Secrets Under Lock and Key

Cryptographic Methods in the Escape Room

Ulrich Viefhaus

October 17, 2026



Secrets Under Lock and Key
Cryptographic Methods in the Escape Room
Ulrich Viefhaus
October 17, 2026



Contents

Introduction
Encodings
Substitution
Transposition
Steganography
Your Turn
And in Real Life?
Wrap-up

Contents

Introduction
Encodings
Substitution
Transposition
Steganography
Your Turn
And in Real Life?
Wrap-up

- Schedule: approx. 15 minutes total, approx. 1 minute per slide
- Introduction 2 min, methods 9 min, hands-on 2 min, reality and conclusion 2 min



Introduction

Who am I and how can you escape?

Introduction

Who am I and how can you escape?



About me

Ulrich Viefhaus aka seism0saurus

- DevOps Engineer and Information Security Officer at BRANDAD Solutions GmbH
- Certified Ethical Hacker, Platform Security Engineer and Application Security Engineer (Java)
- Blogger: seism0saurus.de
- Mastodon: @seism0saurus@infosec.exchange
- Co-organizer of the Open Security Conference

About me

Ulrich Viefhaus aka seism0saurus
- DevOps Engineer and Information Security Officer at BRANDAD Solutions GmbH
- Certified Ethical Hacker, Platform Security Engineer and Application Security Engineer (Java)
- Blogger: seism0saurus.de
- Mastodon: @seism0saurus@infosec.exchange
- Co-organizer of the Open Security Conference

- Keep it short
- Transition: Professionally, I work with cryptography, and in my spare time ... too. But the requirements are different.



Escape Rooms

approx. 60 minutes, one team, one goal

- You and your team get locked in a room
- Solve puzzles → find codes → open locks
- Number locks, letter locks, padlocks, electronics
- Some puzzles are based on historical ciphers

Escape Rooms
approx. 60 minutes, one team, one goal
- You and your team get locked in a room
- Solve puzzles → find codes → open locks
- Number locks, letter locks, padlocks, electronics
- Some puzzles are based on historical ciphers

- Question to the audience: Who has been to an escape room before? Please raise your hand
- The goal of each puzzle is usually a code for a lock: three to five digits, letters or directions
- That's why classical methods fit so well: short messages can be solved without pen and paper or a computer



Terminology

Not everything that looks secret is encryption[6]

- **Encoding**[1]: representation in a different symbol system, without a key
- **Cryptography**[2]: encryption with a secret key
  - Substitution[3]: characters are *replaced*
  - Transposition[4]: characters are *rearranged*
- **Steganography**[5]: the message is hidden

Terminology
Not everything that looks secret is encryption[6]
• Encoding[1]: representation in a different symbol system, without a key
• Cryptography[2]: encryption with a secret key
— Substitution[3]: characters are replaced
— Transposition[4]: characters are rearranged
• Steganography[5]: the message is hidden

- These three categories structure the rest of the talk
- Encoding: Anyone who knows the method can read the message. No key. E.g. Morse code
- Cryptography: The method may be public, the key may not (Kerckhoffs's principle, comes at the end). E.g. Caesar
- Steganography: Nobody should even notice that there is a message



Encodings

No key, just a different alphabet

Encodings

No key, just a different alphabet



Morse Code

Light, sound, patterns[7]

- Short (`.`) and long (`-`)
- In the escape room: blinking lamps, knocking sounds, patterns on the wall
- The code table is often hidden somewhere in the room
- Frequent characters have shorter codes

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

Morse Code
Light, sound, patterns[7]
• Short (.) and long (-)
• In the escape room: blinking lamps, knocking sounds, patterns on the wall
• The code table is often hidden somewhere in the room
• Frequent characters have shorter codes
... .- ..-. . SAFE
-.-. --- -.. . CODE
... --- ... SOS

- Invented from 1837 by Samuel Morse
- Improved from 1838 by his assistant Alfred Vail
- Today's international code dates from 1848, by Friedrich Clemens Gerke
- Typical puzzle: A lamp blinks in an endless loop. Difficulty: Where does the message start?
- Often with digits: digits are five symbols long in Morse code, e.g. 1 = `.----`



Numbers and Symbols Instead of Letters

A1Z26, phone keypad, Braille and co.

- **A1Z26**: A=1, B=2, ..., Z=26 `8-5-12-16` → HELP
- **Phone keypad**: 2=ABC, 3=DEF, ... letter lock → number lock
- **Braille**: dot patterns to feel, e.g. in a dark room
- **Flag semaphore**: arm positions on pictures or figures
- **Binary**: lamps on and off, `0101` → 5

Numbers and Symbols Instead of Letters
A1Z26, phone keypad, Braille and co.
• A1Z26: A=1, B=2, ..., Z=26 8-5-12-16 → HELP
• Phone keypad: 2=ABC, 3=DEF, ... letter lock → number lock
• Braille: dot patterns to feel, e.g. in a dark room
• Flag semaphore: arm positions on pictures or figures
• Binary: lamps on and off, 0101 → 5

- A1Z26 is the classic way to turn a word into a number code
- Braille and semaphore are great because players first have to realize that it is a script at all
- Core problem for players: recognizing which encoding is used. Decoding itself is then easy



Substitution

Every letter gets a stand-in

Substitution
Every letter gets a stand-in



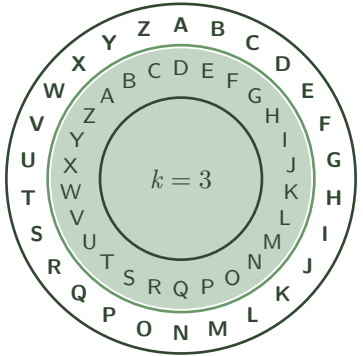
Caesar Shift

The classic with a cipher disk[8]

- Every letter is shifted by k positions
- Key: $k \in \{1, \ldots, 25\}$
- In the escape room: rotating disk, k hidden somewhere in the room

$k = 3$:

```
THE KEY IS IN THE FIREPLACE
WKH NHB LV LQ WKH ILUHSODFH
```



Caesar Shift
The classic with a cipher disk[8]
Every letter is shifted by k positions
Key: $k \in \{1, \ldots, 25\}$
In the escape room: rotating disk, k hidden somewhere in the room
$k = 3$:
THE KEY IS IN THE FIREPLACE
WKH NHB LV LQ WKH ILUHSODFH



- According to Suetonius, Julius Caesar used a shift of three for military messages
- ROT13 is the special case $k = 13$: encryption and decryption are identical
- Only 25 possible keys: brute force cracks it in a few minutes, even by hand
- Escape room variant: two cardboard disks, the number k is e.g. on a calendar page



Atbash

The mirrored alphabet[9]

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
↕
ZYXWVUTSRQPONMLKJIHGFEDCBA
```

- No key needed: A ↔ Z, B ↔ Y, …
- `VAULT` → `EZFOG`
- Popular as an entry-level puzzle, hint e.g. a mirror in the room

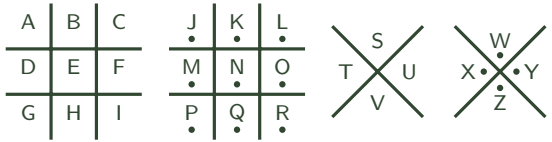
Atbash
The mirrored alphabet[9]
ABCDEFGHIJKLMNOPQRSTUVWXYZ
↕
ZYXWVUTSRQPONMLKJIHGFEDCBA
- No key needed: A ↔ Z, B ↔ Y, …
- VAULT → EZFOG
- Popular as an entry-level puzzle, hint e.g. a mirror in the room

- Originally for the Hebrew alphabet, already appears in the Book of Jeremiah
- Strictly speaking more of an encoding, since there is no key
- Like ROT13: encryption and decryption are the same operation



Pigpen Cipher

Also known as the Freemason's cipher[10]



- Letter → shape of its enclosure
- Looks like a foreign script
- Perfect for murals, chests, old books



- Used by Freemasons in the 18th century, found e.g. on gravestones
- The key is the arrangement of the letters in the grid. There are many variants
- Its mystical look makes it ideal for themed rooms: pirates, Templars, secret societies
- Mathematically just a simple monoalphabetic substitution



Polybius Square

Letters as coordinates[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

- Every letter becomes row and column
- 23 15 31 35 → HELP
- **Tap code**: knock twice, pause, knock three times = H
- In the escape room: knocking from the neighboring cell

Polybius Square
Letters as coordinates[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

- Every letter becomes row and column
- 23 15 31 35 → HELP
- **Tap code**: knock twice, pause, knock three times = H
- In the escape room: knocking from the neighboring cell

- Described by the Greek historian Polybius around 200 BC, originally for torch signals
- 25 cells, so I and J share one cell
- The tap code was used e.g. by US prisoners of war in Vietnam (there with C/K merged)
- Variant with a keyword: the alphabet starts with a code word, then it is actually encrypted



Vigenère Cipher

Many Caesars at once[12]

- A keyword determines the shift for each letter
- A = 0, B = 1, ..., Z = 25
- Considered *le chiffre indéchiffrable* for 300 years and was of great importance in politics

Plaintext:	`COMBINATIONLOCK`
Key:	`ROOMROOMROOMROO`
Ciphertext:	`TCANZBOFZCBXFQY`

Vigenère Cipher
Many Caesars at once[12]
- A keyword determines the shift for each letter
- A = 0, B = 1, ..., Z = 25
- Considered *le chiffre indéchiffrable* for 300 years and was of great importance in politics

Plaintext: COMBINATIONLOCK
Key: ROOMROOMROOMROO
Ciphertext: TCANZBOFZCBXFQY

- Named after Blaise de Vigenère, 16th century
- Polyalphabetic: the same plaintext letter is encrypted differently. Here O becomes C twice and F once, C becomes T and Q
- Frequency analysis does not work directly. Only Babbage and Kasiski broke it in the 19th century
- In the escape room: the Vigenère square hangs on the wall, the keyword is the actual puzzle
- The most demanding cipher for players, often only used in hard rooms



Transposition

All letters are there, just not in their place

└Transposition

Transposition

All letters are there, just not in their place



Scytale and Rail Fence

Rearranging instead of replacing[4]

Scytale[13]

- Leather strip wound around a rod
- Key: the diameter of the rod

E	X	I	T
B	E	H	I
N	D	T	H
E	P	I	C
T	U	R	E

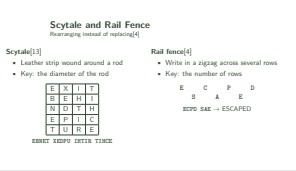
`EBNET XEDPU IHTIR TIHCE`

Rail fence[4]

- Write in a zigzag across several rows
- Key: the number of rows

```
E   C   P   D
 S   A   E
```

`ECPD SAE` → ESCAPED



- Scytale: Spartans, approx. 5th century BC. Write row by row on the wrapped rod; unwound, the text runs column by column along the strip
- Here: EXIT BEHIND THE PICTURE
- In the escape room: a paper strip with jumbled letters and several wooden rods, only one has the right diameter
- Rail fence: easy to recognize because the letter frequencies stay unchanged
- Characteristic of all transpositions: frequencies like normal English text, but unreadable



Steganography

The best message is the one nobody finds

└Steganography

Steganography

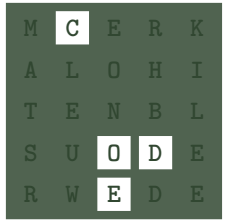
The best message is the one nobody finds



Grilles and Acrostics

The secret hides in plain sight[5]

- **Cardan grille**[14]: place a stencil with holes over a harmless text
- **Acrostic**[15]: the first letters of each line of a poem
- **Invisible ink**: only visible under UV light or heat



Grille reveals: `CODE`

- Steganography: Greek for covered writing
- Cardan grille, after Girolamo Cardano, 16th century
- In the escape room: a letter lies around openly, the grille is in another drawer
- UV flashlights are a staple of almost every escape room
- Without the grille or the light the clue is worthless. So it is a kind of key



Book Cipher

The book is the key[16]

- Number triples: `page-line-word`
- Example: `12-3-5  47-1-2  3-10-1`
- Unsolvable without the right book (and the right edition!)
- In the escape room: suddenly the bookshelf is no longer just decoration

Book Cipher
The book is the key[16]
- Number triples: page-line-word
- Example: 12-3-5 47-1-2 3-10-1
- Unsolvable without the right book (and the right edition!)
- In the escape room: suddenly the bookshelf is no longer just decoration

- Also called Ottendorf cipher or Arnold cipher[17]
- Famous example: the Beale ciphers, an alleged treasure, encrypted using the US Declaration of Independence
- Tip for players: if many numbers in groups of three show up in the room, check the bookshelf immediately
- Variants: only the first letter of the word counts, or page and letter



Now it's your turn!

Crack the code

FVB JYHJRLK PA

Now it's your turn!
Crack the code
FVB JYHJRLK PA



Now it's your turn!

Crack the code

FVB JYHJRLK PA

- Hint 1: It is a Caesar shift

Now it's your turn!
Crack the code
FVB JYHJRLK PA
- Hint 1: It is a Caesar shift



Now it's your turn!

Crack the code

FVB JYHJRLK PA

- Hint 1: It is a Caesar shift
- Hint 2: The first word addresses you directly

Now it's your turn!
Crack the code
FVB JYHJRLK PA
- Hint 1: It is a Caesar shift
- Hint 2: The first word addresses you directly



Now it's your turn!

Crack the code

FVB JYHJRLK PA

- Hint 1: It is a Caesar shift
- Hint 2: The first word addresses you directly
- Solution: $\texttt{F} \to \texttt{Y}$, so $k = 7$

YOU CRACKED IT

Now it's your turn!
Crack the code
FVB JYHJRLK PA
• Hint 1: It is a Caesar shift
• Hint 2: The first word addresses you directly
• Solution: F → Y, so k = 7
YOU CRACKED IT

- Give approx. 60 to 90 seconds, then show hint 1, then hint 2
- Solution: a three-letter word that addresses you: YOU. F becomes Y, that is 7 positions back
- Alternative: brute force over all 25 keys, or frequency analysis. Unreliable for such short texts
- This is exactly how a known-plaintext attack works: a guessed piece of plaintext reveals the key



And in Real Life?

Why you shouldn't protect your data with Caesar

└And in Real Life?

And in Real Life?

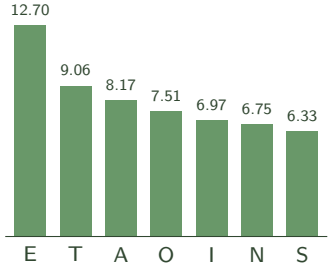
Why you shouldn't protect your data with Caesar



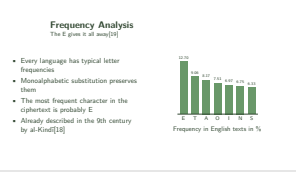
Frequency Analysis

The E gives it all away[19]

- Every language has typical letter frequencies
- Monoalphabetic substitution preserves them
- The most frequent character in the ciphertext is probably E
- Already described in the 9th century by al-Kindī[18]



Frequency in English texts in %



- That is why Caesar, Atbash, Pigpen and co. are trivial to crack for longer texts
- Also holds for the 26! possible keys of an arbitrary substitution. The key space alone does not protect
- Vigenère obscures the frequencies, but is vulnerable via the key length (Kasiski examination[20])



From the Cipher Disk to AES

What we learn from it[21]

- **Kerckhoffs's principle**: security must depend only on the key, not on keeping the method secret
- **Key space**:
  - Caesar: 25
  - Arbitrary substitution: $26! \approx 4 \cdot 10^{26}$
  - AES-128: $2^{128} \approx 3.4 \cdot 10^{38}$
- Modern ciphers also withstand known-plaintext attacks
- Don't roll your own crypto!

From the Cipher Disk to AES
What we learn from it[21]
• Kerckhoffs's principle: security must depend only on the key, not on keeping the method secret
• Key space:
— Caesar: 25
— Arbitrary substitution: 26! ≈ 4 · 10^26
— AES-128: 2^128 ≈ 3.4 · 10^38
• Modern ciphers also withstand known-plaintext attacks
• Don't roll your own crypto!

- Auguste Kerckhoffs, 1883: sooner or later the method falls into the hands of the enemy
- Escape rooms rely on exactly the opposite: security by obscurity. The puzzle is recognizing the method
- A large key space is necessary, but not sufficient. See frequency analysis
- In the hands-on puzzle, one guessed word was enough. Modern ciphers like AES are resistant to such known-plaintext attacks
- Bridge to the Enigma: polyalphabetic like Vigenère, but mechanized. Broken partly through guessed plaintext fragments (cribs) such as weather reports
- Practical takeaway: use established, audited libraries, don't invent anything yourself



Tips for Your Next Escape Room

From ciphertext to code

- Count the positions on the lock: how long must the solution be?
- Look out for alphabets, number sequences and symbols in the room
- Only dots and dashes? Morse! Groups of three? Book cipher!
- Strange script of corners and dots? Pigpen!
- Flashlight with UV? Shine it on everything!
- Talk to your team: the key is often in another puzzle

Tips for Your Next Escape Room
From ciphertext to code
- Count the positions on the lock: how long must the solution be?
- Look out for alphabets, number sequences and symbols in the room
- Only dots and dashes? Morse! Groups of three? Book cipher!
- Strange script of corners and dots? Pigpen!
- Flashlight with UV? Shine it on everything!
- Talk to your team: the key is often in another puzzle

- Summary of the talk as a practical checklist
- Escape rooms are a playful introduction to cryptography and information security
- Transition to thanks and questions



Thank you!

Materials available at
https://seism0saurus.de/posts/escape-room-kryptographie/

Materials and recording of the Nürnberg Digital workshop
"Alles auf ROT - wie du Verschlüsselung anwendest ... und knackst!" (German)
available at
https://seism0saurus.de/posts/session-nue-digital-alles-auf-rot/

Thank you!

Materials available at
https://seism0saurus.de/posts/escape-room-kryptographie/

Materials and recording of the Nürnberg Digital workshop
"Alles auf ROT - wie du Verschlüsselung anwendest ... und knackst!" (German)
available at
https://seism0saurus.de/posts/session-nue-digital-alles-auf-rot/



References I

[1] *Character encoding*. URL: https://en.wikipedia.org/wiki/Character_encoding (visited on 11/05/2026).

[2] *Cryptography*. URL: https://en.wikipedia.org/wiki/Cryptography (visited on 11/05/2026).

[3] *Substitution cipher*. URL: https://en.wikipedia.org/wiki/Substitution_cipher (visited on 11/05/2026).

[4] *Transposition cipher*. URL: https://en.wikipedia.org/wiki/Transposition_cipher (visited on 11/05/2026).

References I

[1] *Character encoding*. URL: https://en.wikipedia.org/wiki/Character_encoding (visited on 11/05/2026).

[2] *Cryptography*. URL: https://en.wikipedia.org/wiki/Cryptography (visited on 11/05/2026).

[3] *Substitution cipher*. URL: https://en.wikipedia.org/wiki/Substitution_cipher (visited on 11/05/2026).

[4] *Transposition cipher*. URL: https://en.wikipedia.org/wiki/Transposition_cipher (visited on 11/05/2026).



References II

[5] *Steganography*. URL: https://en.wikipedia.org/wiki/Steganography (visited on 11/05/2026).

[6] Albrecht Beutelspacher. *Cryptology. An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding and Safeguarding*. Mathematical Association of America, 1994.

[7] *Morse code*. URL: https://en.wikipedia.org/wiki/Morse_code (visited on 11/05/2026).

[8] *Caesar cipher*. URL: https://en.wikipedia.org/wiki/Caesar_cipher (visited on 11/05/2026).

References II

[5] *Steganography*. URL: https://en.wikipedia.org/wiki/Steganography (visited on 11/05/2026).

[6] Albrecht Beutelspacher. *Cryptology. An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding and Safeguarding*. Mathematical Association of America, 1994.

[7] *Morse code*. URL: https://en.wikipedia.org/wiki/Morse_code (visited on 11/05/2026).

[8] *Caesar cipher*. URL: https://en.wikipedia.org/wiki/Caesar_cipher (visited on 11/05/2026)



References III

[9] *Atbash*. URL: https://en.wikipedia.org/wiki/Atbash (visited on 11/05/2026).

[10] *Pigpen cipher*. URL: https://en.wikipedia.org/wiki/Pigpen_cipher (visited on 11/05/2026).

[11] *Polybius square*. URL: https://en.wikipedia.org/wiki/Polybius_square (visited on 11/05/2026).

[12] *Vigenère cipher*. URL: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher (visited on 11/05/2026).

References III

[9] *Atbash*. URL: https://en.wikipedia.org/wiki/Atbash (visited on 11/05/2026).

[10] *Pigpen cipher*. URL: https://en.wikipedia.org/wiki/Pigpen_cipher (visited on 11/05/2026).

[11] *Polybius square*. URL: https://en.wikipedia.org/wiki/Polybius_square (visited on 11/05/2026).

[12] *Vigenère cipher*. URL: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher (visited on 11/05/2026).



References IV

[13] *Scytale*. URL: https://en.wikipedia.org/wiki/Scytale (visited on 11/05/2026).

[14] *Grille (cryptography)*. URL: https://en.wikipedia.org/wiki/Grille_(cryptography) (visited on 11/05/2026).

[15] *Acrostic*. URL: https://en.wikipedia.org/wiki/Acrostic (visited on 11/05/2026).

[16] Simon Singh. *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate, 1999.

References IV

[13] *Scytale*. URL: https://en.wikipedia.org/wiki/Scytale (visited on 11/05/2026).

[14] *Grille (cryptography)*. URL: https://en.wikipedia.org/wiki/Grille_(cryptography) (visited on 11/05/2026).

[15] *Acrostic*. URL: https://en.wikipedia.org/wiki/Acrostic (visited on 11/05/2026).

[16] Simon Singh. *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate, 1999.



References V

[17] *Book cipher*. URL: https://en.wikipedia.org/wiki/Book_cipher (visited on 11/05/2026).

[18] *Al-Kindi*. URL: https://en.wikipedia.org/wiki/Al-Kindi (visited on 11/05/2026).

[19] *Letter frequency*. URL: https://en.wikipedia.org/wiki/Letter_frequency (visited on 11/05/2026).

[20] *Kasiski examination*. URL: https://en.wikipedia.org/wiki/Kasiski_examination (visited on 11/05/2026).

References V

[17] *Book cipher*. URL: https://en.wikipedia.org/wiki/Book_cipher (visited on 11/05/2026).

[18] *Al-Kindi*. URL: https://en.wikipedia.org/wiki/Al-Kindi (visited on 11/05/2026).

[19] *Letter frequency*. URL: https://en.wikipedia.org/wiki/Letter_frequency (visited on 11/05/2026).

[20] *Kasiski examination*. URL: https://en.wikipedia.org/wiki/Kasiski_examination (visited on 11/05/2026).



References VI

[21] *Kerckhoffs's principle*. URL: https://en.wikipedia.org/wiki/Kerckhoffs's_principle (visited on 11/05/2026).

References VI

[21] *Kerckhoffs's principle*. URL: https://en.wikipedia.org/wiki/Kerckhoffs's_principle (visited on 11/05/2026).