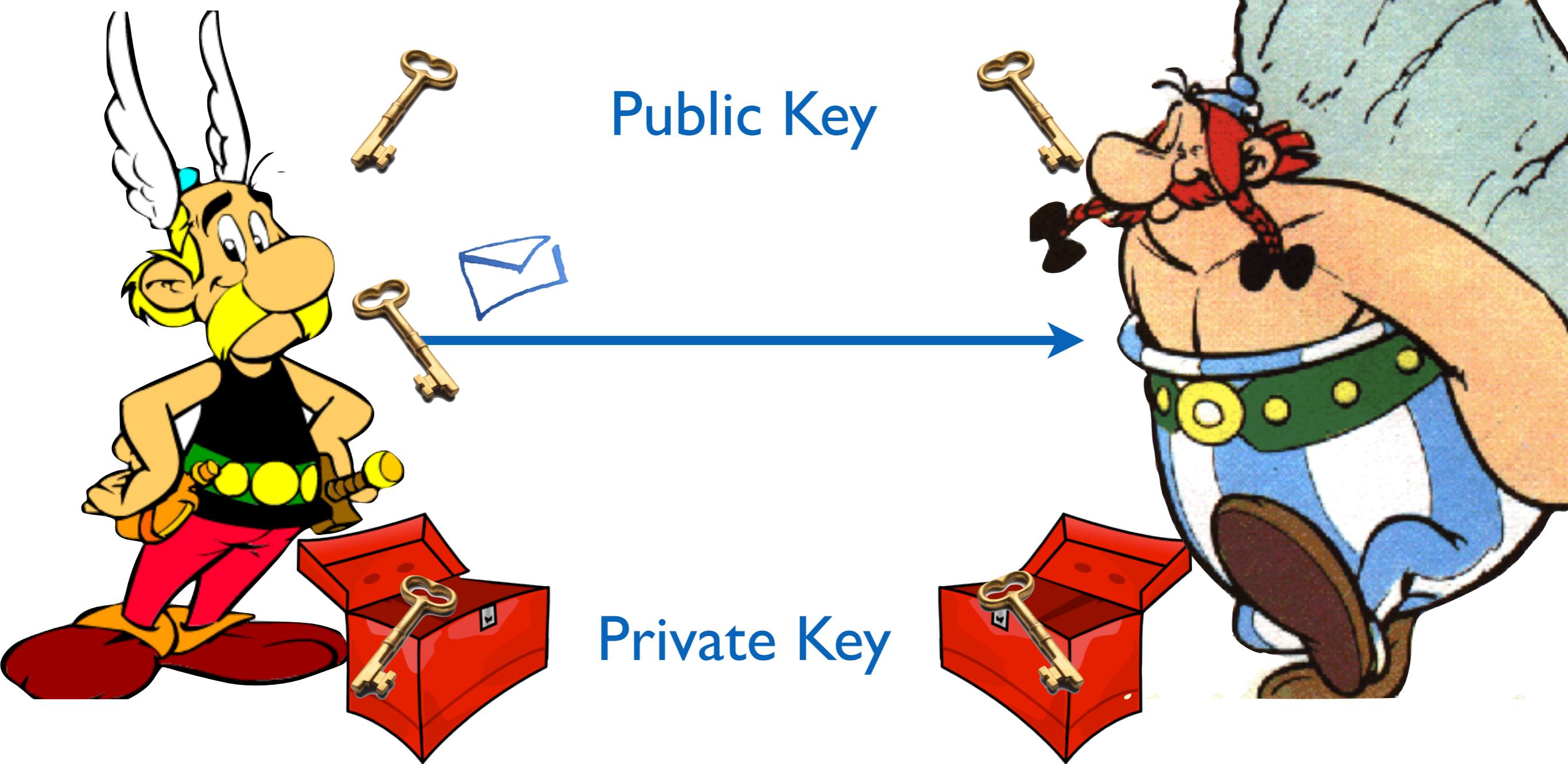
Verschlüsseln



Verschlüsseln



Verschlüsseln

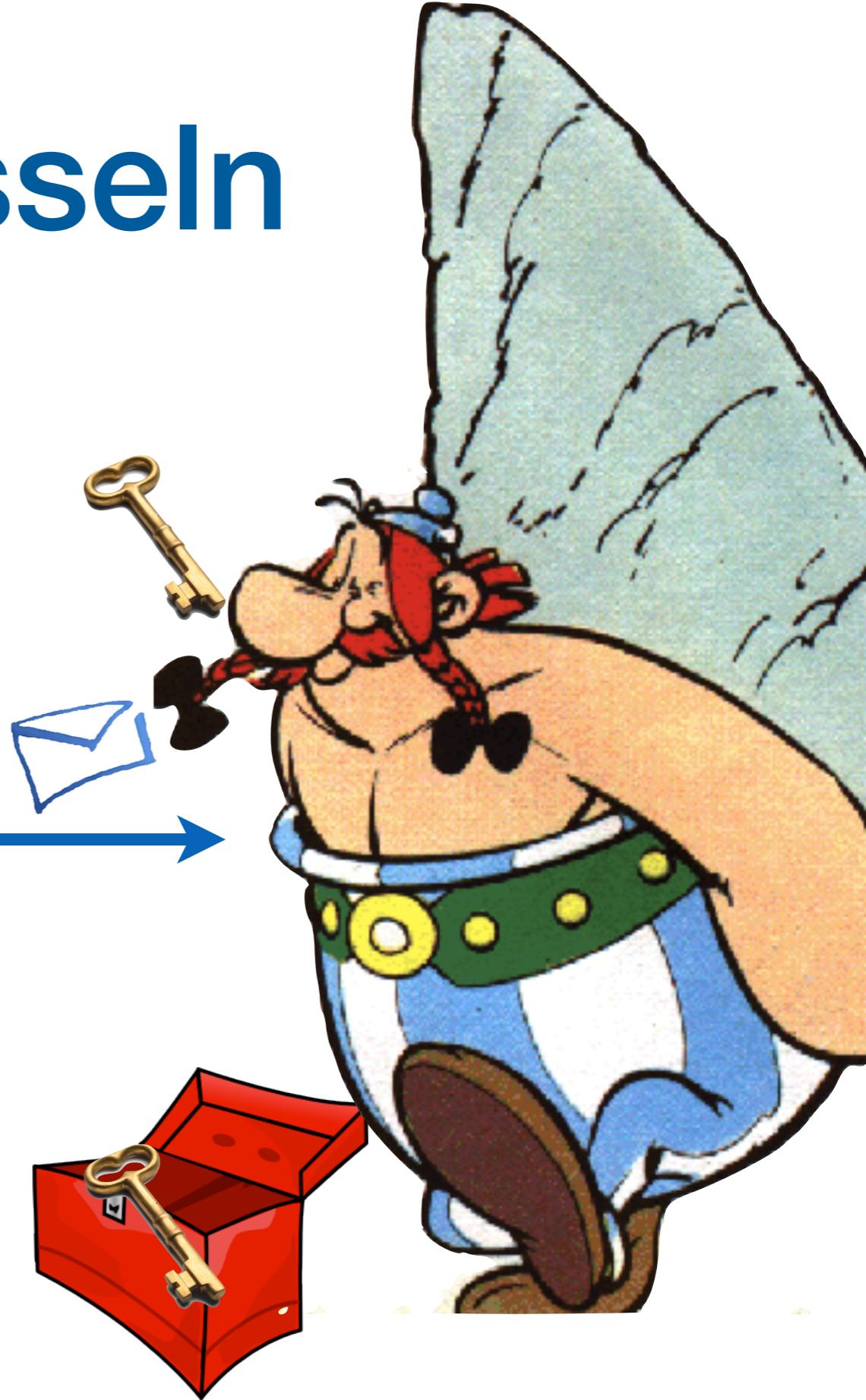


Verschlüsseln



Public Key

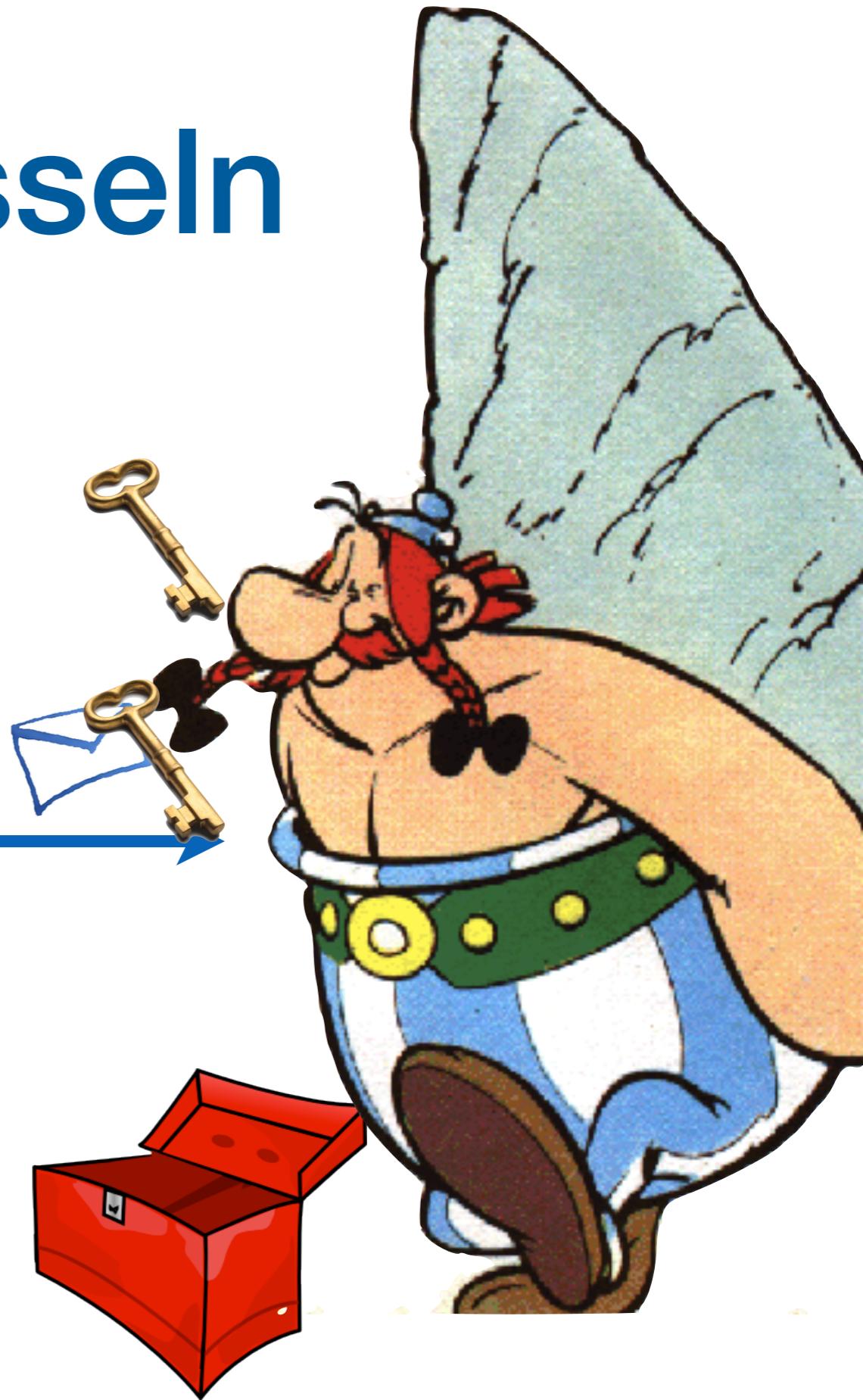
Private Key



Verschlüsseln

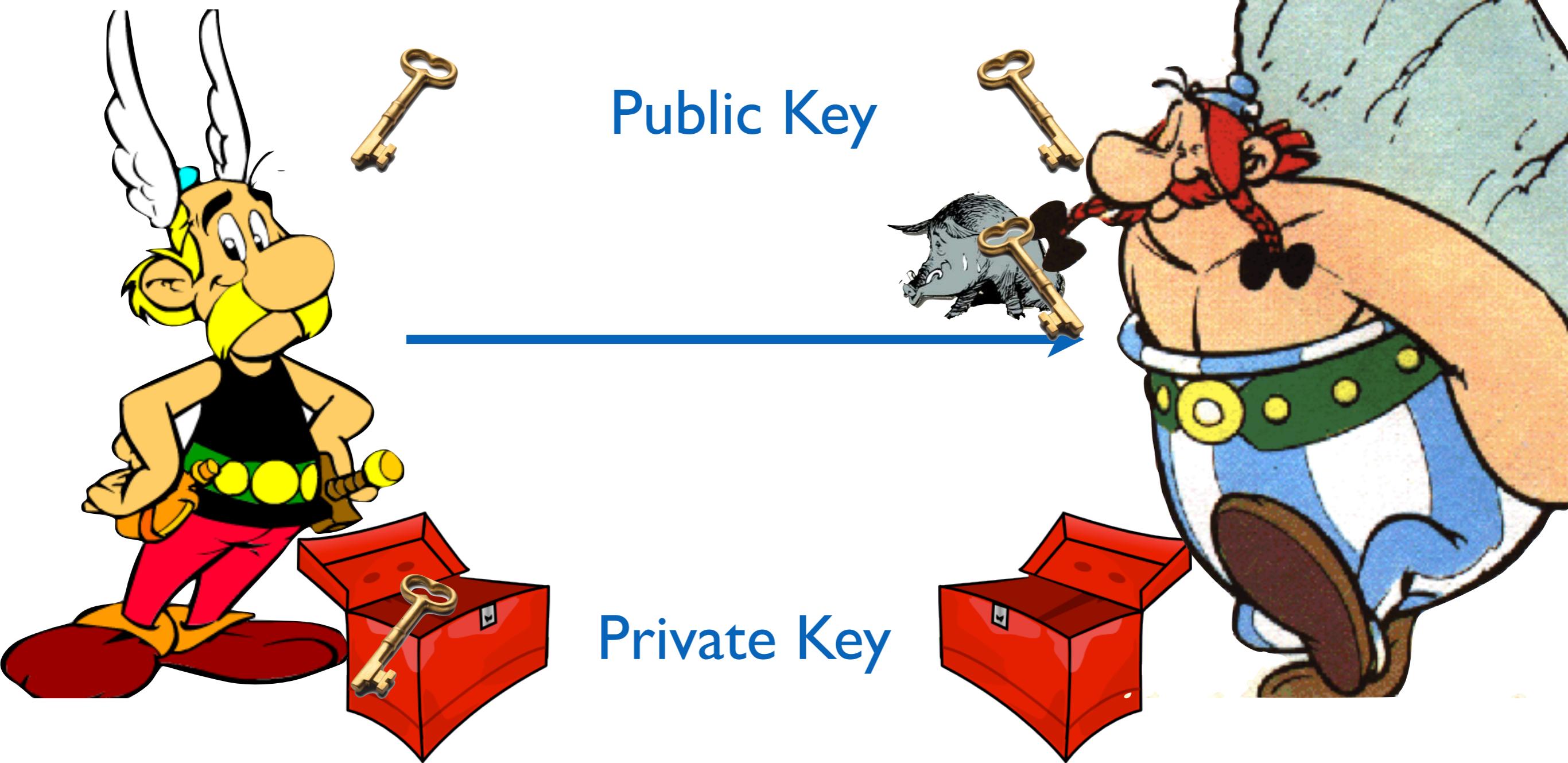


Public Key

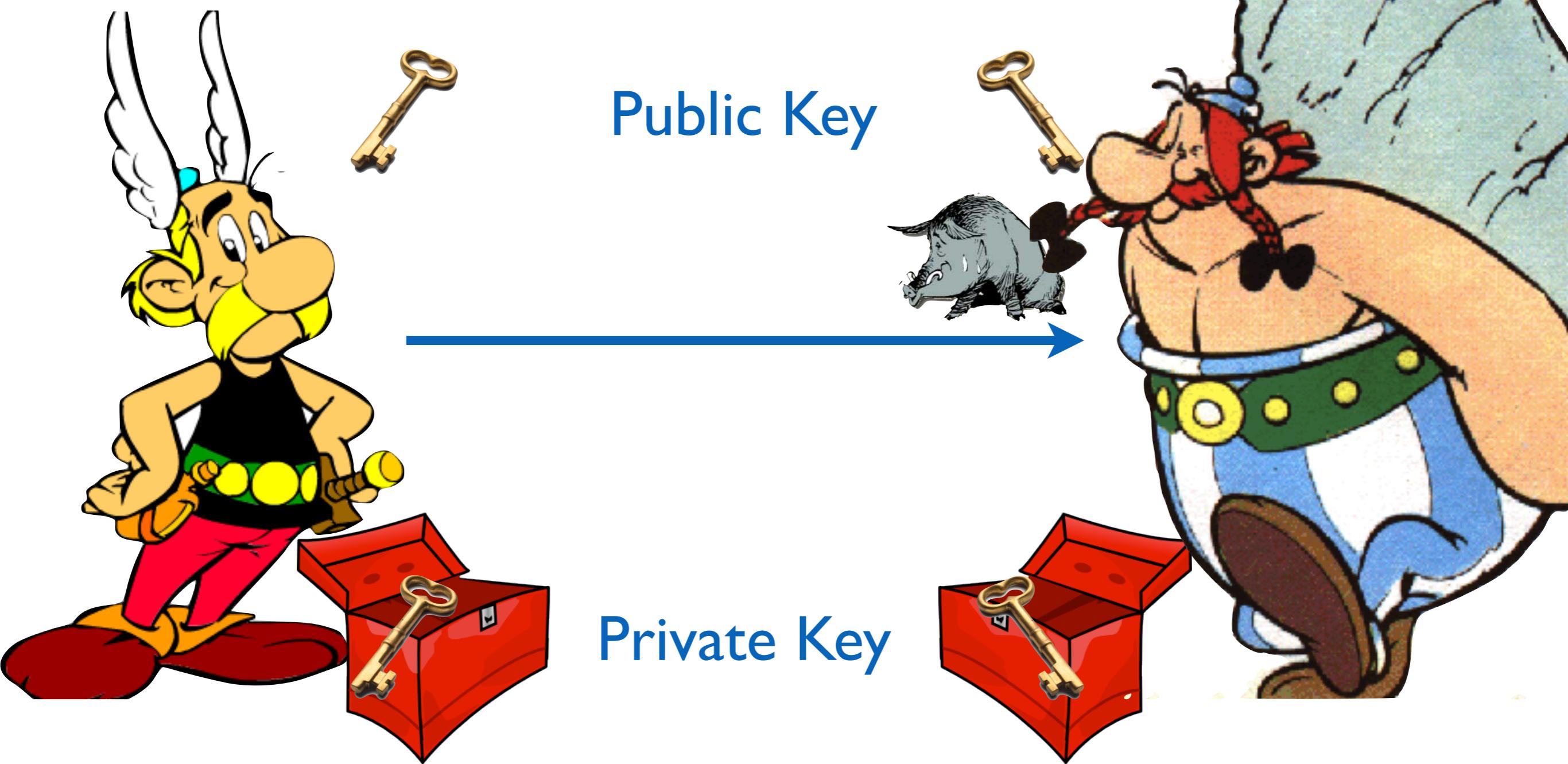


Private Key

Verschlüsseln



Verschlüsseln



RSA

RSA Verfahren

RSA Verfahren

- Primzahlen p, q (zufällig)
- Public Key:
Zahlenpaar (e, N)
- Private Key:
Zahlenpaar (d, N)

Primfaktorzerlegung

$$350 = 2 \cdot 5 \cdot 5 \cdot 7$$

- Aufwendig bei großen Zahlen
- Große Primzahlen schwer zu finden

Weiter...

$$N = p * q$$

Sei: $\phi(N) = (p-1) * (q-1)$

Wähle: e

mit: $1 < e < \phi(N)$

sowie $\phi(N)$ und e sind teilerfremd

Berechne: d

(multiplikativ Inverses zu e bzgl. $\phi(N)$)

Beispiel für Public Key

$$p=11, q=13$$

$$N = p * q = 143$$

$$\phi(N) = (p-1) * (q-1) = 120$$

Wähle: $e = 23$

Public Key: $(23, 143)$

Beispiel für Private Key

$p=11, q=13, N=143, e=23$

Berechne d

$$e^*d + k^*\phi(N) = 1$$

$$23^*d + k^*120 = 1$$

$$23^*47 + (-9)^*120 = 1$$

$$d = 47$$

Private Key: (47, 143)

Verschlüsseln

$$C = K^e \bmod N$$

C: Chiffrat

K: Klartext

Beispiel

K=7

e=23, N=143

$$C = 7^{23} \bmod 143 = 2$$

Entschlüsseln

$$K = C^d \bmod N$$

Beispiel

C=2

d=47, N=143

$$K = 2^{47} \bmod 143 = 7$$

Geekstuff

<http://www.cypherspace.org/rsa/story2.html>



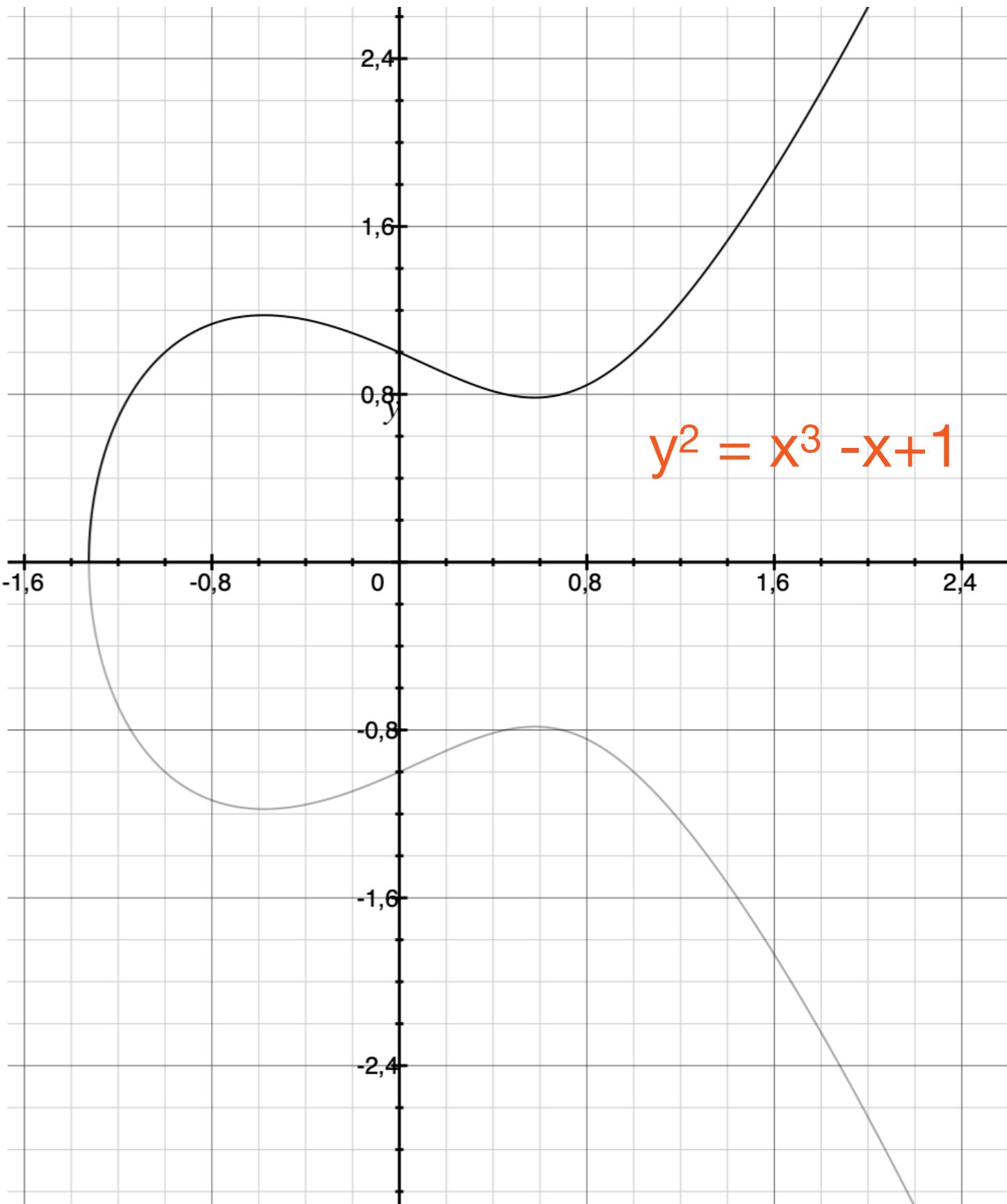
Technische Hochschule
Ingolstadt

Elliptic Curve

Elliptische Kurve

$$y^2 = x^3 + ax + b$$
$$y = \pm \sqrt{x^3 + ax + b}$$

Bildet Abelsche Gruppe



Gruppe (I)

- Eine Gruppe G ist eine Menge mit einer Verknüpfung \circ , für die gilt
 - $\forall a,b,c \in G: a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziativ)
 - $\forall a \in G, \exists b \in G: a \circ e = e \circ a = a$ (Neutrales Element)
 - $\forall a \in G, \exists a^{-1} \in G: a \circ a^{-1} = a$ (Inverses Element)

Gruppe (II)

- Wenn
 - ○ für + steht, ist es eine additive Gruppe
 - ○ für * steht, eine multiplikative Gruppe
- Eine endliche Gruppe G hat endlich viele Elemente.

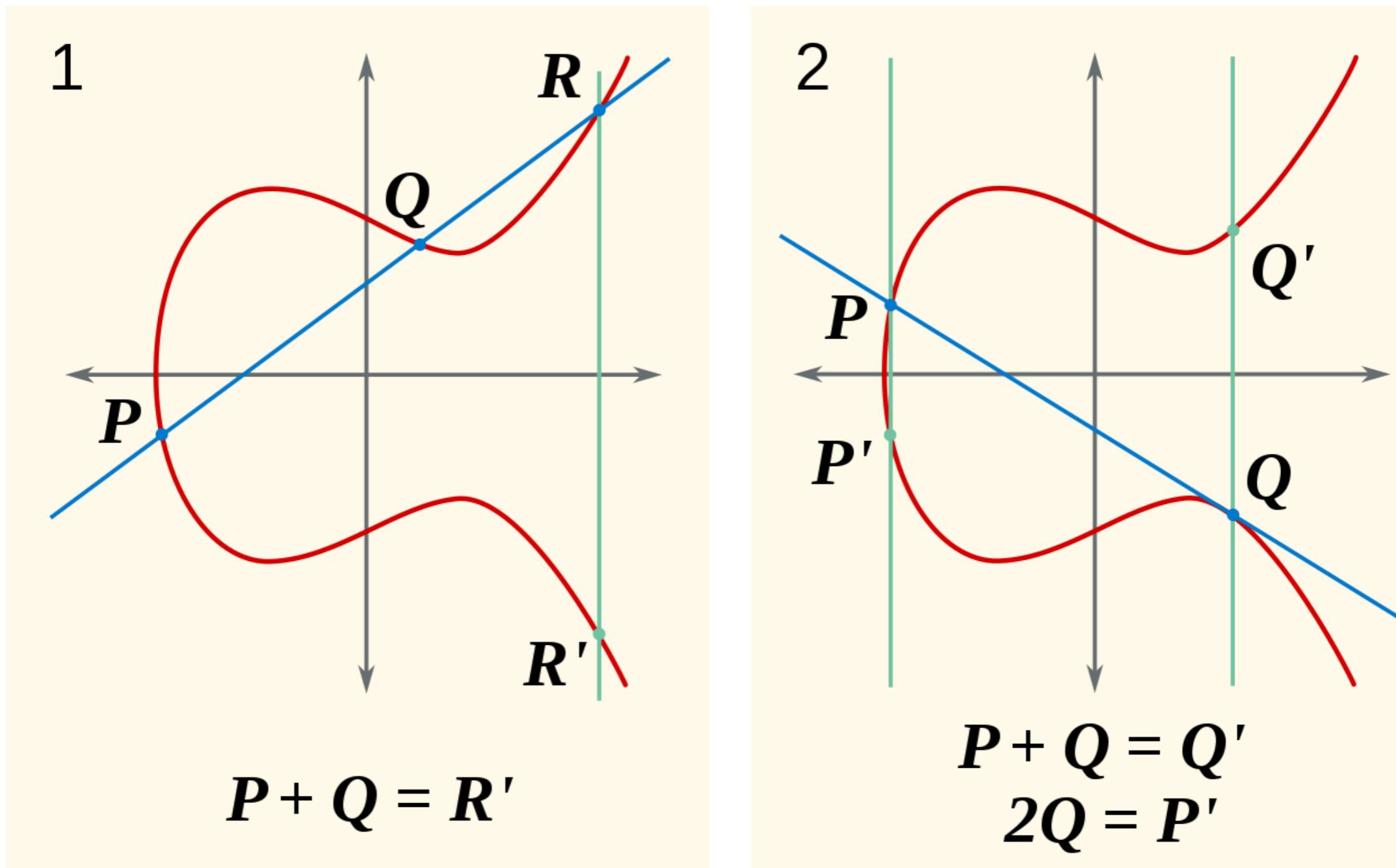
Abelsche Gruppe

Gruppe \mathbb{A} mit einer Operation \circ , für die zusätzlich gilt:

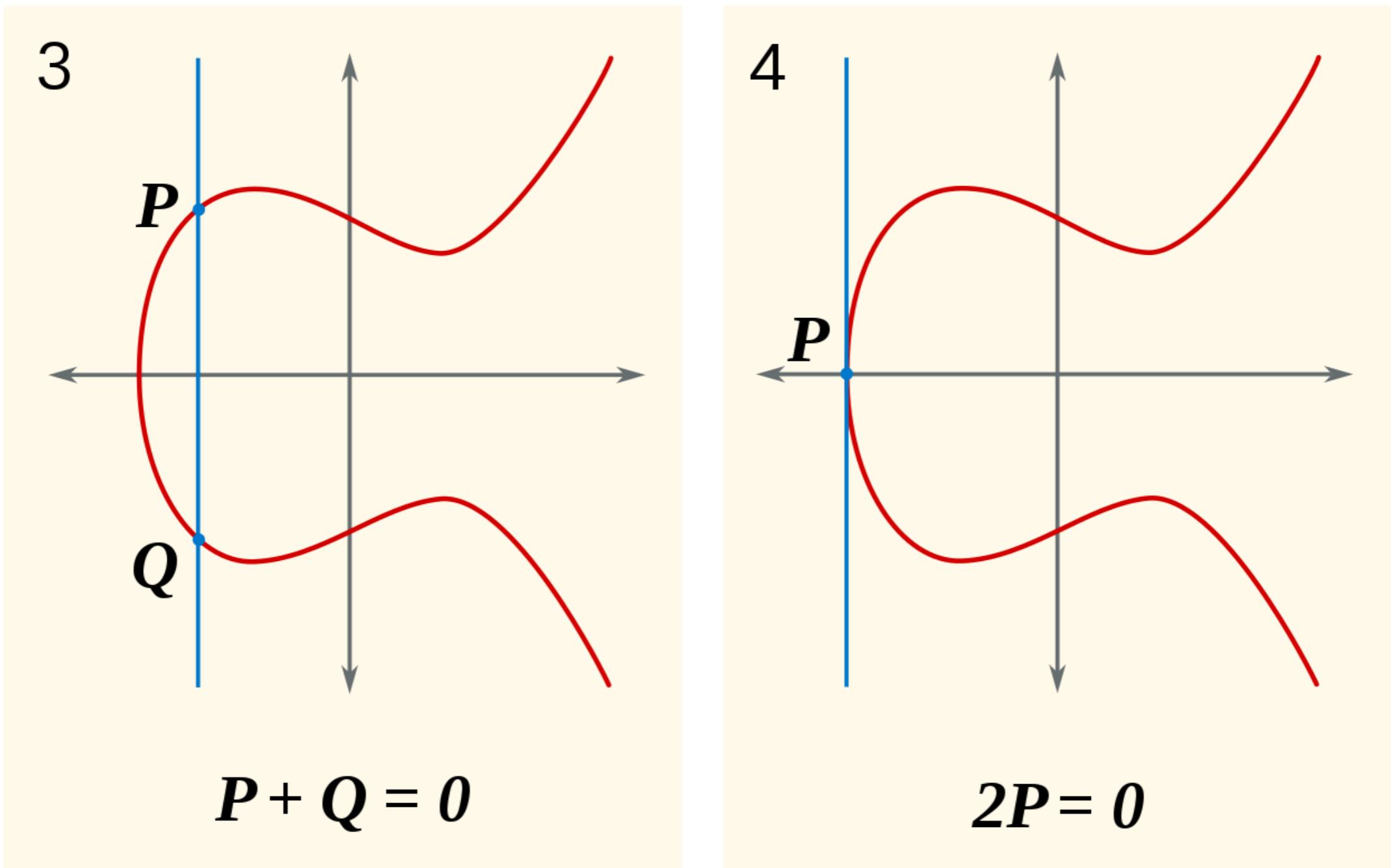
$\forall a, b \in \mathbb{A}: a \circ b = b \circ a$ (kommutativ)

heißt Abelsche oder kommutative Gruppe

Addition (I)



Addition (II)



Idee:

- Addition und Multiplikation ersetzen
Multiplikation und Exponentiation in RSA, Diffie-Hellmann usw.
- Addition / Multiplikation deutlich schwerer umkehrbar als Faktorisierung, daher
 - kürzere Schlüssel
 - effizienter zum Ver- und Entschlüsseln
- Nebeneffekt:
 - Post-Quantum sicher

Vorteil asymmetrischer Verfahren

- einfacher Schlüsseltausch

Nachteil

- Berechnung aufwendiger als symmetrische
- Längere Schlüssel nötig als symmetrische
(bei gleicher Sicherheit)

Hybride Verschlüsselung

Problem

- Schlüsseltausch symmetrisch ist organisatorisch aufwendig
- Verschlüsselung asymmetrisch ist rechen aufwendig

Lösungsidee

- Erzeuge zufälligen, symmetrischen Sitzungsschlüssel S
- Verschlüssele Nachricht M mit S symmetrisch
 $C_M = \text{enc}_{\text{sym}}(M, S)$
- Verschlüssele S asymmetrisch an Public Key K_{pub}
Empfänger
 $C_S = \text{enc}_{\text{asym}}(S, K_{\text{pub}})$
- Sende (C_M, C_S) an den Empfänger, der dann:
 - $S = \text{dec}_{\text{asym}}(C_S, K_{\text{priv}})$
 - $M = \text{dec}_{\text{sym}}(C_M, S)$

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

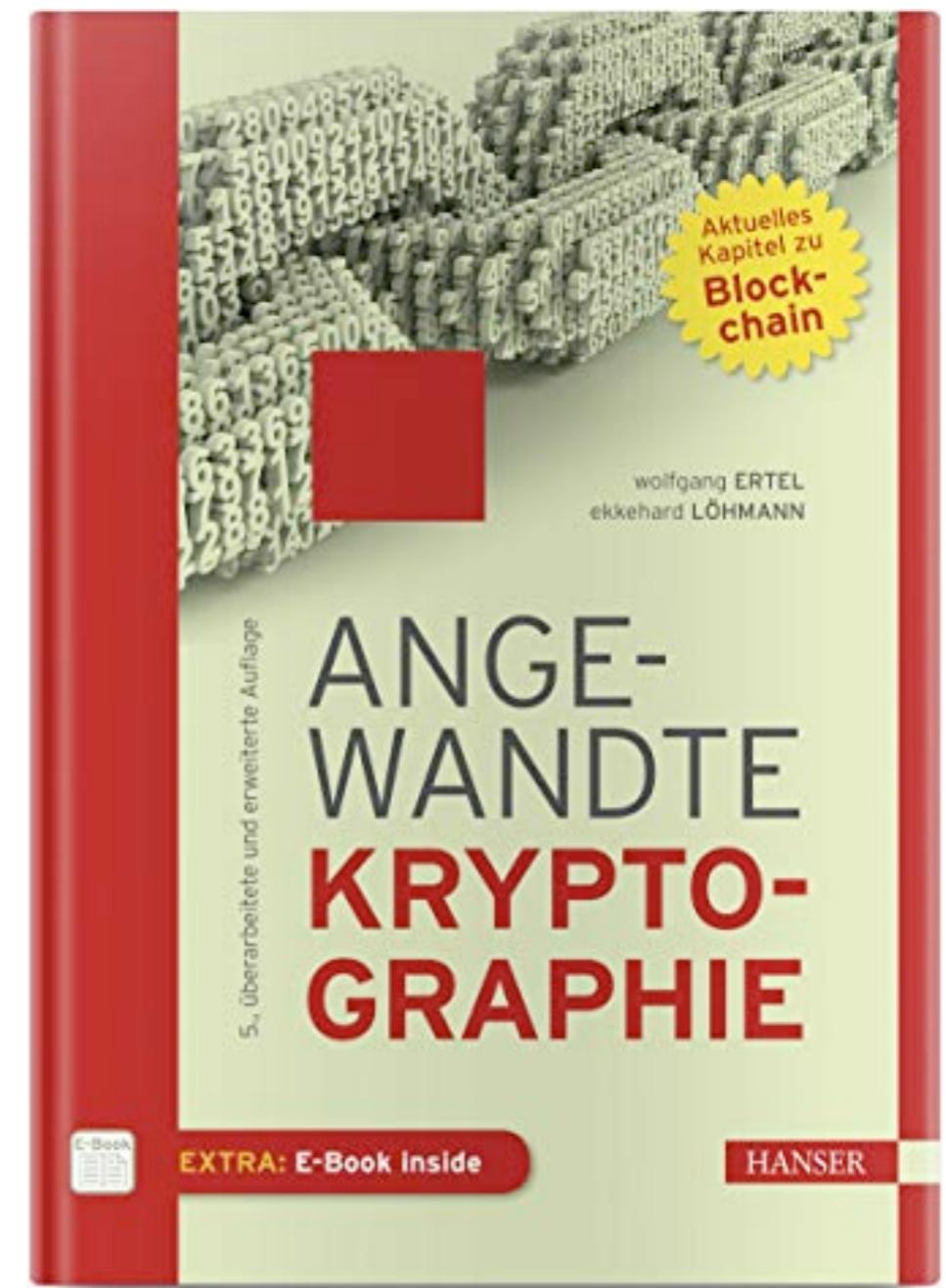
HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



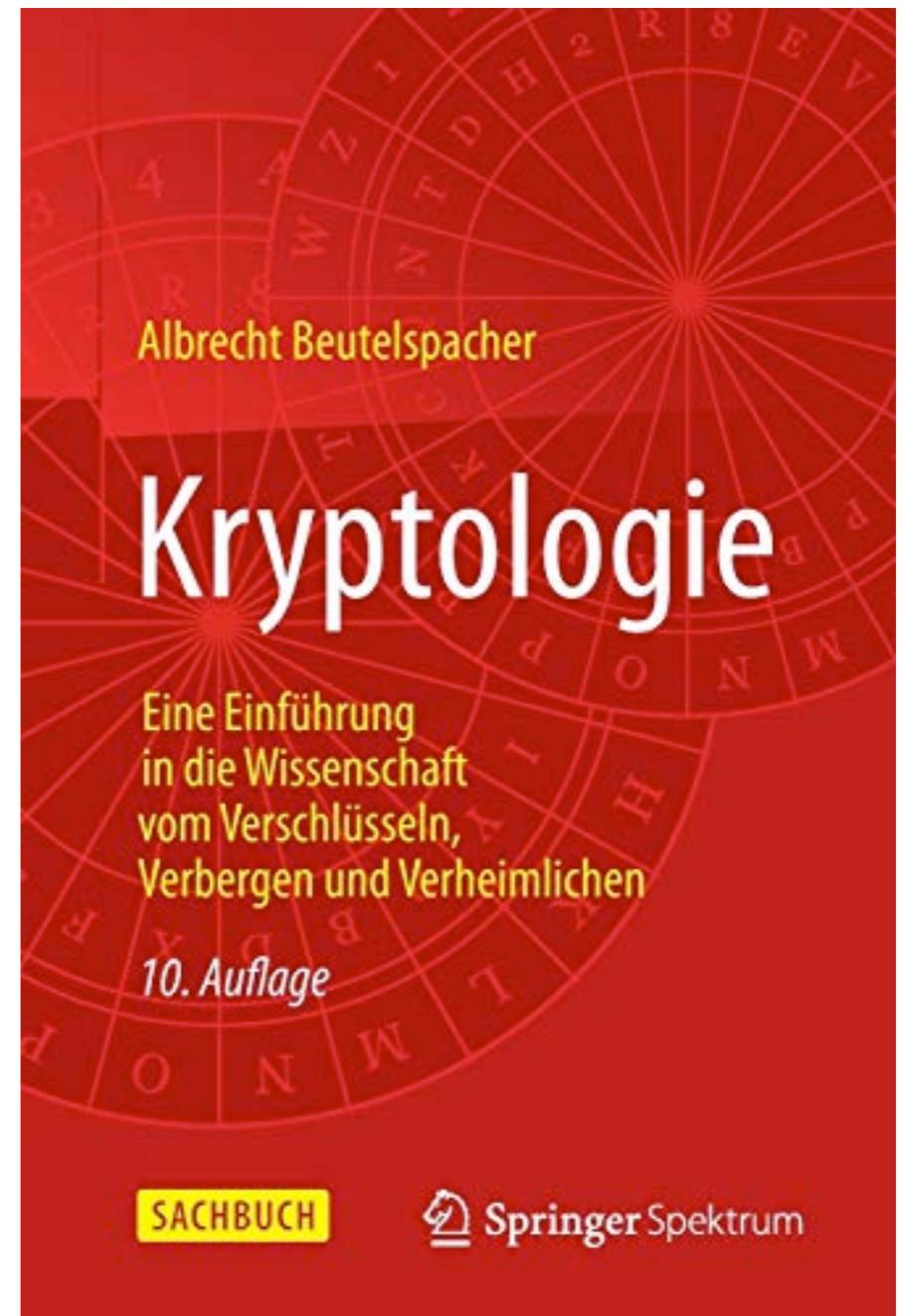
Literaturhinweise

- Wolfgang Ertel
Ekkehard Löhmann
Angewandte Kryptographie



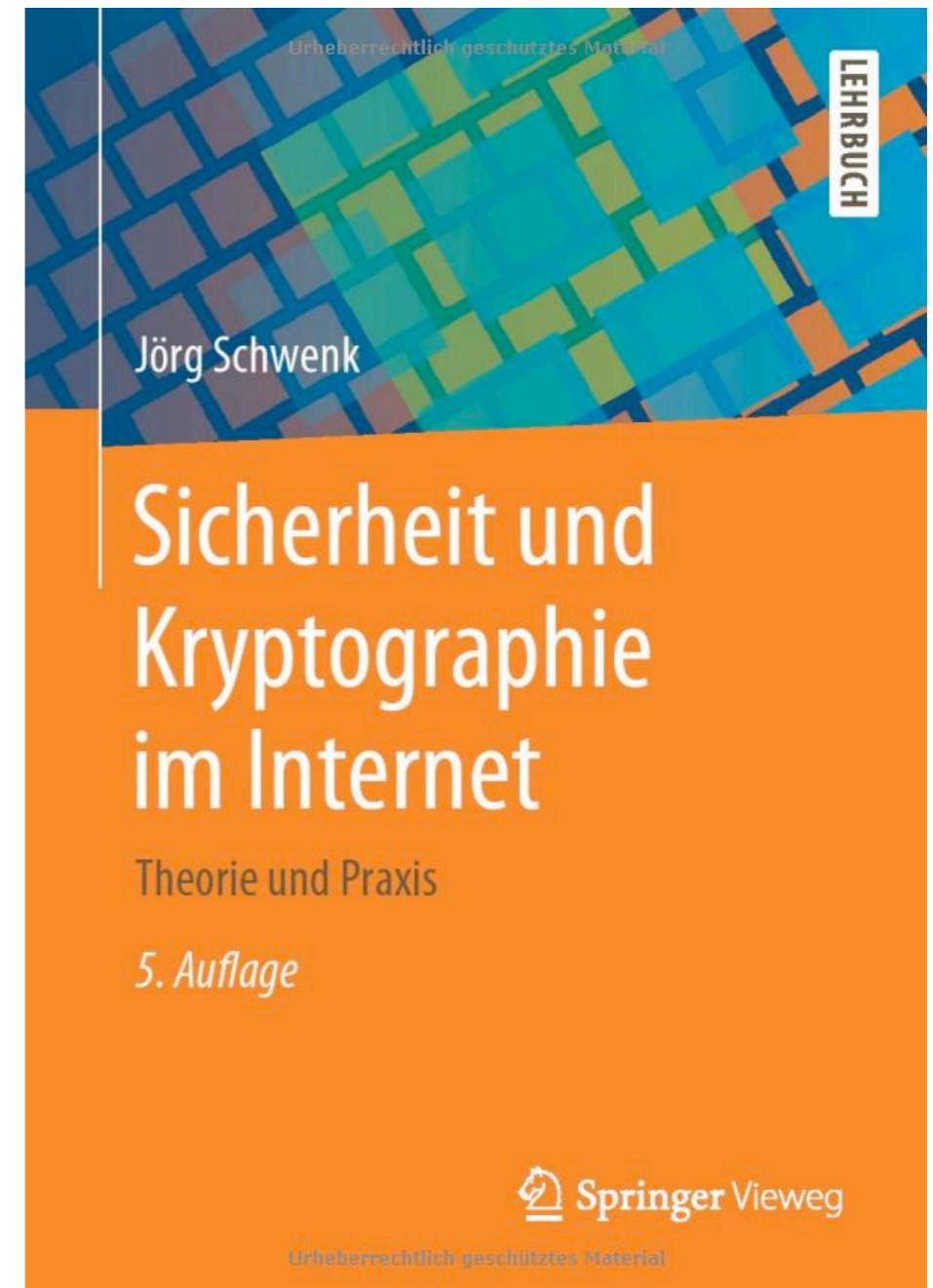
Literaturhinweise

- Albrecht Beutelspacher
Kryptologie
(neben zahlreichen Werken von
Beutelspacher)



Literaturhinweise

- Jörg Schwenk
Sicherheit und Kryptographie
im Internet



Link-Hinweise

- <https://www.heise.de/blog/Was-man-ueber-Kryptografie-wissen-sollte-5001908.html>
- <https://kryptografie.de/kryptografie/index.htm>
- <https://cryptool.org>

Integrität

Ziel

- Nachweis, das Nachricht unverändert
- Hinweis: Verschlüsseln verhindert Veränderung nicht!
- Beispiel
 - ROT13(Hello World) = UryyB jBEyq!
 - Angreifer manipuliert: UnyyB OnLrE!
 - ROT13(UnyyB OnLrE!) = Hallo Bayer!

Idee Hash-Funktion:

- Hash-Funktion
- Hash-Funktion bildet eine Menge M auf M' ab,
i.d.R. mit $|M| > |M'|$
- Also: Kollisionsgefahr

Kollisionsgefahr

- „Geburtstagsparadoxon“
- Wie hoch ist die Wahrscheinlichkeit für zwei beliebige $a, b \in M$, das $\text{hash}(a) = \text{hash}(b)$?
- Unterschied zur Wahrscheinlichkeit für ein festes $a \in M$, daß es ein $b \in M$ gibt, mit $\text{hash}(a) = \text{hash}(b)$
- Wie aufwendig ist $\text{hash}^{-1}(a) = a$?

Relevante Hash-Funktionen

- SHA, SHA256, SHA512
- MD5 (immer noch)

SHA256 - Ausprobieren

- Ausführlich erklärt am selbstgewählten Beispiel:
<https://www.cryptool.org/de/cto/sha2>

Aber:

- Nachricht N=„Hello World“
- $H = \text{MD5}(N) = b10a8db164e0754105b7a99be72e3fe5$
- Sende N, H
- Angreifer manipuliert: N'=„Hallo Welt“
Berechnet neuen Hash
 $H' = \text{md5}(N') = 5c372a32c9ae748a4c040ebadc51a829$
- Leitet weiter N', H'
- Wie erkennt das der Empfänger?

Lösung: Signatur

- Sender:
 - Nachricht N , Hash $H = \text{hash}(N)$
 - Signatur $S = \text{enc}(H, K_{\text{priv}})$
- Sendet N, S
- Empfänger:
 - $\text{hash}(N)$
 - $\text{dec}(H, K_{\text{pub}})$
 - Nachricht unverändert, wenn $\text{hash}(N) = \text{dec}(H, K_{\text{pub}})$

Lösung: Signatur

- Sender:
 - Nachricht N , Hash $H = \text{hash}(N)$
 - Signatur $S = \text{enc}(H, K_{\text{priv}})$
- Sendet N, S
- Empfänger:
 - $\text{hash}(N)$
 - $\text{dec}(H, K_{\text{pub}})$
 - Nachricht unverändert, wenn $\text{hash}(N) = \text{dec}(H, K_{\text{pub}})$

Denn K_{pub} muß zu
 K_{priv} passen, den nur der
Sender kennt

Lösung: Signatur

- Sender:
 - Nachricht N , Hash $H = \text{hash}(N)$
 - Signatur $S = \text{enc}(H, K_{\text{priv}})$
- Sendet N, S
- Empfänger:
 - $\text{hash}(N)$
 - $\text{dec}(H, K_{\text{pub}})$
 - Nachricht unverändert, wenn $\text{hash}(N) = \text{dec}(H, K_{\text{pub}})$

Randnotiz: Hash & Salt

- Passwörter häufig als Hash-Wert gespeichert
- Angriff-Idee mit viel RAM
 - Generiere zu jedem Passwort einen Hash
 - Suche nach Hash
 - Reverse das Passwort
- Optimierung: Rainbow-Table
- Gegenmaßnahme: Salt

Notiz

- Salt: Zusatzwert pro „Passwort“
- Pepper: Globaler Zusatzwert (also einheitlicher Salt)

Literatur Hashing

- [https://www.linux-magazin.de/ausgaben/2015/10/
hashfunktionen/](https://www.linux-magazin.de/ausgaben/2015/10/hashfunktionen/)

Authentizität

Ziel

- Nachweis, daß der Sender wirklich der Sender ist

Im Alltag



Warum dem vertrauen?



- Vertrauen in Ausgabestelle
- Vertrauen in Echtheit des Dokumentes

Digitale Zertifikate

- Vertrauenswürde Herausgeber (Root-CA)
- Signieren Zertifikate oder Key (Echtheit)

Digitale Identitäten

- Sichere Identität: Nur durch berechtigten nutzbar
- Identitätsdiebstahl: Mißbrauch einer Identität

SSL / TLS

TLS 1.3

Anwendung von TLS

- HTTPS
- STARTTLS in SMTP
- IMAPS
- POP3S
- NTPS
- LDAPS
- ...S
- stunnel
- OpenVPN

Anwendung von TLS

- HTTPS
- STARTTLS in SMTP
- IMAPS
- POP3S
- NTPS
- LDAPS
- ...S
- stunnel
- OpenVPN



Was sind die Ziele?

Ziele von TLS

- Authentifikation des Servers und ggf. Clients
- Integrität der Datenübertragung
- Vertrauliche Kommunikation

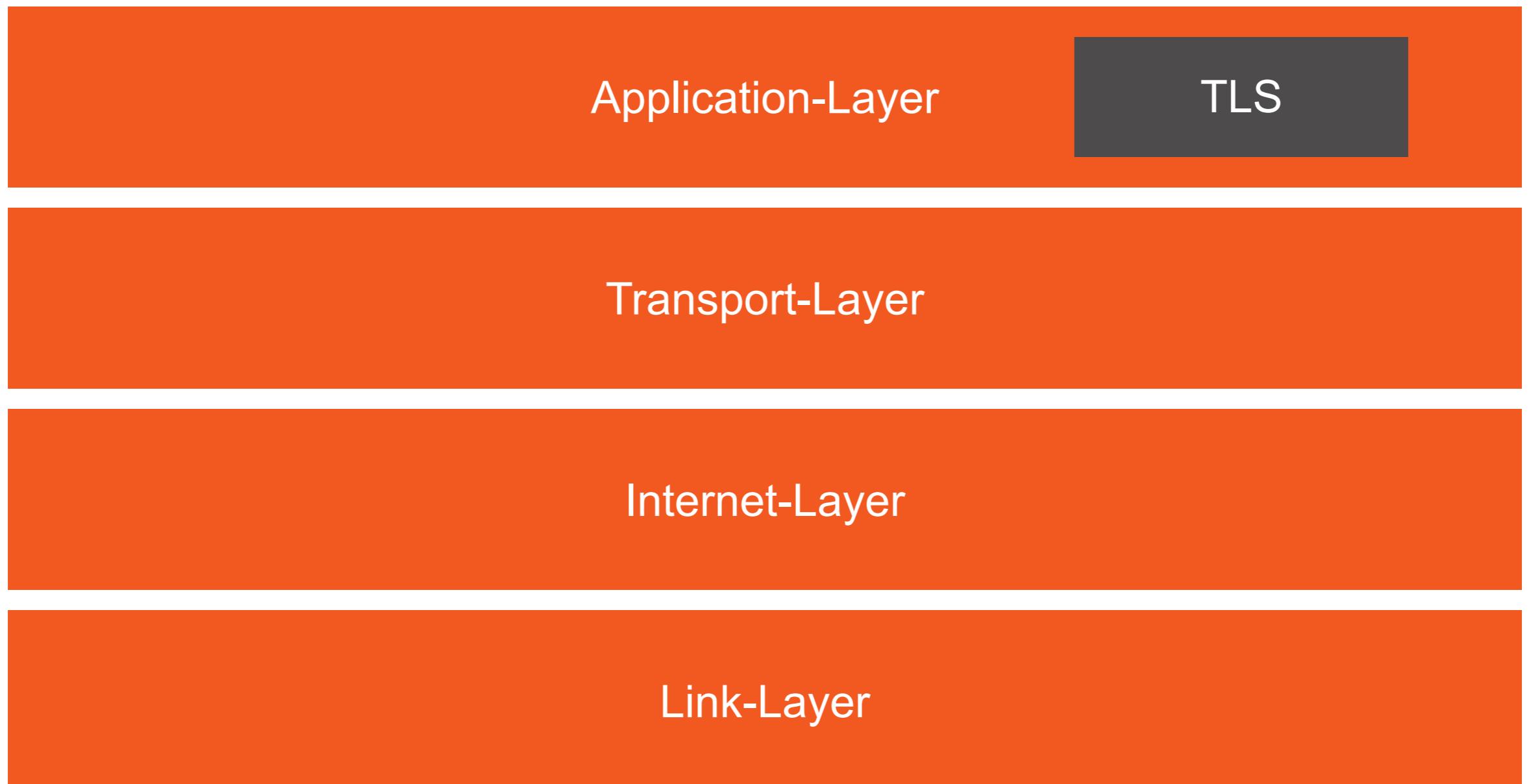
Wie funktioniert TLS?

- Grundidee
- TCP/IP-Stack
- TLS-Protokolle
- Key-Exchange

Grundidee

- Symmetrische ↘ Asymmetrische Verschlüsselung
Schlüsseltausch ↘ Performance
- Lösung Hybride Verschlüsselung:
 - Generiere zufälligen symmetrischen Schlüssel
 - Tausche ihn asymmetrisch verschlüsselt
 - Kommuniziere symmetrisch verschlüsselt

TLS im TCP/IP-Stack



Wahrgenommen:

Application-Layer

TLS

Transport-Layer

Internet-Layer

Link-Layer

TLS-Protokolle

- TLS Handshake
- TLS Record

TLS-Protokolle

- TLS Handshake
- TLS Record

Schlüsseltausch
Authentifizierung

Datenübertragung mit
Vertraulichkeit, Integrität und
Authentizität

TLS Handshake

Ziele

- Authentifizierung des Servers
(ggf. auch Client)
- Aushandeln
 - Verschlüsselungsalgorismus
 - ggf. Kompression
- Austausch symmetrischer Schlüssel

Ablauf

Client



Server



Ablauf

Client

Server

ClientHello

Unterstützte TLS-
Versionen, Cipher, Session-ID,
Kompression, zufällige
Nonce...



Ablauf

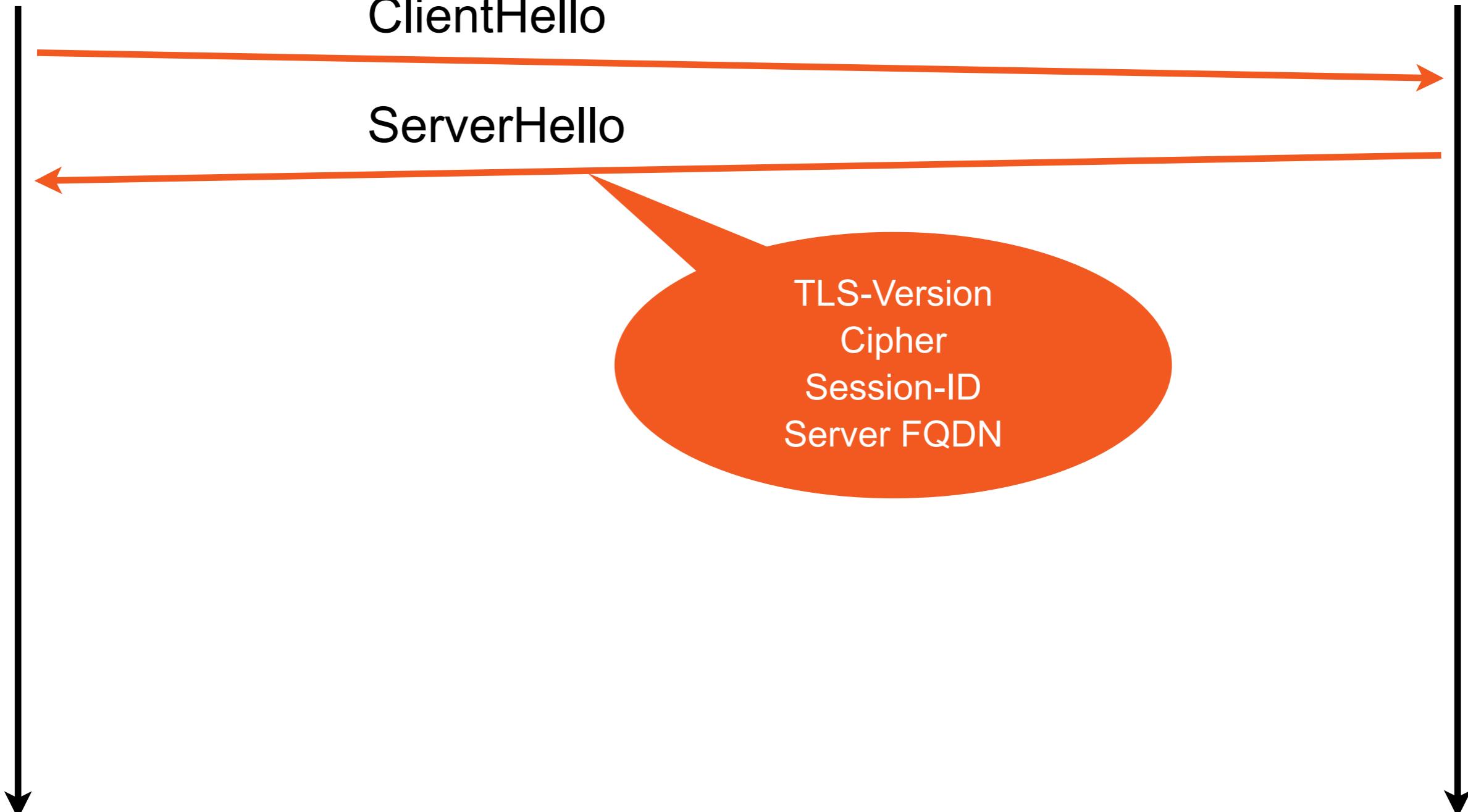
Client

Server

ClientHello

ServerHello

TLS-Version
Cipher
Session-ID
Server FQDN



Ablauf

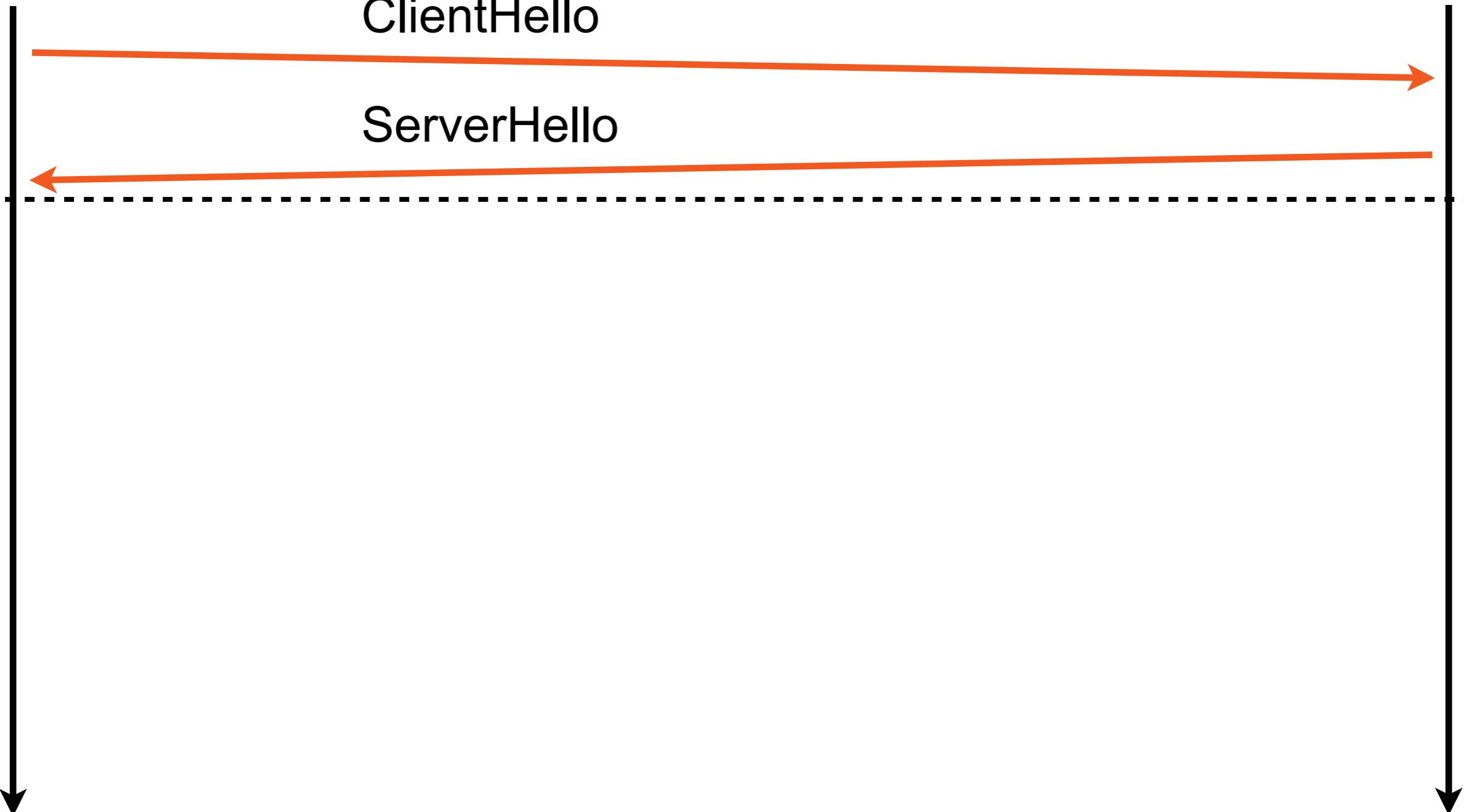
Client

Server

ClientHello

ServerHello

Verschlüsselt



Ablauf

Client

Server

ClientHello

ServerHello

Server-Cert

ggf. Client Certificate Request

ServerHello Done

Verschlüsselt



Ablauf

Client

Server

ClientHello

ServerHello

Server-Cert

ggf. Client Certificate Request

ServerHello Done

ggf. Client-Cert

ClientHello Done und Daten

Verschlüsselt



Vor ClientHello

- Client generiert sein Key-Paar und Kurvenparameter P (z.B. Curve25519)
- k_{secret_client} = Zufallswert (256 Bit)
- $k_{public_client} = P * k_{secret_client}$
- Elliptic-Curve-Krypto: ↗ Vorlesung Kryptographie

ClientHello

- Record Header (Protokoll-Version, Gesamtlänge)
- Handshake Header (Nachrichten-Typ: ClientHello)
- ClientVersion (1.2)
- 32 Byte Client-Random-Data
- Session ID (alter Mechanismus)
- Cipher Suites
- Compression Methods
- Extensions

Extensions - Beispiele

- ServerName - HTTP virtual Host Support
- Elliptic Curve Point Formats
- Elliptic Curve Supported Groups
- Session Ticket
- Encrypt-Then-MAC (Default in 1.3)
- Signature Algorithms
- Supported Versions („03 04“ = TLS 1.3)
- Pre-Shared Key Exchange
- Key Share (erlaubt verschlüsselten Handshake, P,

Vor ServerHello

- Server generiert sein Key-Paar mit P von Client
- $k_{secret_server} = \text{Zufallswert (256 Bit)}$
- $k_{public_server} = P * k_{secret_server}$

Server Hello

- Record Header
 - Handshake Header
 - Server Version (1.2, wie Client Hello)
 - 32 Byte Server Random Data
 - Session ID
 - Gewählte Verschlüsselung
 - Gewählte Kompression
 - k_{public_server}
 - Gewählte Protokoll-Version
- } Über Extensions

Key Erzeugung

- $k_{shared_secret} = k_{public_client} * k_{private_server}$
- hash=SHA384(ClientHello, ServerHello)
- Key-Erzeugungs-Funktion
 - Salt
 - Hash
 - k_{shared_secret}

Zertifikate etc.

- ServerCertificate-Nachricht
Zertifikat, ggf. „Unterschriften“
- ServerCertificate-Verify
 k_{server_public} mit Zertifikat unterschrieben
- ServerHandshake-Finished
SHA384(Handshake) mit Key signiert

Application Key

- Server Key aus Key-Derivation
- SHA384 aus allen Handshake-Nachrichten
- Neue Key-Derivation

ClientHello Done

- SHA384(Handshake) und Key via Key-Derivation
- Nachweis: Handshake unverfälscht

Tricks & Kniffe

- Einige Nachrichten als TLS 1.2 markiert
- Einige TLS 1.2-Nachrichten-Typen „mißbraucht“
- Ziel: Abwärtskompatibilität

Perfect Forward Secrecy

- Default in TLS 1.3, früher Add-On
- **Ohne** Perfect Forward Secrecy:
 - Session-Key verschlüsselt an Public Key übertragen
 - Risiko: Private Key Verlust macht alle Pakete lesbar
 - Heartbleed-Angriff
- **Mit** Perfect Forward Secrecy
 - Session-Key über sicheres Key-Austauschverfahren
 - Unabhängig von Private-Key

Session Resumption

- Spart Batterie (4% der CPU-Auslastung)
- 0 Round-Trip statt 1 Round-Trip → schneller
- Lösung: Session-Ticket
 - Verschlüsselt mit Server Ticket Encryption Key (STEK)
 - Einzig bei Client gespeichert
- Contra: Keine Perfect Forward Secrecy
 - STEK gebrochen → Session Key bekannt
 - Empfehlung: STEK-Wechsel alle 24h

Session Resumption

- TLS 1.3:
 - Wahlweise neuer Diffie-Hellman-Key-Exchange
 - Hashed Master-Secret (statt „plain“ in TLS 1.2)
- Early Application Data
 - Unmittelbar nach Übertragen der Session-ID
 - Ggf. nicht forward-secure

TLS Record

- Datenübertragung in max. 16 KB Blöcken
- verschlüsselt
- MAC für
 - Integrität
 - Authentizität

Stärken von TLS 1.3

- Perfect Forward Secrecy
- Elliptic Curve Kryptographie
- Schlanker als TLS 1.2
- Single Round Trip Verbindungsaufbau
- Zero Round Trip Session-Resumption

Nachteile von TLS

- Network Intrusion Detection System eingeschränkt
- Data Ex- / Infiltration schwerer zu erkennen

Literatur-Hinweise

- RFC8446, 8448 - TLS + Beispiel-Handshakes
- RFC5077 Session Resumption
- RFC9147 - TLS über UDP
- <https://tls13.xargs.org/> - Illustrated TLS 1.3 Connection
- <https://tlseminar.github.io/> - TLS Seminar
- <https://curves.xargs.org/> - Elliptic Curves Überblick
- <https://x25519.xargs.org/> - Elliptic Curve Key Exchange

„Alt“: FREAK

- Factoring Attack on
- RSA
- EXPORT
- Keys

Export Keys?

- USA hielt Verschlüsselung für Waffe
→ Exportbeschränkung
- Aber: HTTPS ohne Verschlüsselung?
- „Lösung“: Rückfall auf schwache Verschlüsselung
Schwach: NSA kann knacken



FREAK-Angriff

- client_hello: Liste sicherer Verfahren
- server_hello: Wählt Export_RSA
- Bug in OpenSSL: Client akzeptiert

Und weiter?

- Factoring des RSA-Keys
- Erleichtert: Da Export bloß 40-Bit Schlüssellänge

Lohnt sich das?

- Nicht für eine Sitzung
- Aber: Apache mod_ssl berechnet einen RSA-Export-Key beim Start
- Denn: RSA-Key-Generierung ist aufwendig

Konsequenzen für Angreifer

- Man-In-The-Middle möglich



NSA Careers

Welcome! Please enter your user name and password to login. If you have not yet registered, click [here](#).

To view additional job openings, click [here](#). Enter key words then click on the "Search" button.

If you do not remember your password, click [here](#).



Basic Job Search

Keywords:	<input type="text"/>
Posted:	Anytime
Search Advanced Search Search Tips	
User Name:	<input type="text"/>
Password:	<input type="password"/>
Login Login Help Register Now	

Select all positions of interest.

Job Postings

				First	Previous	Next	Last
				View 100 1-25 of 176			
<u>Job Title</u>	<u>Job ID</u>	<u>Location</u>					
<input type="checkbox"/> General Counsel, National Security Agency	1055972	Fort George G. Meade, MD					
<input type="checkbox"/> Attorney	1055851	Fort George G. Meade, MD					
<input type="checkbox"/> Cooperative Education Program	1055679	Fort George G. Meade, MD					
<input type="checkbox"/> Language Analyst - Chinese (Mandarin)	1055121	Multiple Locations					
<input type="checkbox"/> Software Engineer	1052899	Honolulu, HI					
<input type="checkbox"/> Software Engineer	1055116	Denver, CO					
<input type="checkbox"/> Multimedia Producer	1055158	Fort George G. Meade, MD					
<input type="checkbox"/> Research Post-Graduate and Postdoctoral Program (RDGPD)	1054712	Fort George G. Meade, MD					

This is not the page you think it is!
Yes, it has the right certificate above.
Do you really want a job here?



Safari is using an encrypted connection to www.nsa.gov.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.nsa.gov.

GeoTrust Global CA
↳ GeoTrust SSL CA - G4
↳ www.nsa.gov



www.nsa.gov

Issued by: GeoTrust SSL CA - G4

Expires: Monday 8 February 2016 22 h 14 min 42 s Central European Standard Time

This certificate is valid

► Trust

► Details



Hide Certificate

OK

HACKERS BRIEFLY TOOK
DOWN THE WEBSITE OF
THE CIA YESTERDAY...



WHAT PEOPLE HEAR:

SOMEONE HACKED
INTO THE COMPUTERS
OF THE **CIA**!!



WHAT COMPUTER
EXPERTS HEAR:

SOMEONE TORE DOWN
A POSTER HUNG UP
BY THE **CIA**!!



```
##  
# Host Database  
#  
# localhost is used to configure the loopback interface  
# when the system is booting. Do not change this entry.  
##  
127.0.0.1      localhost  
255.255.255.255 broadcasthost  
::1            localhost  
fe80::1%lo0    localhost  
  
#127.0.0.1 www.nsa.gov  
  
#127.0.0.1 connect.facebook.net  
#127.0.0.1 www.hsbc.com  
#127.0.0.1 www-secure.symantec.com
```

```
##  
# Host Database  
#  
# localhost is used to configure the loopback interface  
# when the system is booting. Do not change this entry.  
##  
127.0.0.1      localhost  
255.255.255.255 broadcasthost  
::1            localhost  
fe80::1%lo0    localhost  
  
#127.0.0.1 www.nsa.gov  
  
#127.0.0.1 connect.facebook.net  
#127.0.0.1 www.hsbc.com  
#127.0.0.1 www-secure.symantec.com
```

Konsequenzen für Entwickler:

- Prüfen:
 - Passt Server-Reaktion zur Client-Anfrage?
- Finger weg von Export-Beschränkungen und Hintertüren.

**Wenn falsch
verschlüsselt ist:
Enterprise TLS**

TLS

- Transport Layer Security
- Hybride Verschlüsselung
- Bei Forward Secrecy:
Schlüsseltausch mit Diffie-Hellmann

Grober Ablauf

Client Hello



Problem

Ist Server oder Client Private Key kompromittiert
→ Gesamte frühere Kommunikation geknackt

Lösung: Forward Secrecy

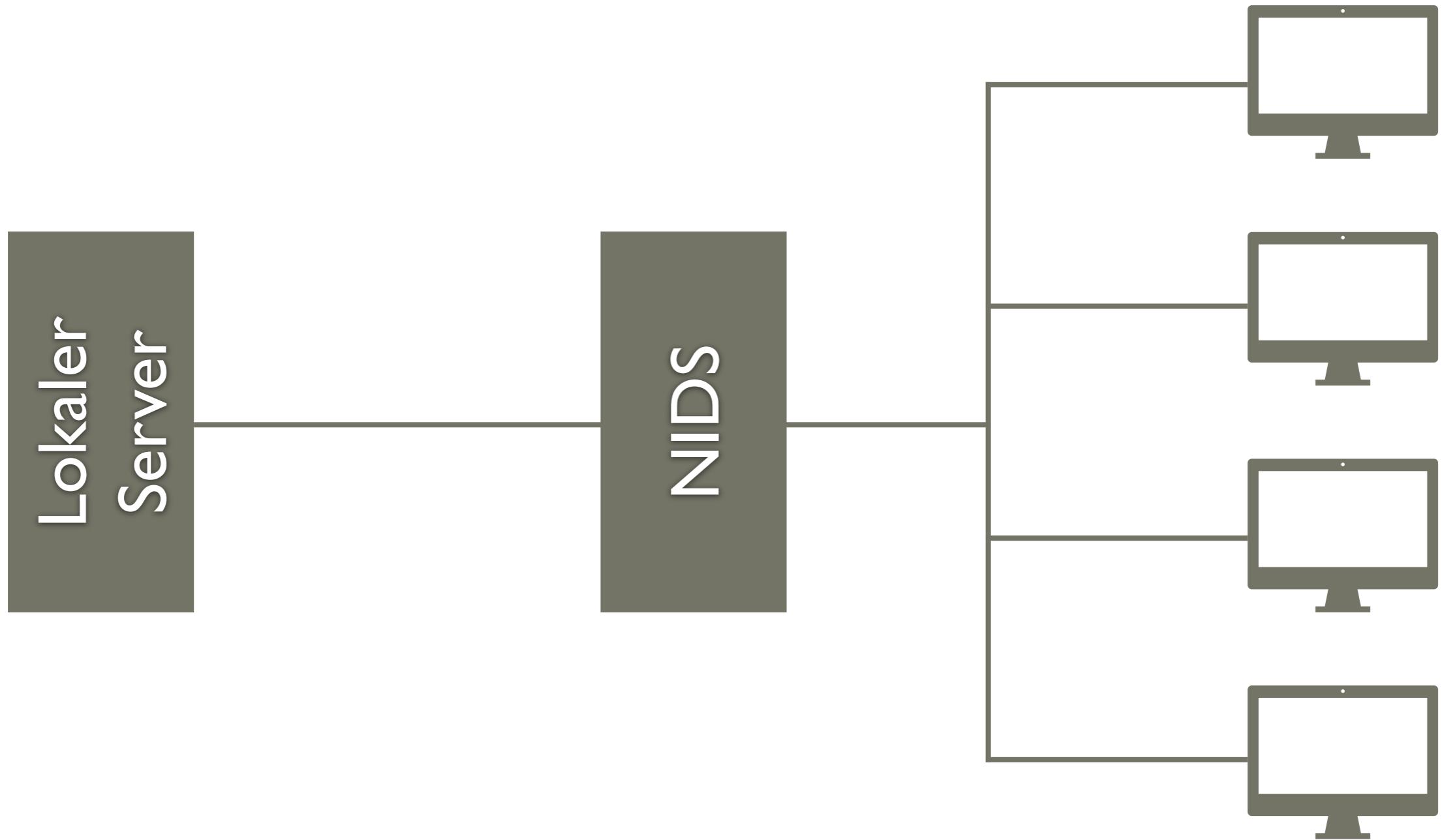
NIDS \leftrightarrow TLS

Paketanalyse erfordert Einsicht in Pakete

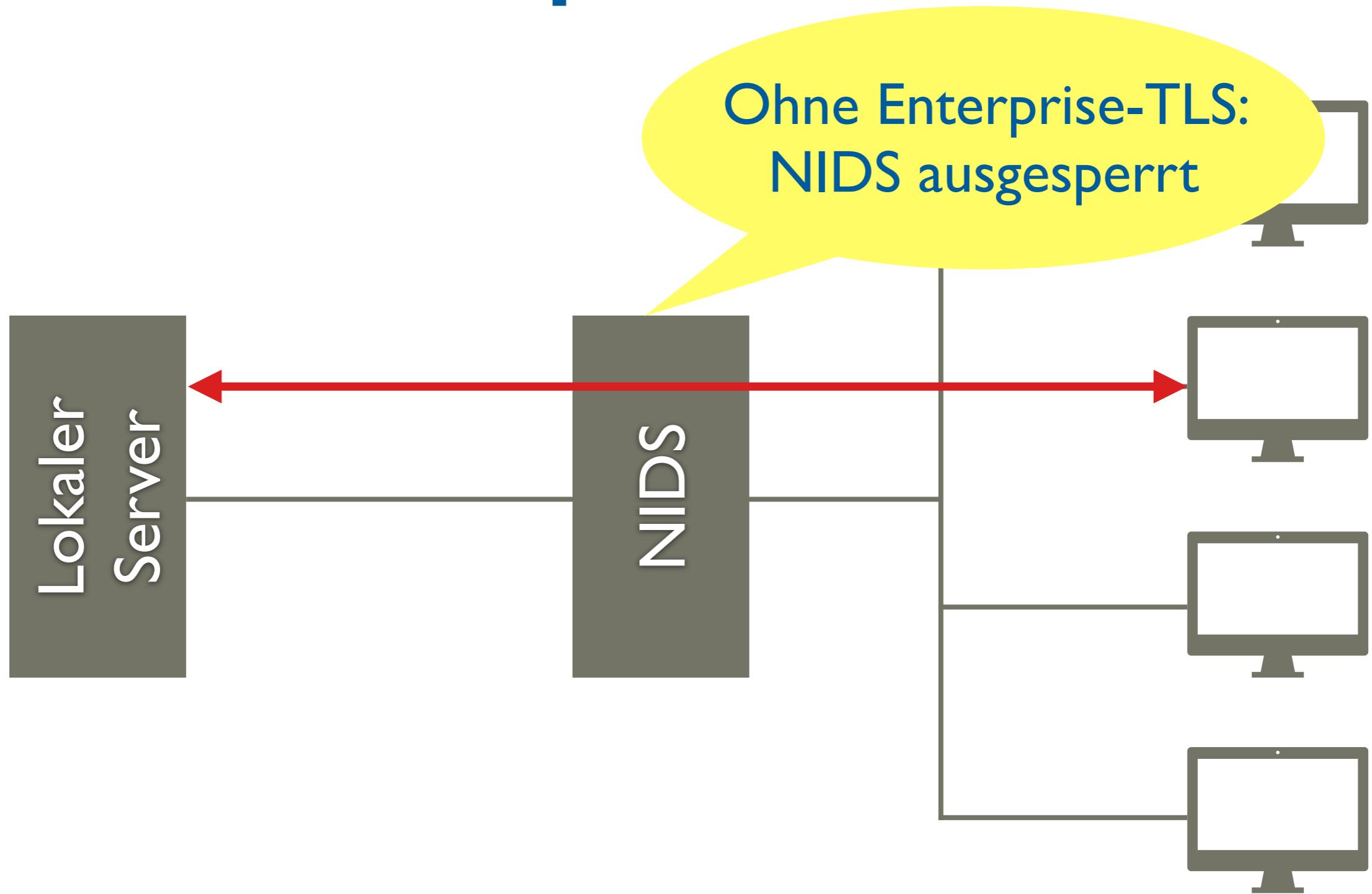


Verschlüsselung schafft Vertraulichkeit

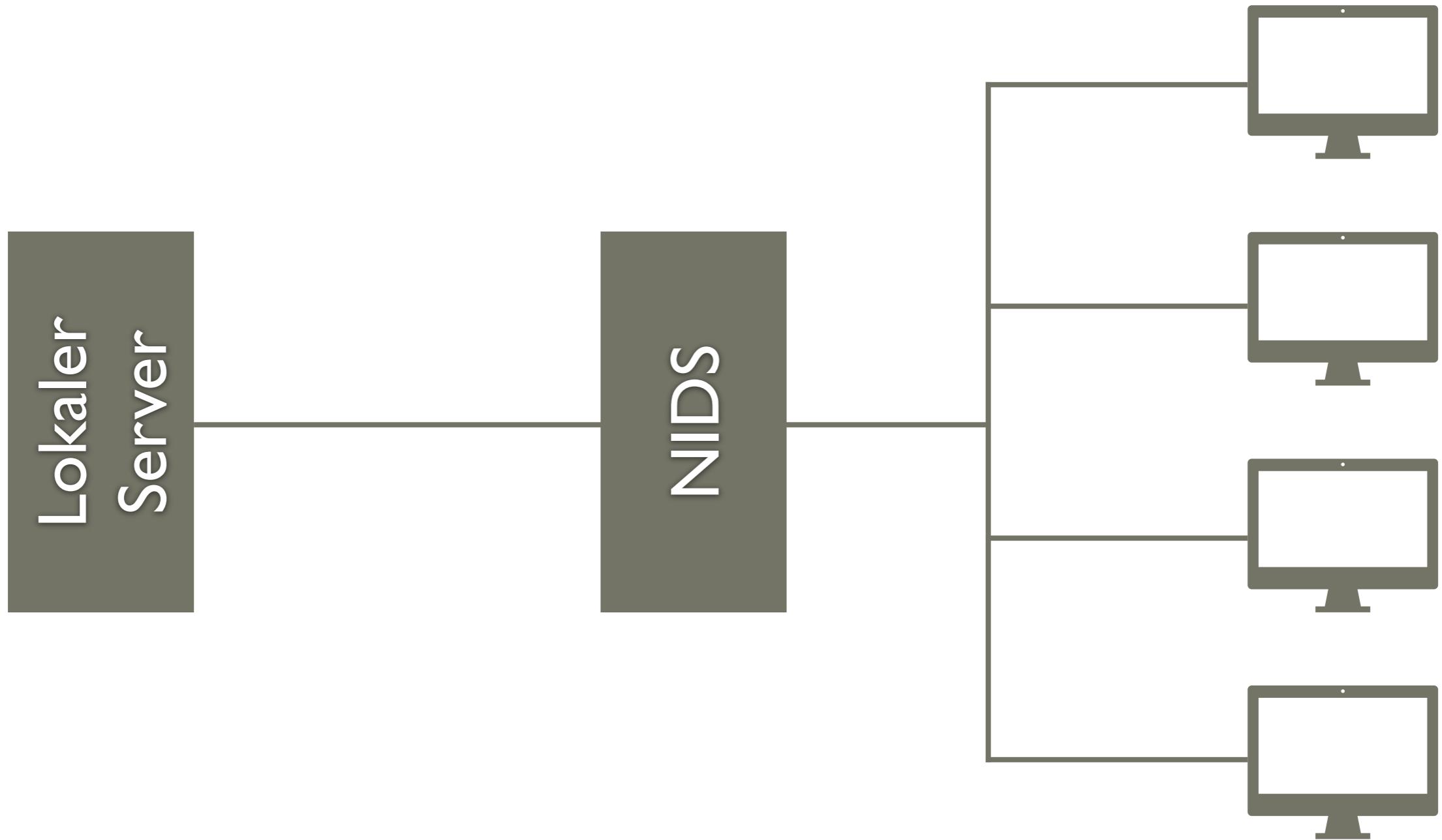
Enterprise TLS



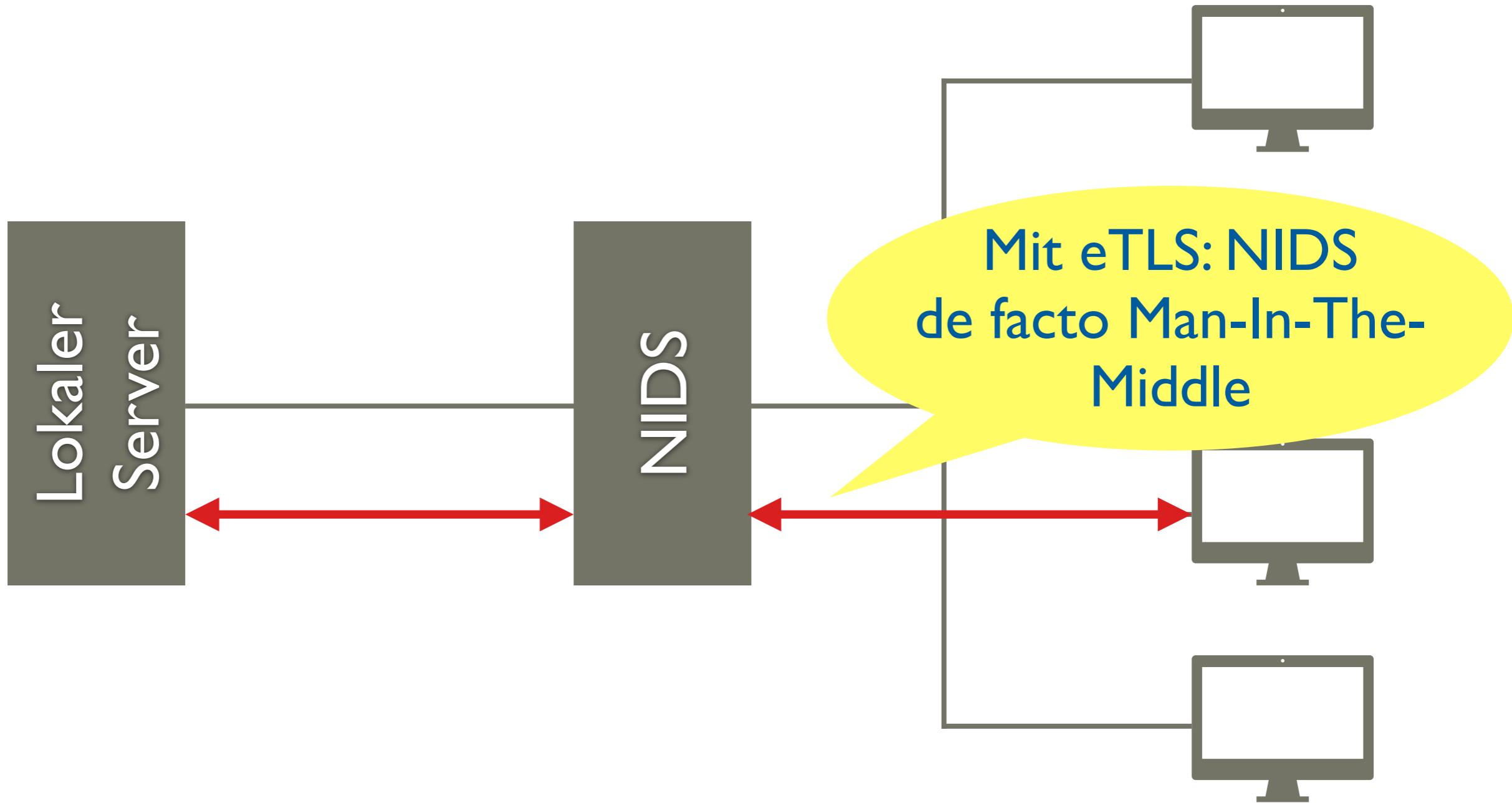
Enterprise TLS



Enterprise TLS



Enterprise TLS



Wie MitM realisieren?

- Fixer Zufallswert bei Diffie-Hellmann
→ stets gleicher Schlüssel
- Fixer Zufallswert in NIDS hinterlegt
→ NIDS kann mitlesen

Nebeneffekt:

- Forward Secrecy abgeschafft.
- Knacken des Private Keys
→ Knacken aller Nachrichten

ETSI-Vorschlag

ETSI TS 103 523-3 v1.2.1 (2019-03)



CYBER;
Middlebox Security Protocol;
Part 3: Enterprise Transport Security

Hinweis

- eTLS wg. Namensrechten an TLS unzulässig
- Offizieller Name:
ETSI Enterprise Transport Security (ETS)
- eTLS / ETS = CVE-2019-9191 (26.02.2019)

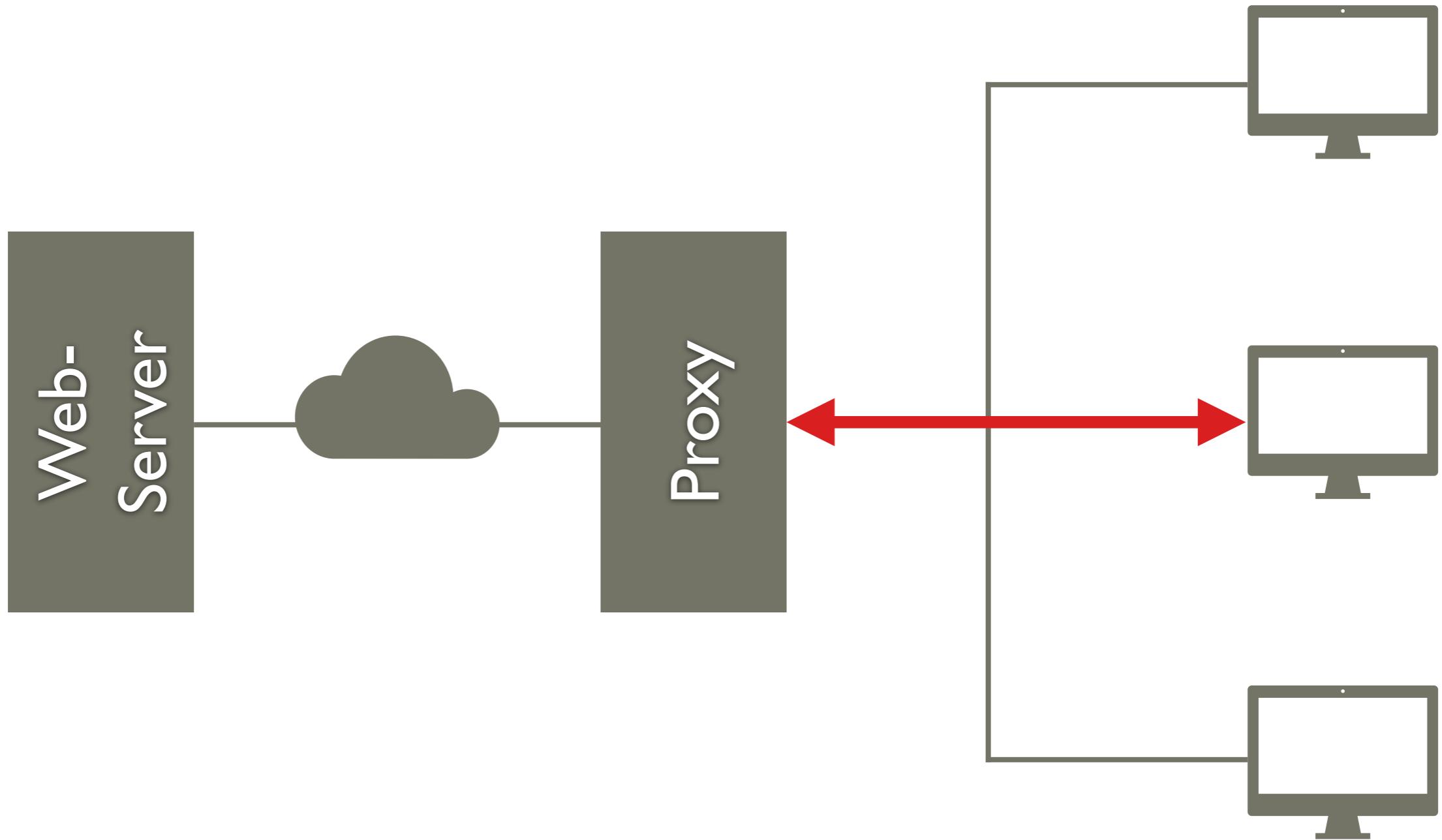
Pros & Cons

- Vorsätzliche Backdoor in Verschlüsselung
- Forward Secrecy abgeschaltet
- Monitoring des Netzwerktraffics möglich
- Datenschutz? Geheimschutz?

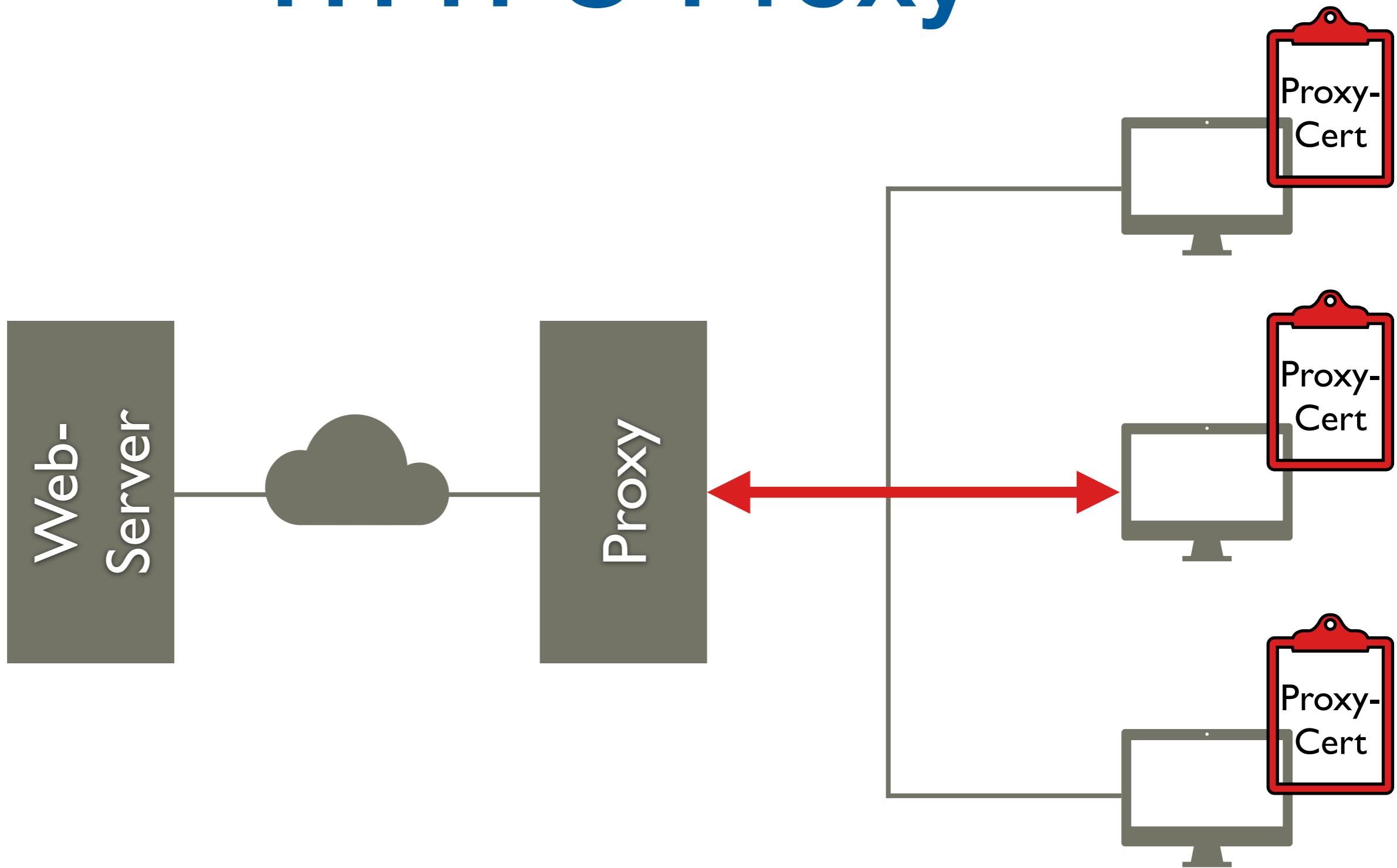
Alternative: HTTPS-Proxy

- Konzept ähnlich:
Proxy-Zertifikat auf den Clients hinterlegt
 - Vertrauenswürdig
 - Für alle entfernten System gültig

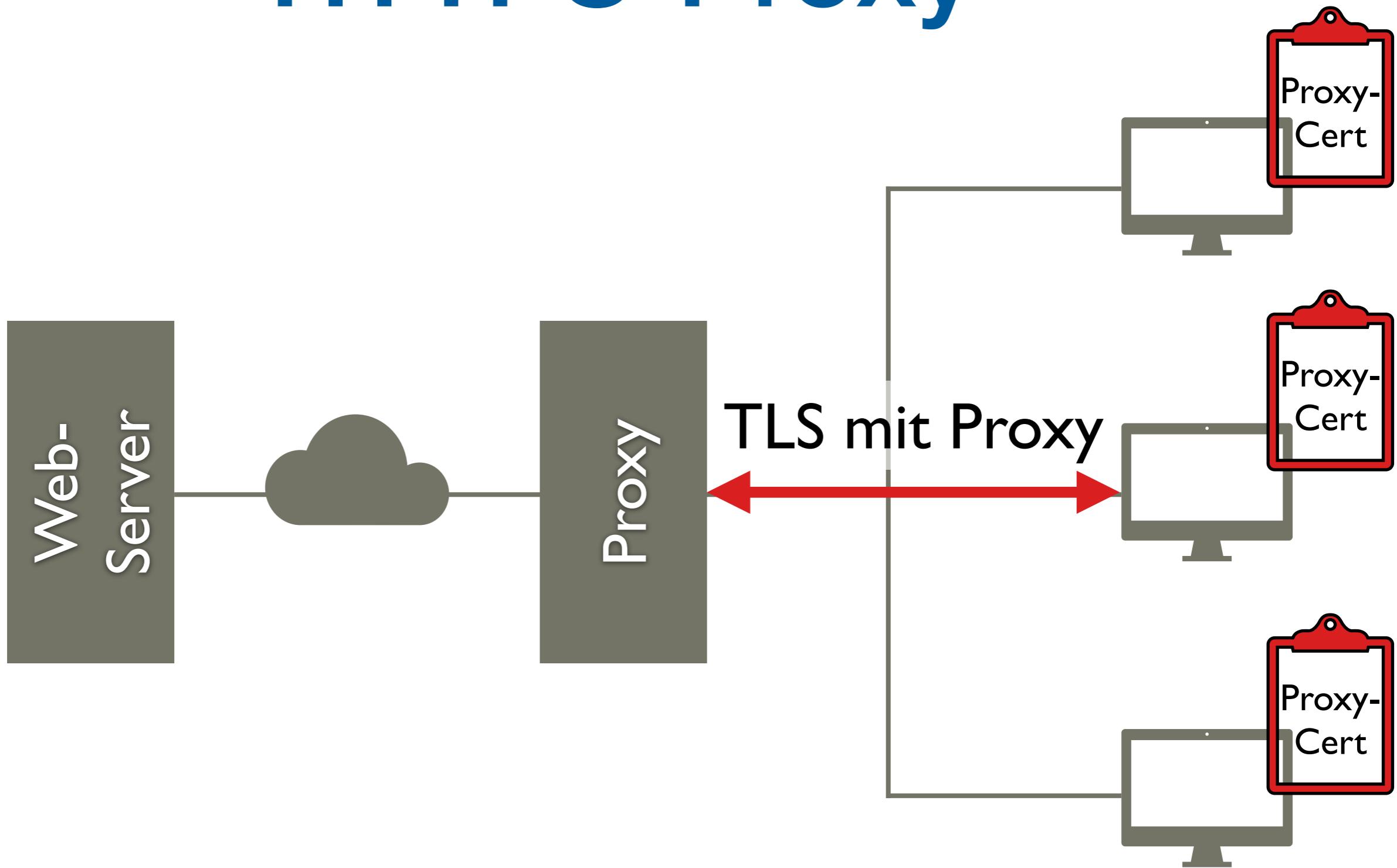
HTTPS-Proxy



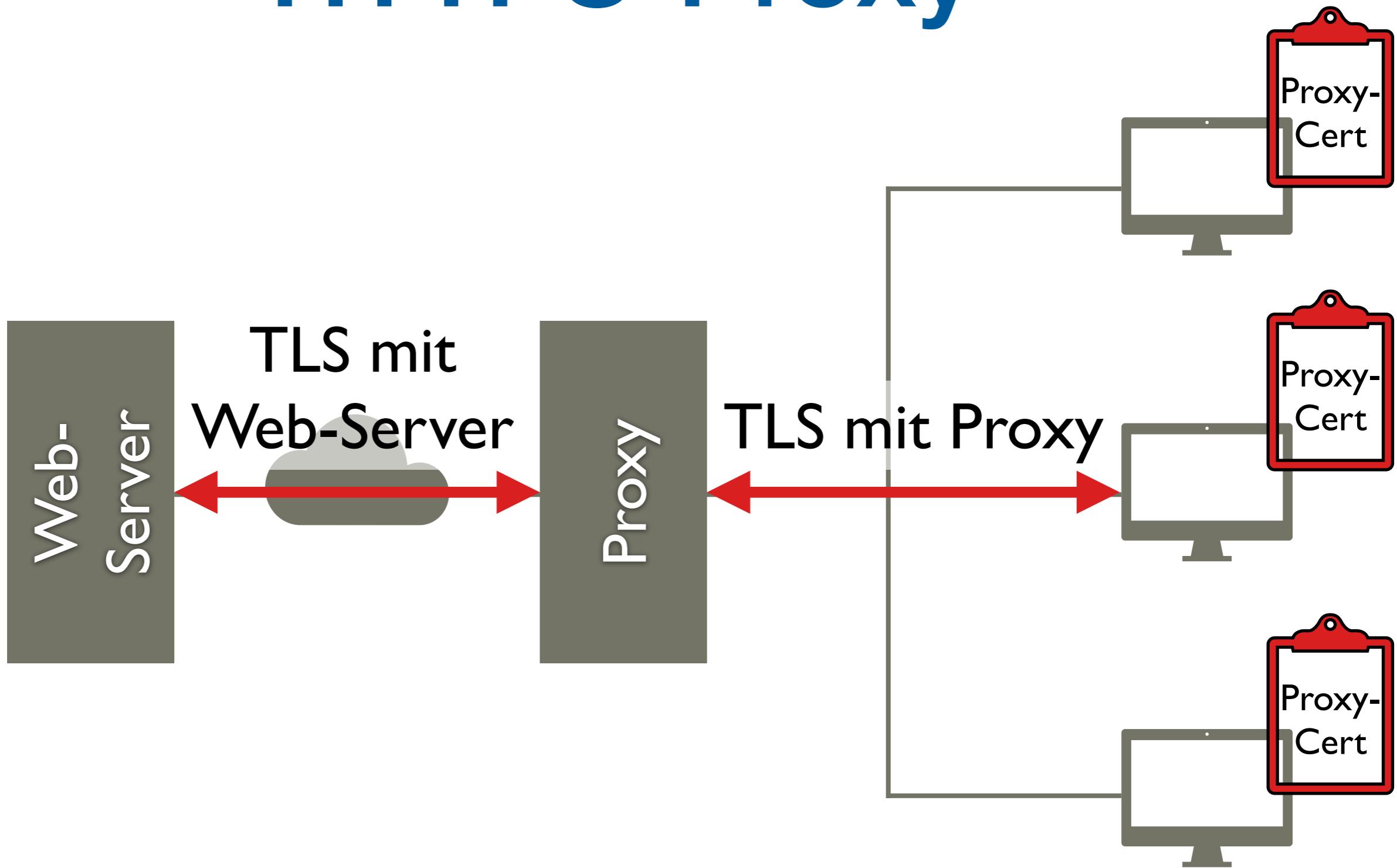
HTTPS-Proxy



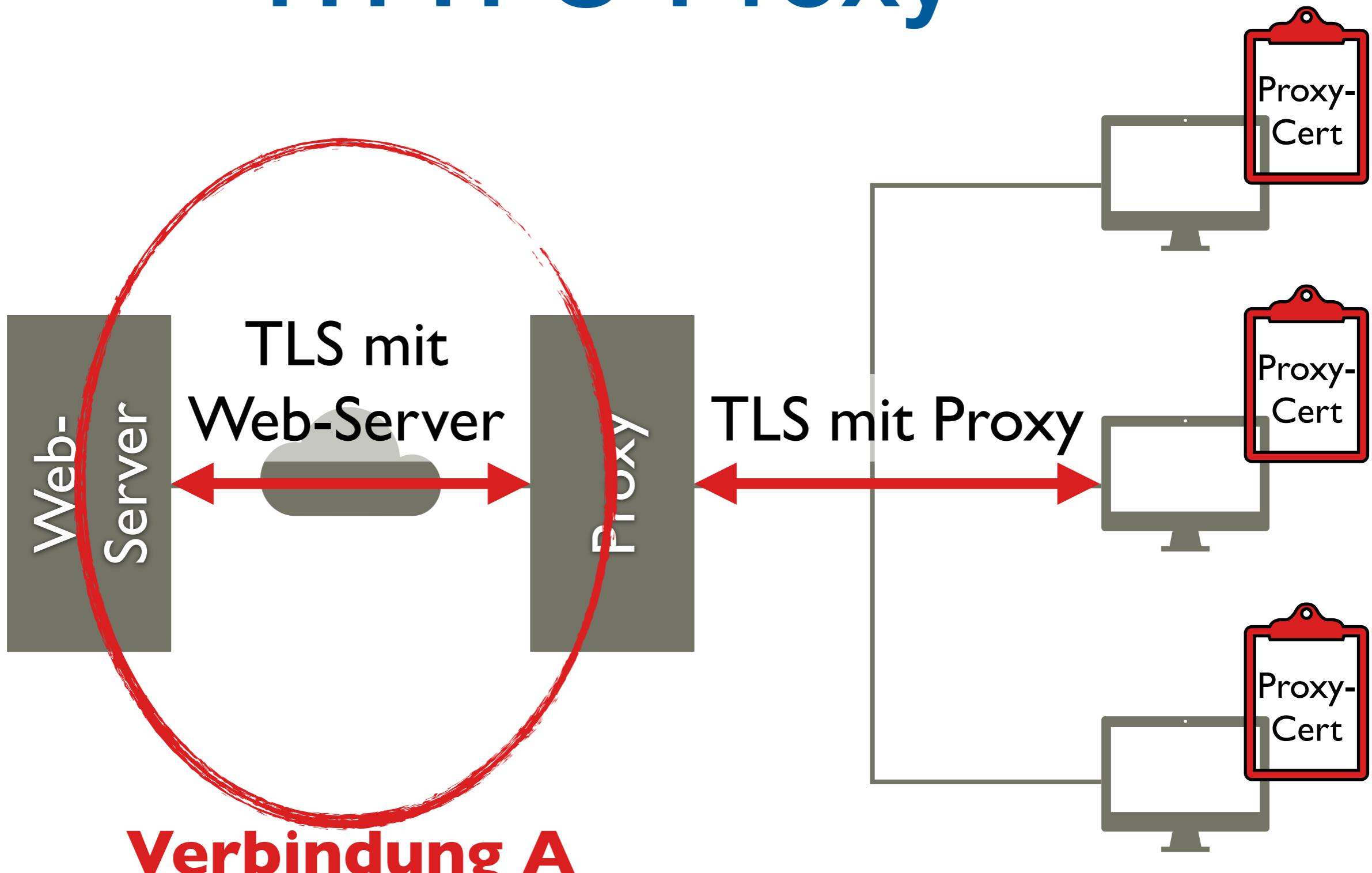
HTTPS-Proxy



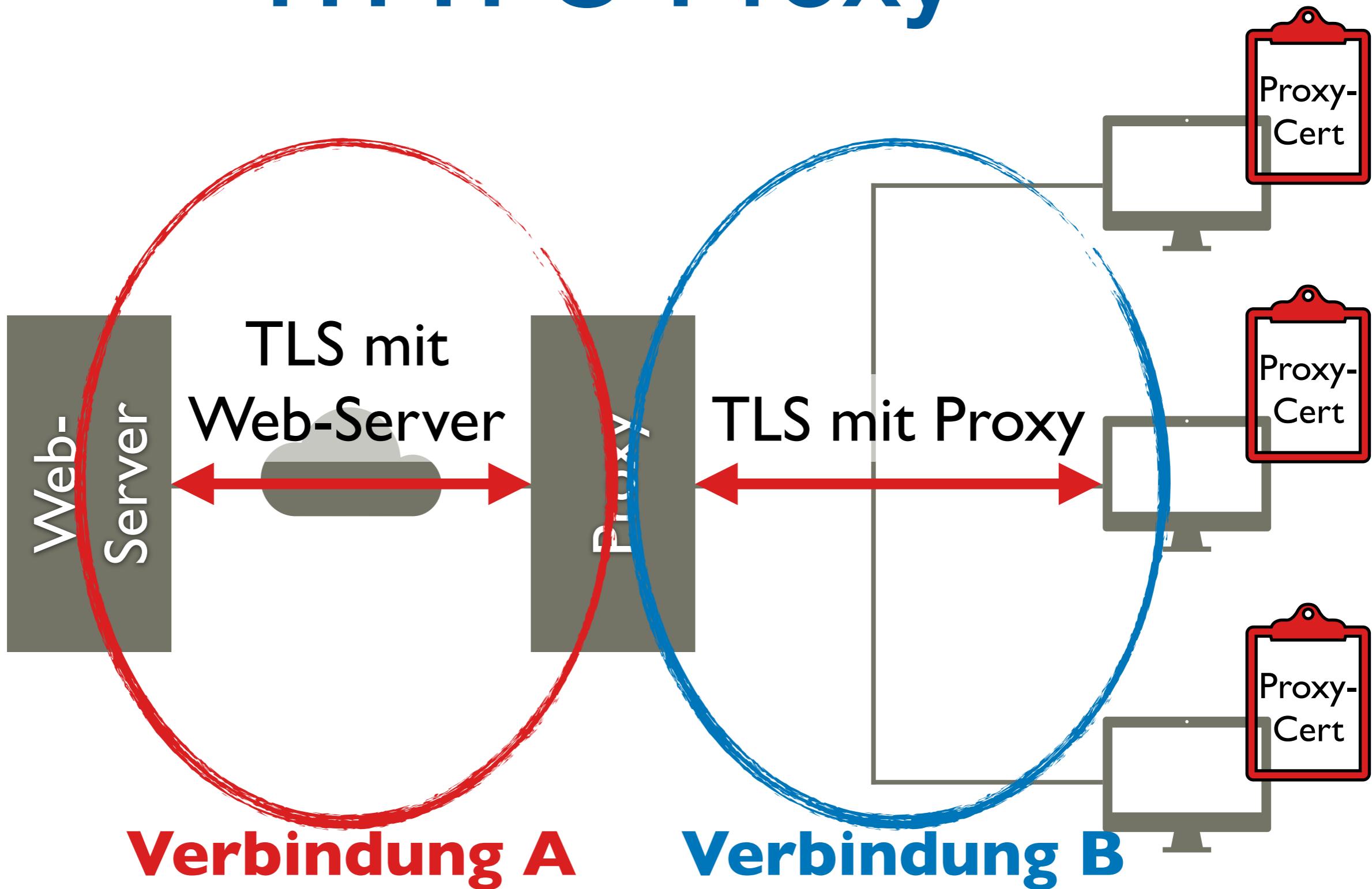
HTTPS-Proxy



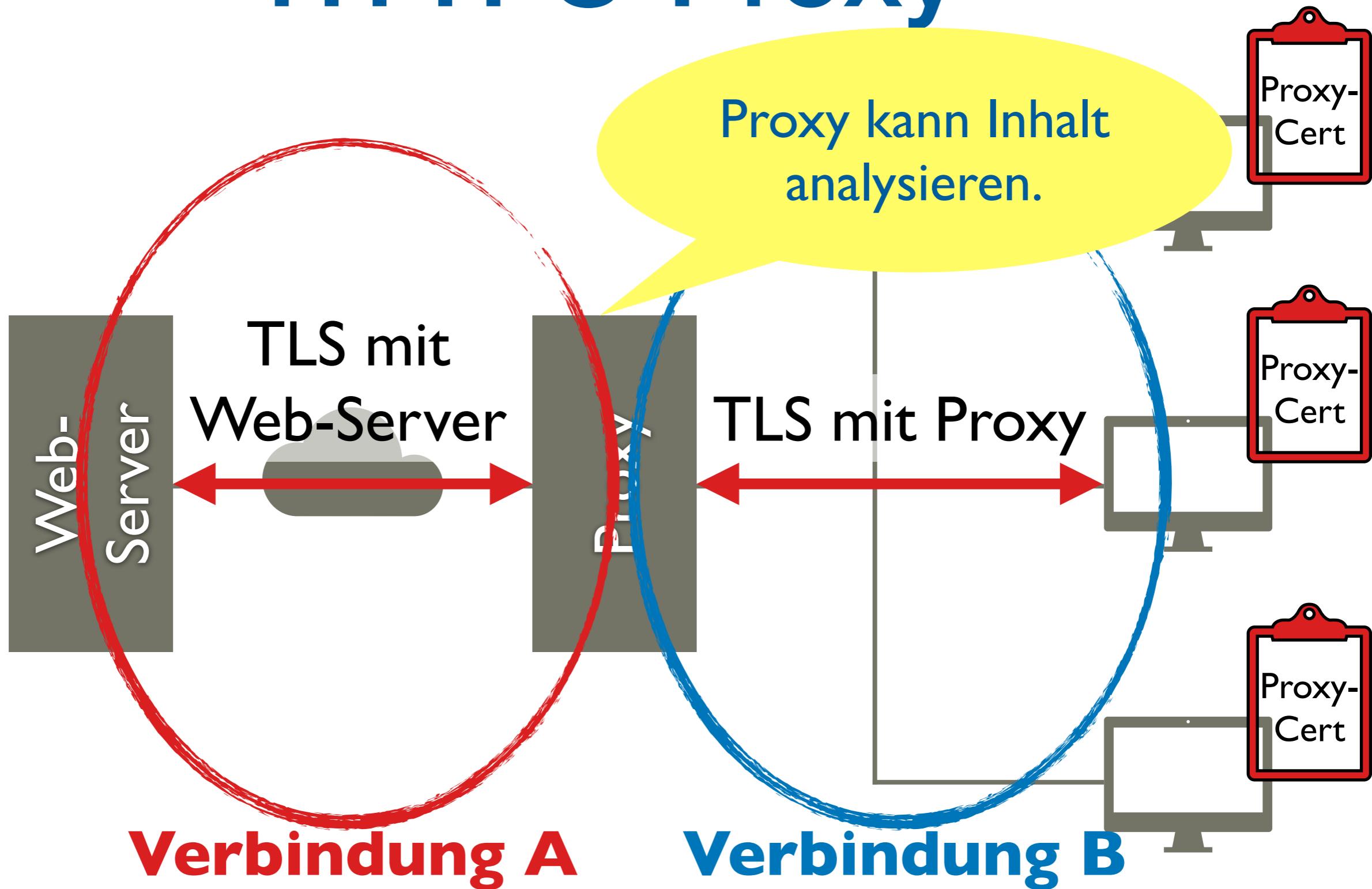
HTTPS-Proxy



HTTPS-Proxy



HTTPS-Proxy



Pros & Cons

- Proxy-fähiges Protokoll erforderlich
- Verschlüsselung hinfällig, wenn Proxy kompromittiert
- Datenschutz? Geheimschutz?

Heartbleed

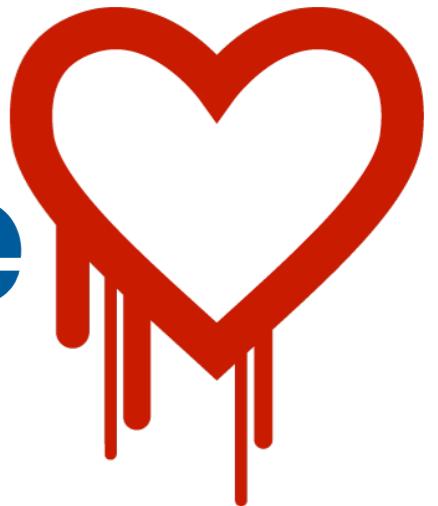


Heartbleed



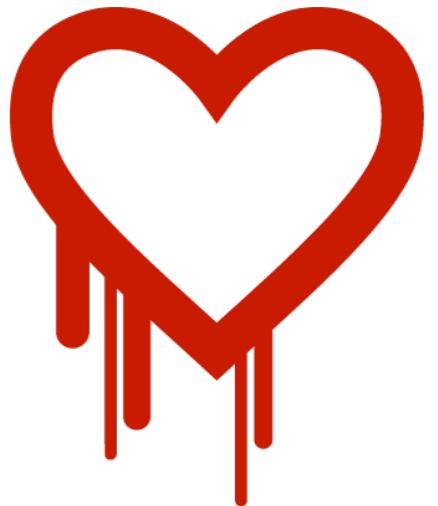
- Betroffen ist OpenSSL 1.0.1 bis 1.0.1f
- Angriff auf: Heart-Beat-Funktionalität von TLS/SSL
- Gefahr: Auslesen beliebiger Speichermengen des Servers
 - u.a. Ausspähen der SSL secret keys
 - Entschlüsseln neuer und „alter“, mitgeschnittener Nachrichten

Betroffene Systeme

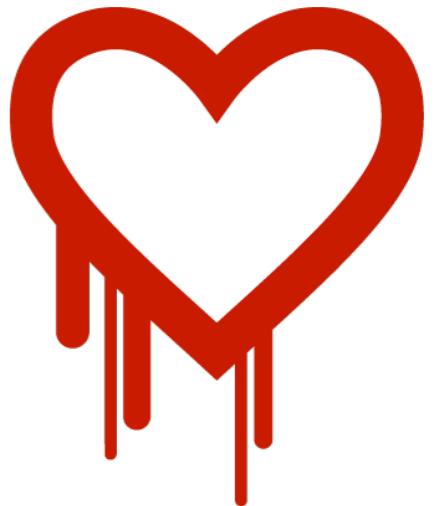


- HTTPS
- IMAPS
- POP3S
- VPN
- ...

Funktionsweise Heartbeat



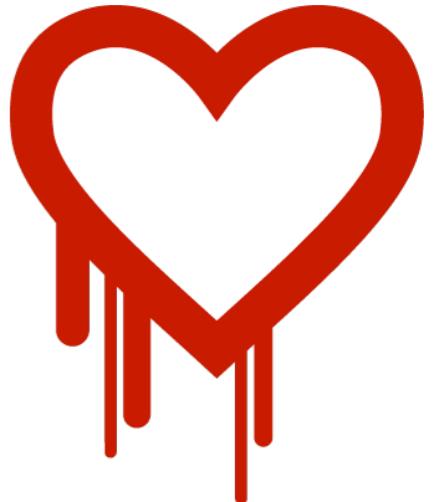
Funktionsweise Heartbeat



Heartbeat-Request



Funktionsweise Heartbeat



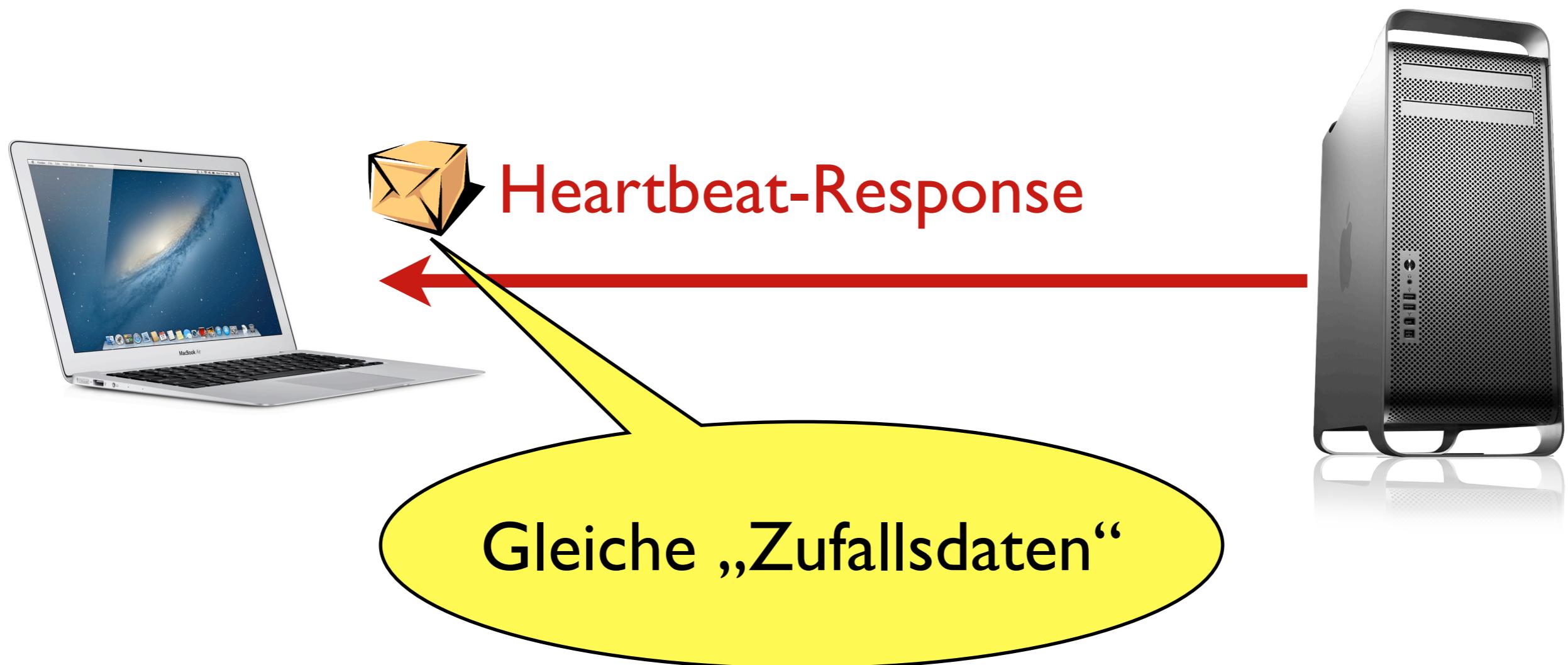
Enthält: „Zufällige“ Daten



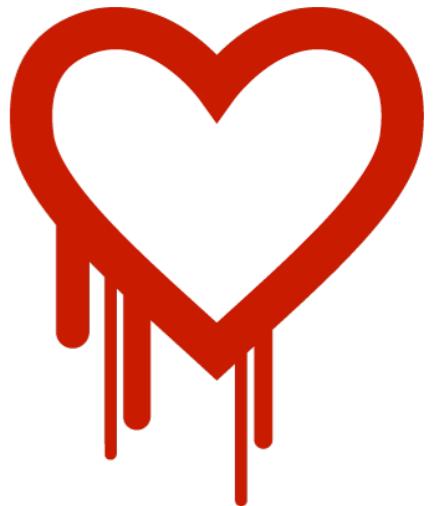
Heartbeat-Request



Funktionsweise Heartbeat



Funktionsweise Heartbeat



Heartbeat-Paket



- Heartbeat-Header-Feld: payload_length
- SSL-Header-Feld: Länge des Inhalts

Heartbeat-Paket



OpenSSL wertet nur
diesen Header aus.

- Heartbeat-Header-Feld: payload_length
- SSL-Header-Feld: Länge des Inhalts

Heartbeat-Paket



- Heartbeat-Header-Feld: payload_length
- SSL-Header-Feld: Länge des Inhalts

Erkennt also keinen
Widerspruch dazu.

Heartbeat-Paket

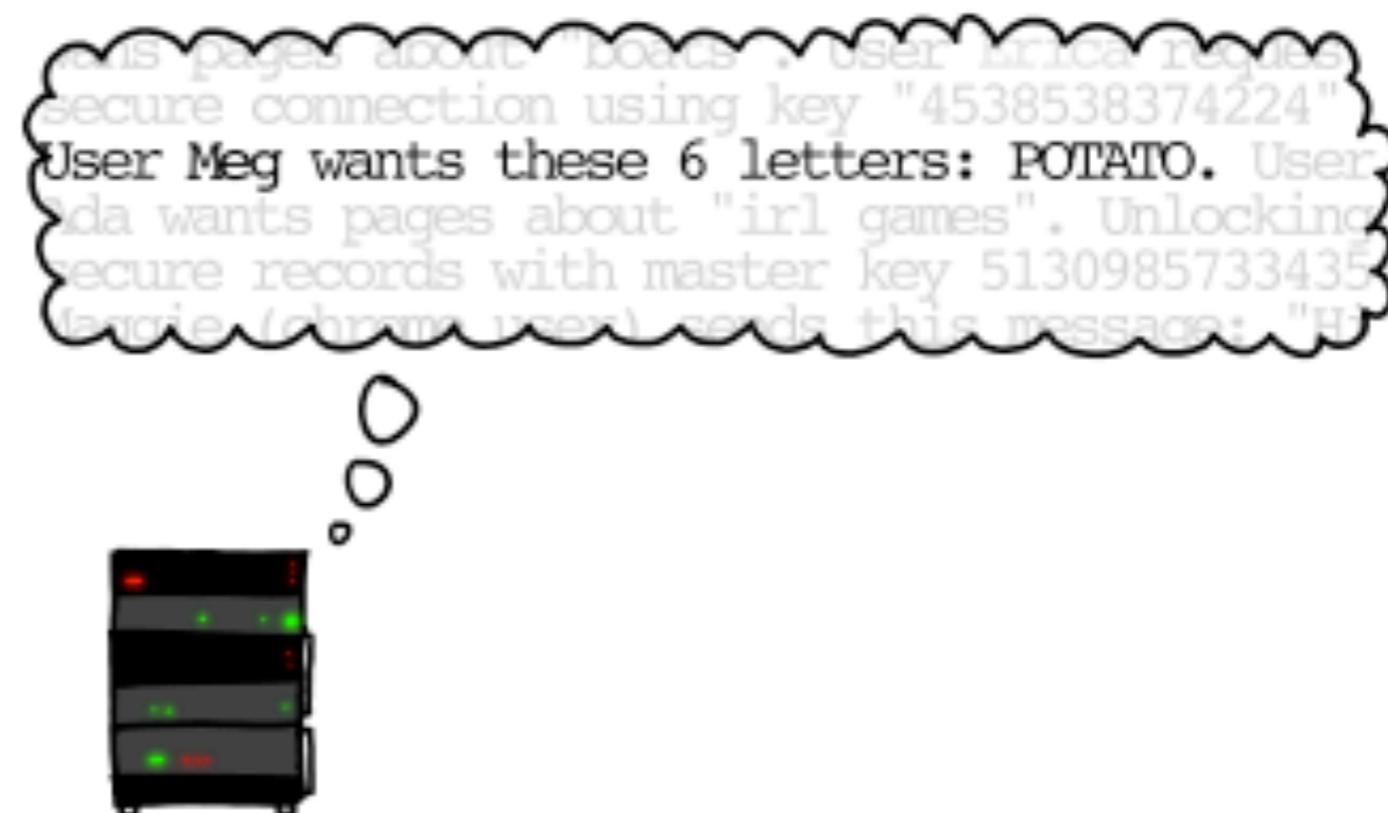


Und prüft auch nicht die
übertragene Datenmenge

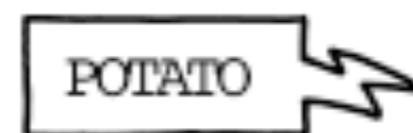
- Heartbeat-Header-Feld: payload_length
- SSL-Header-Feld: Länge des Inhalts

HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



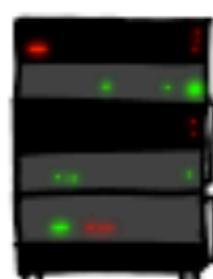
User Meg wants these 6 letters: **POTATO**. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435 Maggie (chrome user) sends this message: "H



SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).



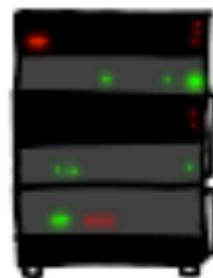
User Olivia from London wants pages about "nar
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 348
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2ceb9ff89bd3bf84



HMM...



BIRD

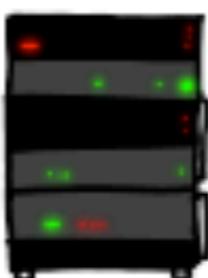


User Olivia from London wants pages about "nar
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: **BIRD**. There are currently 348
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2ceb9ff89bd3bf84

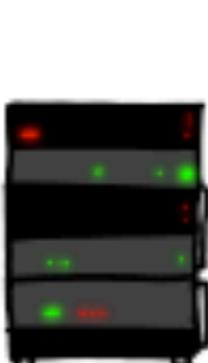
SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).

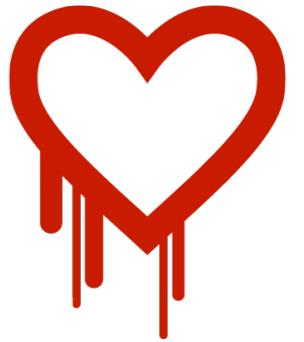


a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
"snakes but not too long". User Karen wants to
change account password to "CoHeBaSt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHeBaSt". User

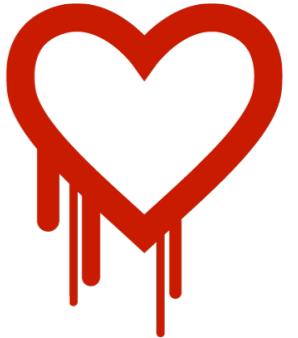




Code-Auszug

```
/* Allocate memory for the response, size is 1 byte message type,
 * plus 2 bytes payload length, plus payload, plus padding
 */
buffer = OPENSSL_malloc(1 + 2 + payload + padding);
bp = buffer;

/* Enter response type, length and copy payload */
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
bp += payload;
/* Random padding */
RAND_pseudo_bytes(bp, padding);
r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload +
padding);
```



Aus dem TLS-Header

HSZUG

```
/* Allocate memory for the response, size is 1 byte message type,  
 * plus 2 bytes payload length, plus payload, plus padding  
 */  
  
buffer = OPENSSL_malloc(1 + 2 + payload + padding);  
bp = buffer;  
  
/* Enter response type, length and copy payload */  
*bp++ = TLS1_HB_RESPONSE;  
s2n(payload, bp);  
memcpy(bp, pl, payload);  
bp += payload;  
/* Random padding */  
RAND_pseudo_bytes(bp, padding);  
r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload +  
padding);
```



Code-Auszug

```
/* Allocate memory  
 * plus 2 bytes  
 */  
buffer = OPENSSL_malloc(payload + 2);  
bp = buffer;  
  
/* Enter response type, length and copy payload */  
*bp++ = TLS1_HB_RESPONSE;  
s2n(payload, bp);  
memcpy(bp, pl, payload);  
bp += payload;  
/* Random padding */  
RAND_pseudo_bytes(bp, padding);  
r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload +  
padding);
```

„übertragenen“
Speicherinhalt hineinkopieren



Code-Auszug

```
/* Allocate memory for the response, size is 1 byte message type,  
 * plus 2 bytes payload length, plus payload, plus padding  
 */  
  
buffer = OPENSSL_malloc(1 + 2 + payload + padding);  
bp = buffer;  
  
/* Enter response type, length and copy payload */  
*bp++ = TLS1_HB_RESPONSE;  
s2n(payload, bp);  
memcpy(bp, pl, payload);  
bp += payload;  
/* Random padding */  
RAND_pseudo_bytes(bp, padding);  
r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload +  
padding);
```

Zurücksenden.



Code-Auszug

```
/* Allocate memory for the response, size is 1 byte message type,
 * plus 2 bytes payload length, plus payload, plus padding
 */
buffer = (char*) malloc(3 + payload + padding);

Kein Standard-malloc
/* Copy payload */
*bp++ = payload;
s2n(payload, bp);
memcpy(bp, pl, payload);
bp += payload;
/* Random padding */
RAND_pseudo_bytes(bp, padding);
r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload +
padding);
```

OPENSSL_malloc



- Standardfall: Wrapper um malloc
- Ggf. anderweitig konfigurierbar

Probleme



- OpenSSL entschlüsselt Buffer „in place“
- OpenSSL verwaltet eigene Free-List
- Quelle nicht vollständig gefüllt
→ „Überlesen“ von Daten oberhalb des Quellbereichs

Eigene Free-List



- Beschleunigt finden freien Speichers
- Merkt sich genutzte „Blöcke“
- „Spart“ malloc-Aufrufe

Out of Bounds Read

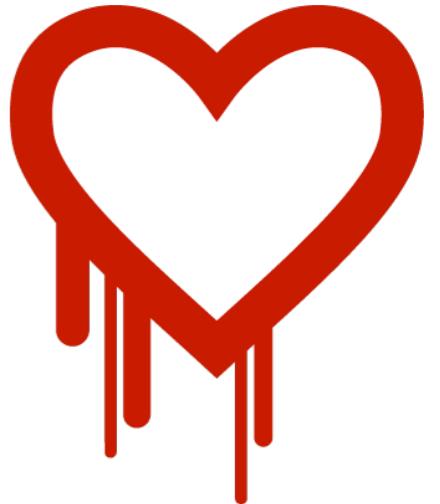


Beispiel



```
int main(int argc, char * argv [])
{
    char geheim[] = "Hier steht irgendwas gaaaaanz wichtiges.";
    char schmarrn[] = "Und hier ein Schmarrn zum Kopieren.";
    char *buff;
    unsigned int size = 200;
    buff = malloc(size);
    if (buff == 0) { printf ("Speicherfehler. Abbruch."); }
    else
    {
        printf ("Zufälliger Inhalt des Buffers: \n");
        hexDump(buff, size);
        memcpy(buff, schmarrn, size);
        printf("Inhalt des Buffers nach memcpy: \n");
        hexDump(buff, size);
    }
}
```

Ausprobieren



`./out_of_bounds_read`



Beispiel (I)

```
Talentix:heartbleed tobias$ ./heartbleed.pl -H5 -s  
www.wisegeek.com  
...ssl received type=22 ver=0x301 ht=0x2 size=77  
...ssl received type=22 ver=0x301 ht=0xb size=4674  
...ssl received type=22 ver=0x301 ht=0xe size=0  
...send heartbeat#1  
...send heartbeat#2  
...send heartbeat#3  
...send heartbeat#4  
...send heartbeat#5  
...ssl received type=24 ver=301 size=16384  
BAD! got 16384 bytes back instead of 3 (vulnerable)  
02 40 00 41 03 01 53 4a e7 e2 71 7c 38 12 c5
```

Beispiel (II)



Beispiel (III)



```
.....  
2ff0: 00 00 00 00 00 00 00 00 2D 2D 2D 2D 2D 42 45 47 .....-.-.- BEG  
3000: 49 4E 20 52 53 41 20 50 52 49 56 41 54 45 20 4B IN RSA PRIVATE K  
3010: 45 59 2D 2D 2D 2D 0A 4D 49 49 43 58 67 49 42 EY - - - .MIICXgIB  
3020: 41 41 4B 42 67 51 44 55 38 59 36 44 63 66 66 4D AAKBgQDU8Y6DcffM  
3030: 42 4D 36 63 52 56 68 2F 35 61 4F 7A 67 6A 63 44 BM6cRVh/5a0zgjcD  
3040: 68 45 50 68 77 68 44 56 78 34 78 58 70 76 72 62 hEPPhwhDVx4xXpvrb
```



Tomas Rzepka @1njected · 6 Std.

@neelmehta @tqbf @_miw FreeBSD 9.1 #heartbleed
pic.twitter.com/AktnQD3E7w

 Antworten Retweeten Favorisieren

Medium melden

HEARTBLEED MUST
BE THE WORST WEB
SECURITY LAPSE EVER.

WORST SO FAR.
GIVE US TIME.



I MEAN, THIS BUG ISN'T
JUST BROKEN ENCRYPTION.

IT LETS WEBSITE VISITORS
MAKE A SERVER DISPENSE
RANDOM MEMORY CONTENTS.



IT'S NOT JUST KEYS.
IT'S TRAFFIC DATA.
EMAILS. PASSWORDS.
EROTIC FANFICTION.

IS EVERYTHING
COMPROMISED?



WELL, THE ATTACK IS
LIMITED TO DATA STORED
IN COMPUTER MEMORY.

SO PAPER IS SAFE.
AND CLAY TABLETS.

OUR IMAGINATIONS, TOO.

SEE, WE'LL BE FINE.



Private Key bekannt



- Gefahr: Aufgezeichnete Nachrichten nachträglich entschlüsseln
- Gegenmaßnahme: Forward Secrecy

Ohne Forward Secrecy



Ohne Forward Secrecy

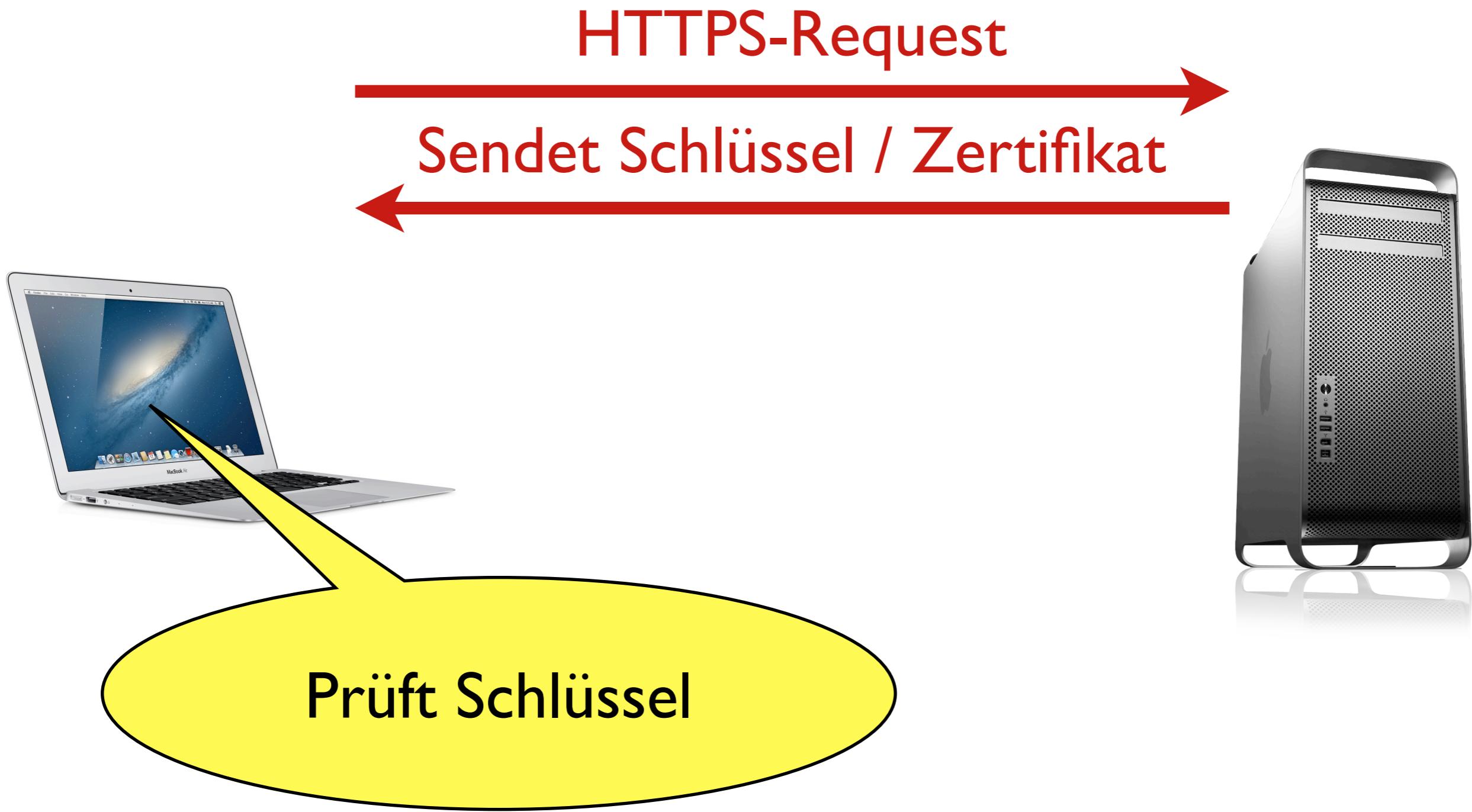
HTTPS-Request



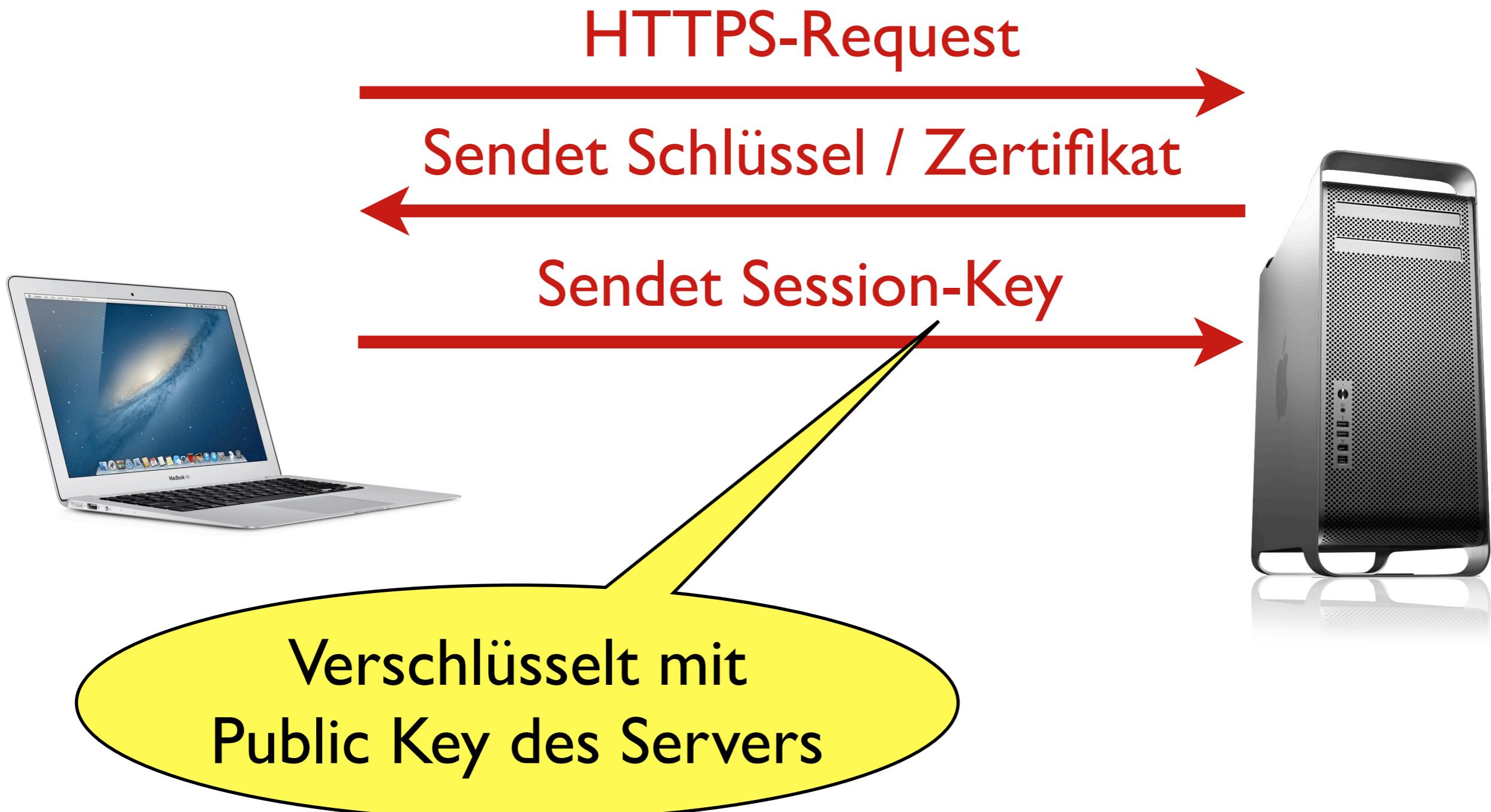
Ohne Forward Secrecy



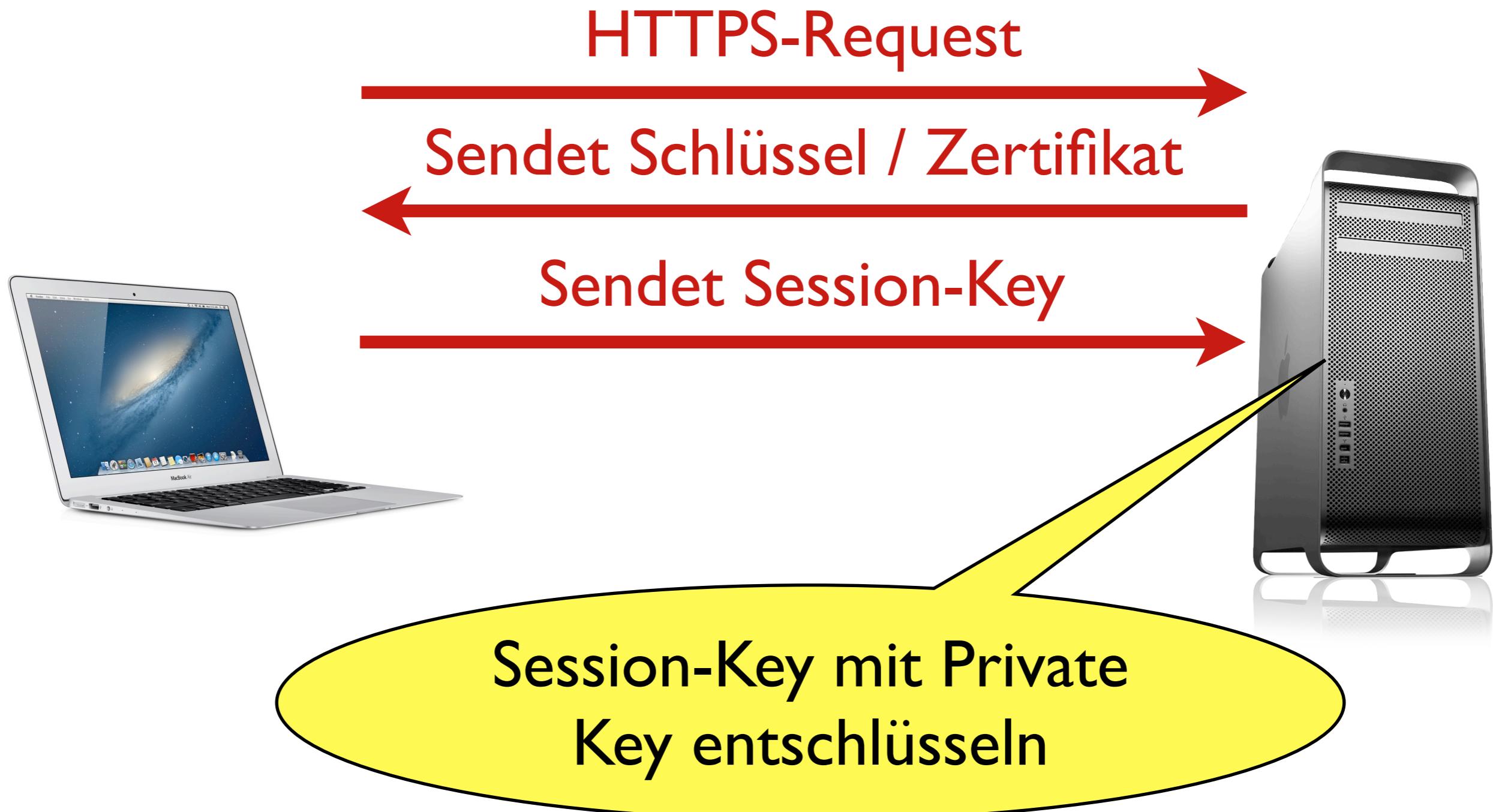
Ohne Forward Secrecy



Ohne Forward Secrecy



Ohne Forward Secrecy



Ohne Forward Secrecy

