

Geheimnisse hinter Schloss und Riegel

Kryptographische Verfahren im

Escape Room

Ulrich Viefhaus

17.10.2026



SEISMOSAURUS

2026-10-15

Geheimnisse hinter Schloss und Riegel

Geheimnisse hinter
Schloss und Riegel
Kryptographische Verfahren im
Escape Room
Ulrich Viefhaus
17.10.2026



Inhalt

Einleitung

Kodierungen

Substitution

Transposition

Steganographie

Mitmachen

Und in echt?

Abschluss

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Einleitung

└─ Inhalt

Inhalt

Einleitung
Kodierungen
Substitution
Transposition

Steganographie
Mitmachen
Und in echt?
Abschluss

- Zeitplan: ca. 15 Minuten gesamt, ca. 1 Minute pro Folie
- Einleitung 2 min, Verfahren 9 min, Mitmachen 2 min, Realität und Fazit 2 min



Einleitung

*Wer bin ich und wie kannst du
entkommen?*



2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Einleitung

└─ Einleitung

Einleitung

*Wer bin ich und wie kannst du
entkommen?*



Über mich

Ulrich Viefhaus aka seism0saurus

- DevOps Engineer und Information Security Officer bei der BRANDAD Solutions GmbH
- Certified Ethical Hacker, Platform Security Engineer und Application Security Engineer (Java)
- Blogger: seism0saurus.de
- Mastodon: @seism0saurus@infosec.exchange
- Coorganisator der Open Security Conference

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Einleitung

└─ Über mich

- Kurz halten
- Überleitung: Beruflich beschäftige ich mich mit Kryptographie und in meiner Freizeit ... auch. Aber es sind andere Anforderungen.

Über mich

Ulrich Viefhaus aka seism0saurus

- DevOps Engineer und Information Security Officer bei der BRANDAD Solutions GmbH
- Certified Ethical Hacker, Platform Security Engineer und Application Security Engineer (Java)
- Blogger: seism0saurus.de
- Mastodon: @seism0saurus@infosec.exchange
- Coorganisator der Open Security Conference



Escape Rooms

ca. 60 Minuten, ein Team, ein Ziel

- Du wirst mit deinem Team in einen Raum eingeschlossen
- Rätsel lösen → Codes finden → Schlösser öffnen
- Zahlenschlösser, Buchstabenschlösser, Vorhängeschlösser, Elektronik
- Manche Rätsel basieren auf historischen Verschlüsselungsverfahren

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Einleitung

└ Escape Rooms

Escape Rooms
ca. 60 Minuten, ein Team, ein Ziel

- Du wirst mit deinem Team in einen Raum eingeschlossen
- Rätsel lösen → Codes finden → Schlösser öffnen
- Zahlenschlösser, Buchstabenschlösser, Vorhängeschlösser, Elektronik
- Manche Rätsel basieren auf historischen Verschlüsselungsverfahren

- Frage ans Publikum: Wer war schon mal in einem Escape Room? Bitte melden
- Das Ziel jedes Rätsels ist in der Regel ein Code für ein Schloss: drei bis fünf Ziffern oder Buchstaben oder Richtungen
- Deshalb passen klassische Verfahren so gut: kurze Nachrichten sind auch ohne Papier und Stift oder Rechner lösbar



Begriffe

Nicht alles, was geheim aussieht, ist Verschlüsselung[6]

- **Kodierung**[1]: Darstellung in einem anderen Zeichensystem, ohne Schlüssel
- **Kryptographie**[2]: Verschlüsselung mit einem geheimen Schlüssel
 - Substitution[3]: Zeichen werden *ersetzt*
 - Transposition[4]: Zeichen werden *vertauscht*
- **Steganographie**[5]: Die Nachricht wird *versteckt*

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Einleitung

└─ Begriffe

Begriffe

Nicht alles, was geheim aussieht, ist Verschlüsselung[6]

- **Kodierung**[1]: Darstellung in einem anderen Zeichensystem, ohne Schlüssel
- **Kryptographie**[2]: Verschlüsselung mit einem geheimen Schlüssel
 - Substitution[3]: Zeichen werden *ersetzt*
 - Transposition[4]: Zeichen werden *vertauscht*
- **Steganographie**[5]: Die Nachricht wird *versteckt*

- Diese drei Kategorien strukturieren den Rest des Vortrags
- Kodierung: Wer das Verfahren kennt, kann die Nachricht lesen. Kein Schlüssel. Z.B. Morsecode
- Kryptographie: Verfahren darf bekannt sein, der Schlüssel nicht (Kerckhoffs' Prinzip', kommt am Ende). Z.B. Caesar
- Steganographie: Niemand soll merken, dass es überhaupt eine Nachricht gibt



Kodierungen

*Kein Schlüssel, nur ein anderes
Alphabet*

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Kodierungen

└─ Kodierungen

Kodierungen

*Kein Schlüssel, nur ein anderes
Alphabet*



Morsecode

Licht, Ton, Muster[7]

- Kurz (.) und lang (-)
- Im Escape Room: blinkende Lampen, Klopfgeräusche, Muster an der Wand
- Code-Tabelle hängt oft versteckt im Raum
- Häufige Zeichen haben kürzere Notation

... .- ..-. . SAFE
-.-. --- -.. . CODE
... --- ... SOS

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Kodierungen

└─ Morsecode

- Erfunden ab 1837 von Samuel Morse
- Ab 1838 verbessert durch seinen Mitarbeiter Alfred Vail
- Heutiger internationaler Code ab 1848 von Friedrich Clemens Gerke
- Typisches Rätsel: Eine Lampe blinkt in Endlosschleife. Schwierigkeit: Wo fängt die Nachricht an?
- Häufig mit Ziffern: Ziffern sind im Morsecode fünf Zeichen lang, z.B. 1 = .----

Morsecode
Licht, Ton, Muster[7]

- Kurz (.) und lang (-)
 - Im Escape Room: blinkende Lampen, Klopfgeräusche, Muster an der Wand
 - Code-Tabelle hängt oft versteckt im Raum
 - Häufige Zeichen haben kürzere Notation
-- ..-. . SAFE
-.-. --- -.. . CODE
... --- ... SOS



Zahlen und Symbole statt Buchstaben

A1Z26, Telefontastatur, Braille und Co.

- **A1Z26:** A=1, B=2, ..., Z=26 8-9-12-6-5 → HILFE
- **Telefontastatur:** 2=ABC, 3=DEF, ... Buchstabenschloss → Zahlenschloss
- **Braille:** Punktmuster zum Ertasten, z.B. im dunklen Raum
- **Winkeralphabet:** Armhaltungen auf Bildern oder Figuren
- **Binär:** Lampen an und aus, 0101 → 5

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Kodierungen

└─ Zahlen und Symbole statt Buchstaben

- A1Z26 ist der Klassiker, um ein Wort in einen Zahlencode zu verwandeln
- Braille und Winkeralphabet sind toll, weil die SpielerInnen erst erkennen müssen, dass es eine Schrift ist
- Kernproblem für SpielerInnen: Erkennen, welche Kodierung vorliegt. Das Entschlüsseln selbst ist dann einfach

Zahlen und Symbole statt Buchstaben
A1Z26, Telefontastatur, Braille und Co.

- **A1Z26:** A=1, B=2, ..., Z=26 8-9-12-6-5 → HILFE
- **Telefontastatur:** 2=ABC, 3=DEF, ... Buchstabenschloss → Zahlenschloss
- **Braille:** Punktmuster zum Ertasten, z.B. im dunklen Raum
- **Winkeralphabet:** Armhaltungen auf Bildern oder Figuren
- **Binär:** Lampen an und aus, 0101 → 5



Substitution

Jeder Buchstabe bekommt einen Stellvertreter

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Substitution

└ Substitution

Substitution

Jeder Buchstabe bekommt einen Stellvertreter



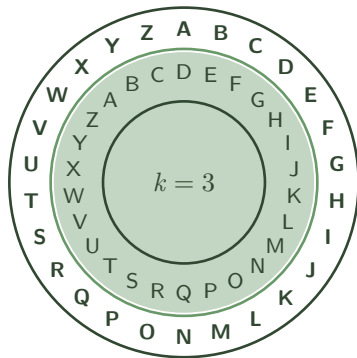
Caesar-Verschiebung

Der Klassiker mit Chiffrierscheibe[8]

- Jeder Buchstabe wird um k Stellen verschoben
- Schlüssel: $k \in \{1, \dots, 25\}$
- Im Escape Room: drehbare Scheibe, k irgendwo im Raum versteckt

$k = 3$:

DER SCHLUESSEL LIEGT IM KAMIN
GHU VFKOXHVVHO OLHJW LP NDPLQ



2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Substitution

└ Caesar-Verschiebung

Caesar-Verschiebung

Der Klassiker mit Chiffrierscheibe[8]

- Jeder Buchstabe wird um k Stellen verschoben
- Schlüssel: $k \in \{1, \dots, 25\}$
- Im Escape Room: drehbare Scheibe, k irgendwo im Raum versteckt

$k = 3$:
DER SCHLUESSEL LIEGT IM KAMIN
GHU VFKOXHVVHO OLHJW LP NDPLQ



- Laut Sueton nutzte Julius Caesar die Verschiebung um drei Stellen für militärische Nachrichten
- ROT13 ist der Spezialfall $k = 13$: Ver- und Entschlüsseln sind identisch
- Nur 25 mögliche Schlüssel: Mit Brute Force in wenigen Minuten auch per Hand knackbar
- Escape Room Variante: Zwei Scheiben aus Pappe, die Zahl k steht z.B. auf einem Kalenderblatt



Atbash

Das gespiegelte Alphabet[9]

ABCDEFGHIJKLMNOPQRSTUVWXYZ
↕
ZYXWVUTSRQPONMLKJIHGFEDCBA

- Kein Schlüssel nötig: $A \leftrightarrow Z$, $B \leftrightarrow Y$, ...
- TRESOR $\rightarrow$ GIVHLI
- Beliebte als Einstiegsrätsel, Hinweis z.B. ein Spiegel im Raum

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Substitution

└ Atbash

Atbash

Das gespiegelte Alphabet[9]

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

ZYXWVUTSRQPONMLKJIHGFEDCBA

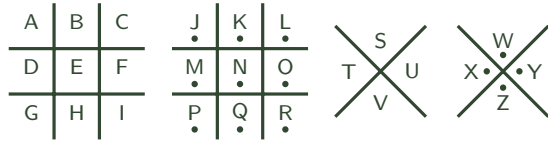
- Kein Schlüssel nötig: $A \leftrightarrow Z$, $B \leftrightarrow Y$, ...
- TRESOR $\rightarrow$ GIVHLI
- Beliebte als Einstiegsrätsel, Hinweis z.B. ein Spiegel im Raum

- Ursprünglich für das hebräische Alphabet, taucht bereits im Buch Jeremia auf
- Streng genommen eher eine Kodierung, da es keinen Schlüssel gibt
- Wie ROT13: Ver- und Entschlüsseln ist dieselbe Operation



Freimaurer-Alphabet

Auch bekannt als Pigpen-Chiffre[10]



V J □ □ = SAFE

- Buchstabe → Form seiner Umrandung
- Sieht aus wie eine fremde Schrift
- Perfekt für Wandmalereien, Truhen, alte Bücher

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Substitution

└ Freimaurer-Alphabet

Freimaurer-Alphabet

Auch bekannt als Pigpen-Chiffre[10]



- Buchstabe → Form seiner Umrandung
- Sieht aus wie eine fremde Schrift
- Perfekt für Wandmalereien, Truhen, alte Bücher

- Im 18. Jahrhundert von Freimaurern genutzt, findet sich z.B. auf Grabsteinen
- Der Schlüssel ist die Anordnung der Buchstaben im Gitter. Es gibt viele Varianten
- Durch den mystischen Look ideal für Themenräume: Piraten, Templer, Geheimbund
- Mathematisch nur eine einfache monoalphabetische Substitution



Polybios-Quadrat

Buchstaben als Koordinaten[11]

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- Jeder Buchstabe wird zu Zeile und Spalte
- 23 24 31 21 15 → HILFE
- **Klopfcode**: zweimal klopfen, Pause, dreimal klopfen = H
- Im Escape Room: Klopfgeräusche aus der Nachbarzelle

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Substitution

└ Polybios-Quadrat

Polybios-Quadrat
Buchstaben als Koordinaten[11]

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- Jeder Buchstabe wird zu Zeile und Spalte
- 23 24 31 21 15 → HILFE
- **Klopfcode**: zweimal klopfen, Pause, dreimal klopfen = H
- Im Escape Room: Klopfgeräusche aus der Nachbarzelle

- Beschrieben vom griechischen Geschichtsschreiber Polybios ca. 200 v. Chr., ursprünglich für Fackelsignale
- 25 Felder, deshalb teilen sich I und J ein Feld
- Klopfcode wurde u.a. von US-Kriegsgefangenen in Vietnam genutzt (dort mit C/K zusammengelegt)
- Variante mit Schlüsselwort: Alphabet beginnt mit einem Codewort, dann ist es wirklich verschlüsselt



Vigenère-Chiffre

Viele Caesars auf einmal[12]

- Ein Schlüsselwort bestimmt die Verschiebung für jeden Buchstaben
- $A = 0, B = 1, \dots, Z = 25$
- Galt 300 Jahre lang als *le chiffre indéchiffrable* und hatte eine große Bedeutung in der Politik

Klartext:	ZAHLENSCHLOSS
Schlüssel:	RAUMRAUMRAUMR
Geheimtext:	QABXVNMOYLIEJ

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Substitution

└ Vigenère-Chiffre

- Benannt nach Blaise de Vigenère, 16. Jahrhundert
- Polyalphabetisch: Derselbe Klartextbuchstabe wird unterschiedlich verschlüsselt. Hier wird S einmal zu M, einmal zu E und einmal zu J
- Häufigkeitsanalyse funktioniert nicht direkt. Erst Babbage und Kasiski haben sie im 19. Jahrhundert gebrochen
- Im Escape Room: Das Vigenère-Quadrat hängt an der Wand, das Schlüsselwort ist das eigentliche Rätsel
- Für Spieler die anspruchsvollste Chiffre, wird oft erst in schweren Räumen eingesetzt

Vigenère-Chiffre

Viele Caesars auf einmal[12]

- Ein Schlüsselwort bestimmt die Verschiebung für jeden Buchstaben
- $A = 0, B = 1, \dots, Z = 25$
- Galt 300 Jahre lang als *le chiffre indéchiffrable* und hatte eine große Bedeutung in der Politik

Klartext:	ZAHLENSCHLOSS
Schlüssel:	RAUMRAUMRAUMR
Geheimtext:	QABXVNMOYLIEJ



Transposition

*Alle Buchstaben sind da, nur
nicht an ihrem Platz*

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Transposition

└ Transposition

Transposition

*Alle Buchstaben sind da, nur
nicht an ihrem Platz*



Skytale und Gartenzaun

Umsortieren statt Ersetzen[4]

Skytale[13]

- Lederband um einen Stab gewickelt
- Schlüssel: der Durchmesser des Stabs

A	U	S	G
A	N	G	H
I	N	T	E
R	D	E	M
B	I	L	D

AAIRB UNNDI SGTEL GHEMD

Gartenzaun[4]

- Zickzack über mehrere Zeilen schreiben
- Schlüssel: die Anzahl der Zeilen

A S A G

 U G N

ASAG UGN → AUSGANG

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Transposition

└ Skytale und Gartenzaun

Skytale und Gartenzaun
Umsortieren statt Ersetzen[4]

Skytale[13]

- Lederband um einen Stab gewickelt
- Schlüssel: der Durchmesser des Stabs

A	U	S	G
A	N	G	H
I	N	T	E
R	D	E	M
B	I	L	D

AAIRB UNNDI SGTEL GHEMD

Gartenzaun[4]

- Zickzack über mehrere Zeilen schreiben
- Schlüssel: die Anzahl der Zeilen

A S A G

 U G N

ASAG UGN → AUSGANG

- Skytale: Spartaner, ca. 5. Jahrhundert v. Chr. Zeilenweise auf den unwickelten Stab schreiben, abgewickelt steht der Text spaltenweise auf dem Band
- Hier: AUSGANG HINTER DEM BILD
- Im Escape Room: Ein Papierstreifen mit wirren Buchstaben und mehrere Rundhölzer, nur eines hat den richtigen Durchmesser
- Gartenzaun (Rail Fence): Leicht zu erkennen, weil die Buchstabenhäufigkeit unverändert bleibt
- Merkmal aller Transpositionen: Häufigkeiten wie normaler deutscher Text, aber unlesbar



Steganographie

*Die beste Nachricht ist die, die
niemand findet*

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Steganographie

└─ Steganographie

Steganographie

*Die beste Nachricht ist die, die
niemand findet*



Schablonen und Akrostichon

Das Geheimnis steckt im Offensichtlichen[5]

- **Cardan-Gitter**[14]: Schablone mit Löchern auf einen harmlosen Text legen
- **Akrostichon**[15]: Die Anfangsbuchstaben jeder Zeile eines Gedichts
- **Unsichtbare Tinte**: nur unter UV-Licht oder Wärme sichtbar

M	Z	E	R	K
A	L	O	H	I
T	E	N	B	L
S	U	A	H	E
R	W	L	D	E

Schablone ergibt: **ZAHL**

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Steganographie

└ Schablonen und Akrostichon

- Steganographie: griechisch für verdecktes Schreiben
- Cardan-Gitter nach Girolamo Cardano, 16. Jahrhundert
- Im Escape Room: Ein Brief liegt offen herum, die Schablone liegt in einer anderen Schublade
- UV-Taschenlampen sind fester Bestandteil fast jedes Escape Rooms
- Ohne die Schablone bzw. das Licht ist der Hinweis wertlos. Es ist also eine Art Schlüssel

Schablonen und Akrostichon
Das Geheimnis steckt im Offensichtlichen[5]

- **Cardan-Gitter**[14]: Schablone mit Löchern auf einen harmlosen Text legen
- **Akrostichon**[15]: Die Anfangsbuchstaben jeder Zeile eines Gedichts
- **Unsichtbare Tinte**: nur unter UV-Licht oder Wärme sichtbar



Schablone ergibt: **ZAHL**



Buch-Chiffre

Das Buch ist der Schlüssel[16]

- Zahlentripel: **Seite-Zeile-Wort**
- Beispiel: 12-3-5 47-1-2 3-10-1
- Ohne das richtige Buch (und die richtige Auflage!) unlösbar
- Im Escape Room: Das Bücherregal ist plötzlich kein Deko mehr

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Steganographie

└ Buch-Chiffre

Buch-Chiffre
Das Buch ist der Schlüssel[16]

- Zahlentripel: **Seite-Zeile-Wort**
- Beispiel: 12-3-5 47-1-2 3-10-1
- Ohne das richtige Buch (und die richtige Auflage!) unlösbar
- Im Escape Room: Das Bücherregal ist plötzlich kein Deko mehr

- Auch Ottendorf-Chiffre oder Arnold-Verschlüsselung genannt[17]
- Berühmtes Beispiel: Die Beale-Chiffren, ein angeblicher Schatz, verschlüsselt mit der Unabhängigkeitserklärung der USA
- Tipp für Spieler: Wenn im Raum viele Zahlen in Dreiergruppen auftauchen, sofort das Bücherregal checken
- Varianten: Nur der erste Buchstabe des Worts zählt, oder Seite und Buchstabe



Jetzt bist du dran!

Knack den Code

KB OHZA LZ NLZJOHMMMA

- Tipp 1: Es ist eine Caesar-Verschiebung

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Mitmachen

└─ Jetzt bist du dran!

Jetzt bist du dran!
Knack den Code

KB OHZA LZ NLZJOHMMMA

- Tipp 1: Es ist eine Caesar-Verschiebung



Jetzt bist du dran!

Knack den Code

KB OHZA LZ NLZJOHMMMA

- Tipp 1: Es ist eine Caesar-Verschiebung
- Tipp 2: Das erste Wort spricht dich direkt an

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Mitmachen

└─ Jetzt bist du dran!

Jetzt bist du dran!
Knack den Code

KB OHZA LZ NLZJOHMMMA

- Tipp 1: Es ist eine Caesar-Verschiebung
- Tipp 2: Das erste Wort spricht dich direkt an



Jetzt bist du dran!

Knack den Code

KB OHZA LZ NLZJOHMMA

- Tipp 1: Es ist eine Caesar-Verschiebung
- Tipp 2: Das erste Wort spricht dich direkt an
- Lösung: $K \rightarrow D$, also $k = 7$

DU HAST ES GESCHAFFT

2026-10-15

Geheimnisse hinter Schloss und Riegel

└─ Mitmachen

└─ Jetzt bist du dran!

Jetzt bist du dran!
Knack den Code

KB OHZA LZ NLZJOHMMA

- Tipp 1: Es ist eine Caesar-Verschiebung
- Tipp 2: Das erste Wort spricht dich direkt an
- Lösung: $K \rightarrow D$, also $k = 7$

DU HAST ES GESCHAFFT

- Ca. 60 bis 90 Sekunden Zeit geben, dann Tipp 2 einblenden
- Lösungsweg: Ein Wort mit zwei Buchstaben, das dich anspricht: DU. K wird zu D, das sind 7 Stellen zurück
- Alternative: Brute Force über alle 25 Schlüssel, oder Häufigkeitsanalyse. Bei so kurzen Texten unzuverlässig
- Genau so funktioniert ein Known-Plaintext-Angriff: Ein erratenes Stück Klartext verrät den Schlüssel



Und in echt?

*Warum du deine Daten nicht
mit Caesar schützen solltest*

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Und in echt?

└ Und in echt?

Und in echt?

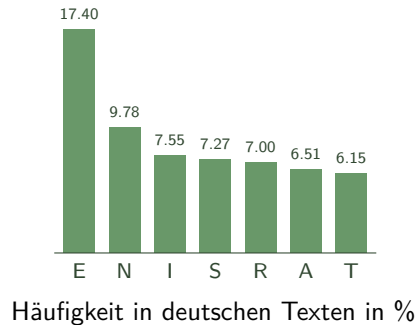
*Warum du deine Daten nicht
mit Caesar schützen solltest*



Häufigkeitsanalyse

Das E verrät alles[19]

- Jede Sprache hat typische Buchstabenhäufigkeiten
- Monoalphabetische Substitution behält sie bei
- Häufigstes Zeichen im Geheimtext ist vermutlich E
- Bereits im 9. Jahrhundert von al-Kindī[18] beschrieben



2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Und in echt?

└ Häufigkeitsanalyse

Häufigkeitsanalyse

Das E verrät alles[19]

- Jede Sprache hat typische Buchstabenhäufigkeiten
- Monoalphabetische Substitution behält sie bei
- Häufigstes Zeichen im Geheimtext ist vermutlich E
- Bereits im 9. Jahrhundert von al-Kindī[18] beschrieben



- Deshalb sind Caesar, Atbash, Freimaurer und Co. bei längeren Texten trivial zu knacken
- Gilt auch für 26! mögliche Schlüssel bei beliebiger Substitution. Der Schlüsselraum allein schützt nicht
- Vigenère verschleiert die Häufigkeiten, ist aber über die Schlüssellänge angreifbar (Kasiski-Test[20])



Von der Chiffrierscheibe zu AES

Was wir daraus lernen[21]

- **Kerckhoffs' Prinzip:** Die Sicherheit darf nur vom Schlüssel abhängen, nicht von der Geheimhaltung des Verfahrens
- **Schlüsselraum:**
 - Caesar: 25
 - Beliebige Substitution: $26! \approx 4 \cdot 10^{26}$
 - AES-128: $2^{128} \approx 3,4 \cdot 10^{38}$
- Moderne Verfahren halten auch Angriffen mit bekanntem Klartext stand
- Don't roll your own crypto!

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Und in echt?

└ Von der Chiffrierscheibe zu AES

- Auguste Kerckhoffs, 1883: Das Verfahren fällt dem Feind früher oder später in die Hände
- Escape Rooms setzen genau auf das Gegenteil: Security by Obscurity. Das Rätsel ist, das Verfahren zu erkennen
- Großer Schlüsselraum ist notwendig, aber nicht hinreichend. Siehe Häufigkeitsanalyse
- Beim Mitmach-Rätsel war ein erratenes Wort genug. Moderne Verfahren wie AES sind gegen solche Known-Plaintext-Angriffe resistent
- Brücke zur Enigma: polyalphabetisch wie Vigenère, aber mechanisiert. Gebrochen u.a. durch erratene Klartextstücke (Crips) wie Wetterbericht
- Fazit für die Praxis: Etablierte, geprüfte Bibliotheken verwenden, nichts selbst erfinden

Von der Chiffrierscheibe zu AES
Was wir daraus lernen[21]

- **Kerckhoffs' Prinzip:** Die Sicherheit darf nur vom Schlüssel abhängen, nicht von der Geheimhaltung des Verfahrens
- **Schlüsselraum:**
 - Caesar: 25
 - Beliebige Substitution: $26! \approx 4 \cdot 10^{26}$
 - AES-128: $2^{128} \approx 3,4 \cdot 10^{38}$
- Moderne Verfahren halten auch Angriffen mit bekanntem Klartext stand
- Don't roll your own crypto!



Tipps für deinen nächsten Escape Room

Vom Geheimtext zum Code

- Zähle die Stellen am Schloss: Wie lang muss die Lösung sein?
- Achte auf Alphabete, Zahlenreihen und Symbole im Raum
- Nur Punkte und Striche? Morse! Dreiergruppen? Buch-Chiffre!
- Fremde Schrift aus Ecken und Punkten? Freimaurer!
- Taschenlampe mit UV? Alles ableuchten!
- Rede mit deinem Team: Der Schlüssel liegt oft in einem anderen Rätsel

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Und in echt?

└ Tipps für deinen nächsten Escape Room

- Zusammenfassung des Vortrags als praktische Checkliste
- Escape Rooms sind ein spielerischer Einstieg in Kryptographie und Informationssicherheit
- Überleitung zum Dank und zu Fragen

Tipps für deinen nächsten Escape Room
Vom Geheimtext zum Code

- Zähle die Stellen am Schloss: Wie lang muss die Lösung sein?
- Achte auf Alphabete, Zahlenreihen und Symbole im Raum
- Nur Punkte und Striche? Morse! Dreiergruppen? Buch-Chiffre!
- Fremde Schrift aus Ecken und Punkten? Freimaurer!
- Taschenlampe mit UV? Alles ableuchten!
- Rede mit deinem Team: Der Schlüssel liegt oft in einem anderen Rätsel



Vielen Dank!

Materialien verfügbar unter
<https://seism0saurus.de/posts/escape-room-kryptographie/>

Materialien und Aufzeichnung des Nürnberg Digital Workshop
"Alles auf ROT - wie du Verschlüsselung anwendest ... und knackst!"
verfügbar unter
<https://seism0saurus.de/posts/session-nue-digital-alles-auf-rot/>

2026-10-15

Geheimnisse hinter Schloss und Riegel
└─ Abschluss

Vielen Dank!

Materialien verfügbar unter
<https://seism0saurus.de/posts/escape-room-kryptographie/>

Materialien und Aufzeichnung des Nürnberg Digital Workshop
"Alles auf ROT - wie du Verschlüsselung anwendest ... und knackst!"
verfügbar unter
<https://seism0saurus.de/posts/session-nue-digital-alles-auf-rot/>



Quellen I

- [1] *Zeichenkodierung*. URL:
<https://de.wikipedia.org/wiki/Zeichenkodierung> (besucht am 12.10.2026).
- [2] *Kryptographie*. URL: <https://de.wikipedia.org/wiki/Kryptographie>
(besucht am 12.10.2026).
- [3] *Substitution*. URL:
[https://de.wikipedia.org/wiki/Substitution_\(Kryptographie\)](https://de.wikipedia.org/wiki/Substitution_(Kryptographie))
(besucht am 12.10.2026).
- [4] *Transposition*. URL:
[https://de.wikipedia.org/wiki/Transposition_\(Kryptographie\)](https://de.wikipedia.org/wiki/Transposition_(Kryptographie))
(besucht am 12.10.2026).

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Abschluss

└ Quellen

Quellen I

- [1] *Zeichenkodierung*. URL:
<https://de.wikipedia.org/wiki/Zeichenkodierung> (besucht am 12.10.2026).
- [2] *Kryptographie*. URL: <https://de.wikipedia.org/wiki/Kryptographie>
(besucht am 12.10.2026).
- [3] *Substitution*. URL:
[https://de.wikipedia.org/wiki/Substitution_\(Kryptographie\)](https://de.wikipedia.org/wiki/Substitution_(Kryptographie))
(besucht am 12.10.2026).
- [4] *Transposition*. URL:
[https://de.wikipedia.org/wiki/Transposition_\(Kryptographie\)](https://de.wikipedia.org/wiki/Transposition_(Kryptographie))
(besucht am 12.10.2026).



Quellen II

- [5] *Steganographie*. URL: <https://de.wikipedia.org/wiki/Steganographie> (besucht am 12.10.2026).
- [6] Albrecht Beutelspacher. *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. 10. Aufl. Springer Spektrum, 2015.
- [7] *Morsecode*. URL: <https://de.wikipedia.org/wiki/Morsecode> (besucht am 12.10.2026).
- [8] *Caesar-Verschlüsselung*. URL: <https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsslung> (besucht am 12.10.2026).

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Abschluss

└ Quellen

Quellen II

- [5] *Steganographie*. URL: <https://de.wikipedia.org/wiki/Steganographie> (besucht am 12.10.2026).
- [6] Albrecht Beutelspacher. *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. 10. Aufl. Springer Spektrum, 2015.
- [7] *Morsecode*. URL: <https://de.wikipedia.org/wiki/Morsecode> (besucht am 12.10.2026).
- [8] *Caesar-Verschlüsselung*. URL: <https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsslung> (besucht am 12.10.2026).



Quellen III

- [9] *Atbasch*. URL: <https://de.wikipedia.org/wiki/Atbasch> (besucht am 12. 10. 2026).
- [10] *Freimaurer-Alphabet*. URL: <https://de.wikipedia.org/wiki/Freimaurer-Alphabet> (besucht am 12. 10. 2026).
- [11] *Polybios-Chiffre*. URL: <https://de.wikipedia.org/wiki/Polybios-Chiffre> (besucht am 12. 10. 2026).
- [12] *Vigenère-Chiffre*. URL: <https://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre> (besucht am 12. 10. 2026).

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Abschluss

└ Quellen

Quellen III

- [9] *Atbasch*. URL: <https://de.wikipedia.org/wiki/Atbasch> (besucht am 12. 10. 2026).
- [10] *Freimaurer-Alphabet*. URL: <https://de.wikipedia.org/wiki/Freimaurer-Alphabet> (besucht am 12. 10. 2026).
- [11] *Polybios-Chiffre*. URL: <https://de.wikipedia.org/wiki/Polybios-Chiffre> (besucht am 12. 10. 2026).
- [12] *Vigenère-Chiffre*. URL: <https://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre> (besucht am 12. 10. 2026).



Quellen IV

- [13] *Skytale*. URL: <https://de.wikipedia.org/wiki/Skytale> (besucht am 12. 10. 2026).
- [14] *Cardan-Gitter*. URL: <https://de.wikipedia.org/wiki/Cardan-Gitter> (besucht am 15. 10. 2026).
- [15] *Akrostichon*. URL: <https://de.wikipedia.org/wiki/Akrostichon> (besucht am 15. 10. 2026).
- [16] Simon Singh. *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Hanser, 2000.

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Abschluss

└ Quellen

Quellen IV

- [13] *Skytale*. URL: <https://de.wikipedia.org/wiki/Skytale> (besucht am 12. 10. 2026).
- [14] *Cardan-Gitter*. URL: <https://de.wikipedia.org/wiki/Cardan-Gitter> (besucht am 15. 10. 2026).
- [15] *Akrostichon*. URL: <https://de.wikipedia.org/wiki/Akrostichon> (besucht am 15. 10. 2026).
- [16] Simon Singh. *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Hanser, 2000.



Quellen V

- [17] *Buch-Verschlüsselung*. URL:
<https://de.wikipedia.org/wiki/Buch-Verschl%C3%BCsslung> (besucht
am 15.10.2026).
- [18] *al-Kindī*. URL: <https://de.wikipedia.org/wiki/Al-Kind%C4%AB> (besucht
am 15.10.2026).
- [19] *Buchstabenhäufigkeit*. URL:
<https://de.wikipedia.org/wiki/Buchstabenh%C3%A4ufigkeit> (besucht
am 12.10.2026).
- [20] *Kasiski-Test*. URL: <https://de.wikipedia.org/wiki/Kasiski-Test>
(besucht am 12.10.2026).

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Abschluss

└ Quellen

Quellen V

- [17] *Buch-Verschlüsselung*. URL:
<https://de.wikipedia.org/wiki/Buch-Verschl%C3%BCsslung> (besucht
am 15.10.2026).
- [18] *al-Kindī*. URL: <https://de.wikipedia.org/wiki/Al-Kind%C4%AB> (besucht
am 15.10.2026).
- [19] *Buchstabenhäufigkeit*. URL:
<https://de.wikipedia.org/wiki/Buchstabenh%C3%A4ufigkeit> (besucht
am 12.10.2026).
- [20] *Kasiski-Test*. URL: <https://de.wikipedia.org/wiki/Kasiski-Test>
(besucht am 12.10.2026).



Quellen VI

[21] *Kerckhoffs' Prinzip*. URL:
https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip
(besucht am 12.10.2026).

2026-10-15

Geheimnisse hinter Schloss und Riegel

└ Abschluss

└ Quellen

Quellen VI

[21] *Kerckhoffs' Prinzip*. URL:
https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip
(besucht am 12.10.2026).