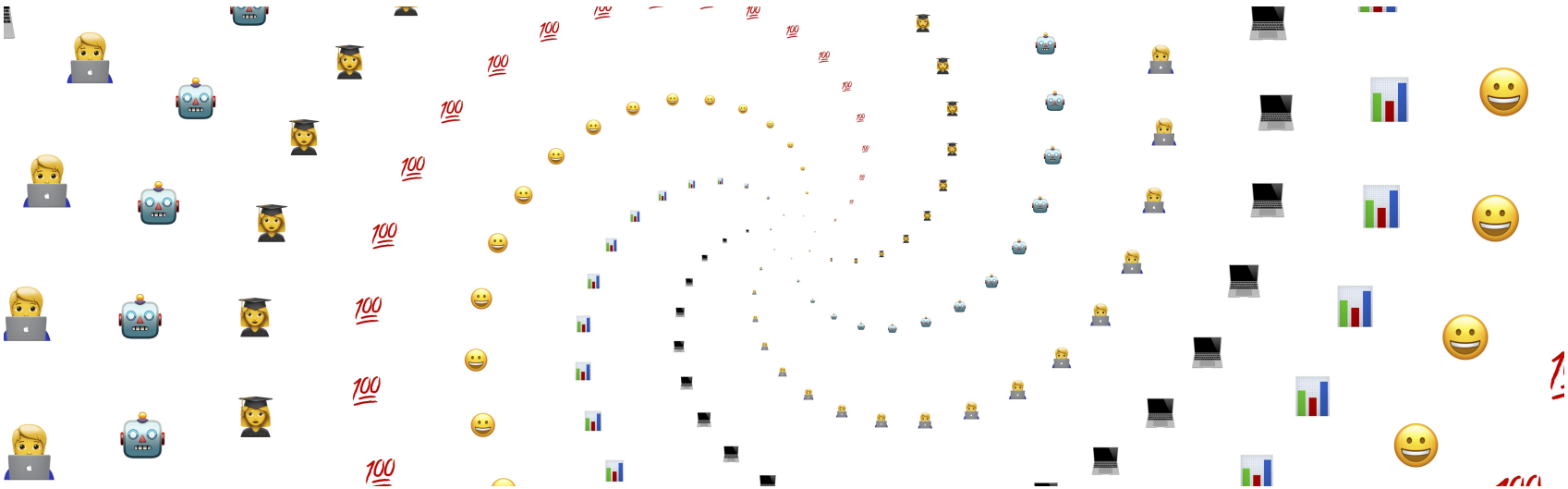
Kryptologie

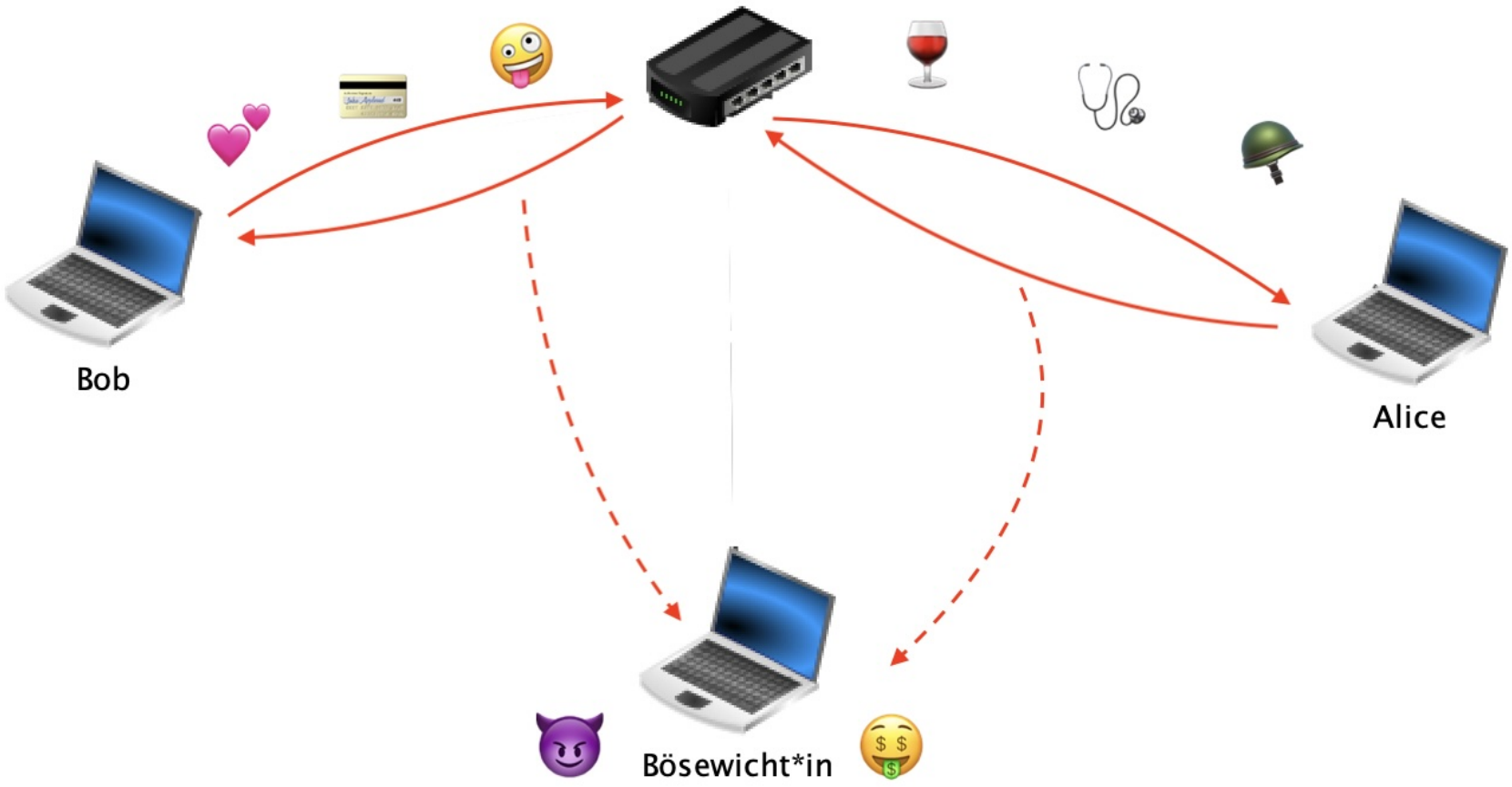
Einführung

Cyril Wendl

Fachschaft Informatik
Kantonsschule im Lee

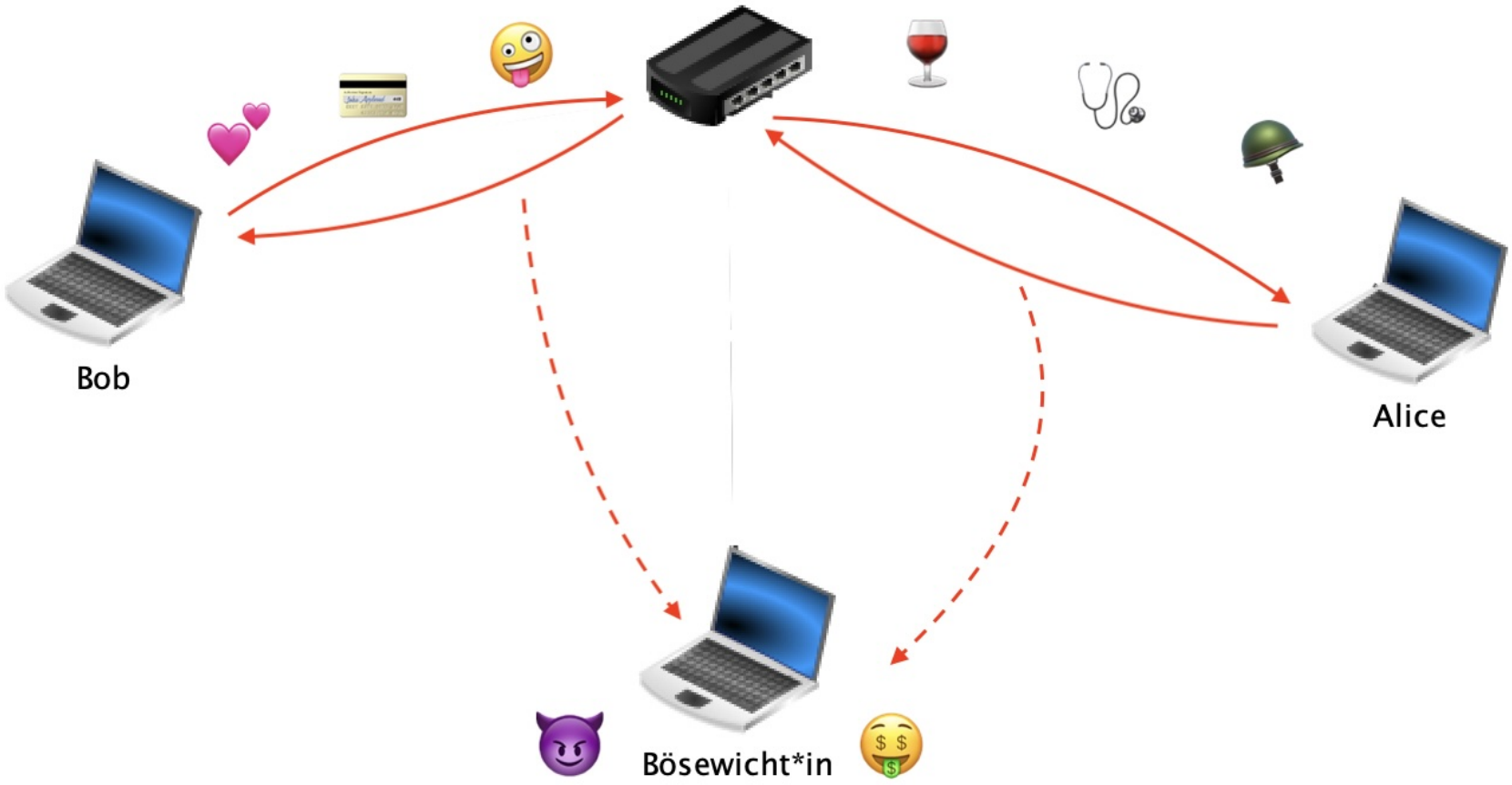


Internet = *offene* Technologie



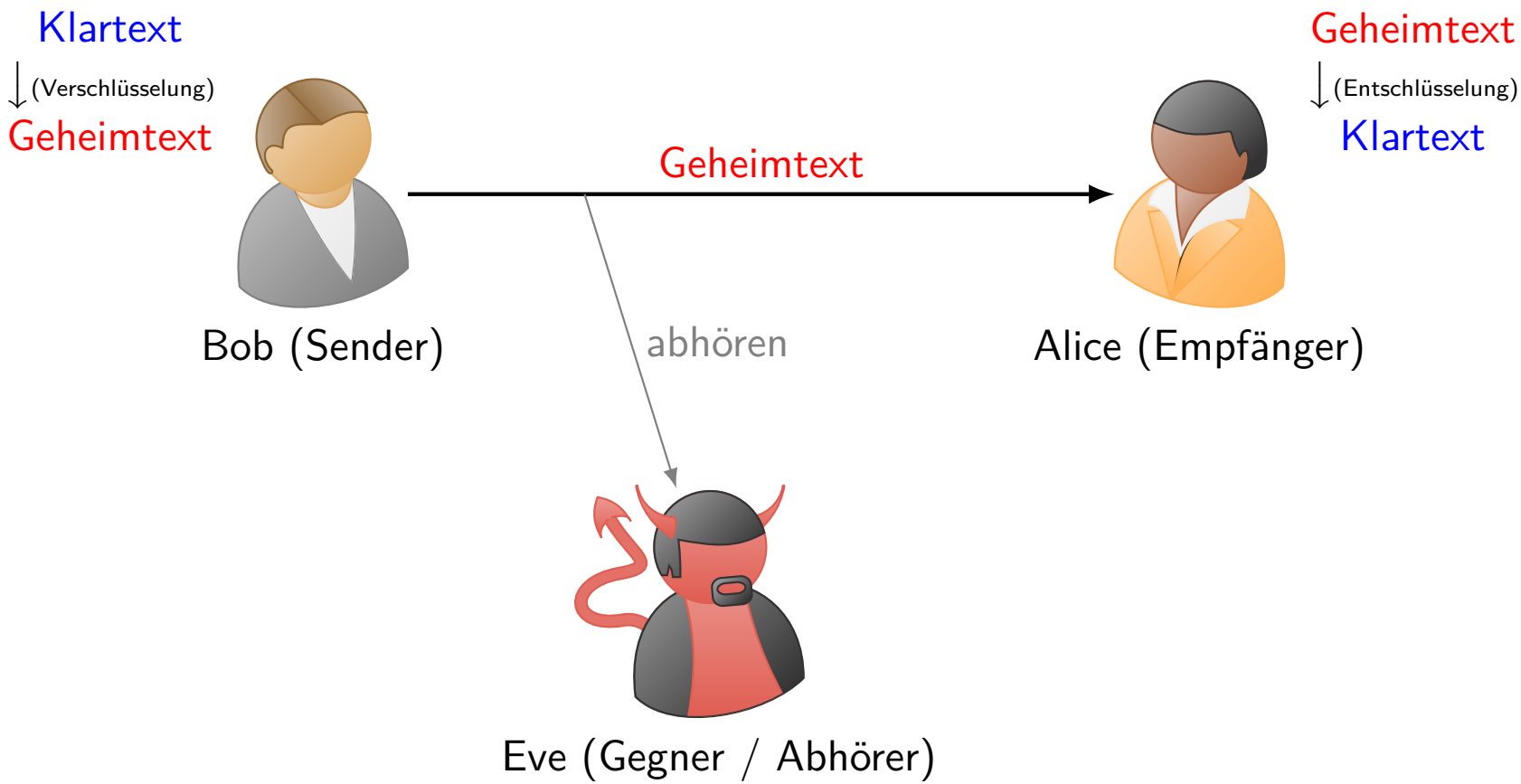
Was machen Sie alles im Internet?

Internet = *offene* Technologie

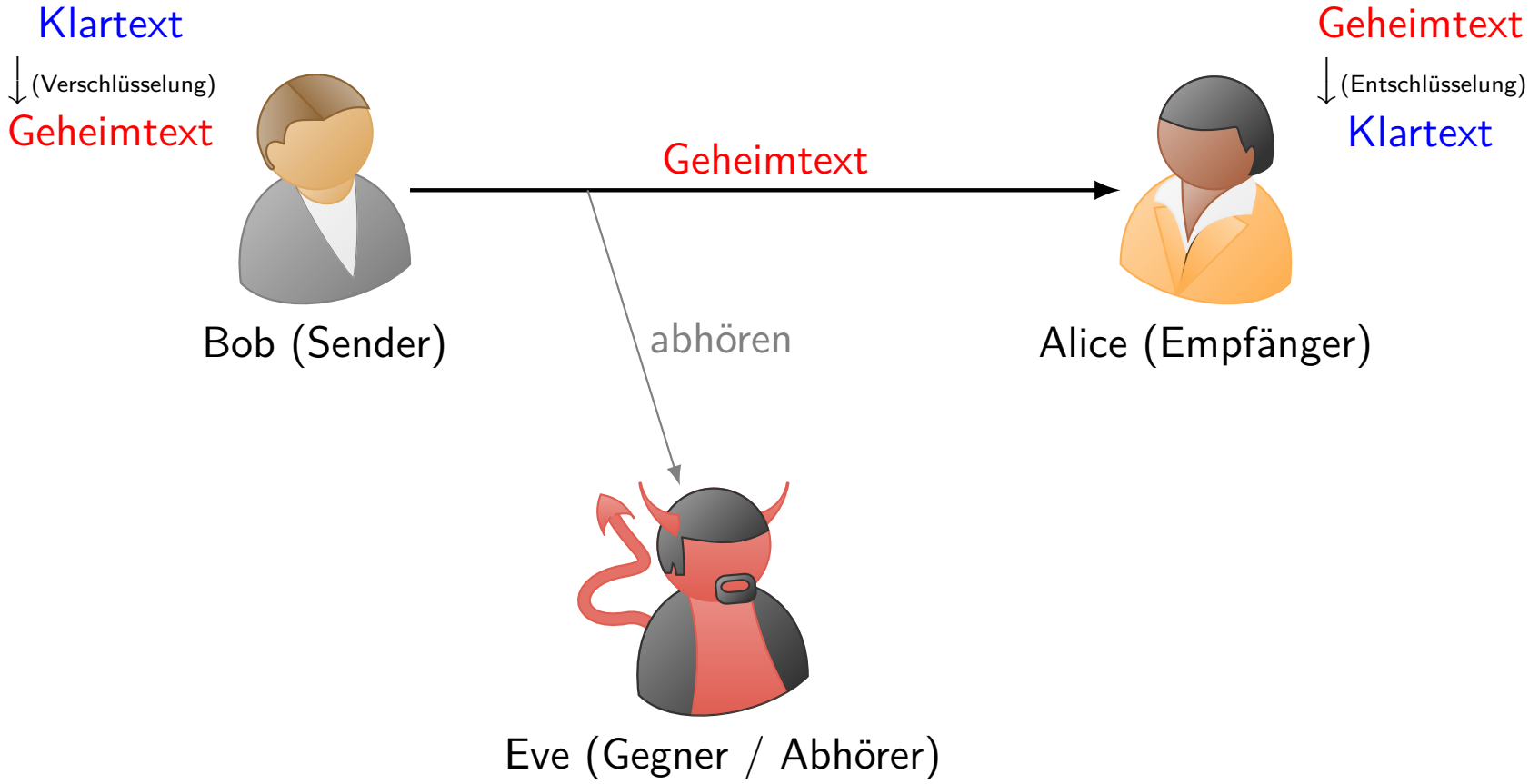


Z.B.: Sie schreiben eine Nachricht an Ihr 💕...
...und ich kann alles mitlesen! 🤦

Geheime Kommunikation zwischen Bob und Alice



Geheime Kommunikation zwischen Bob und Alice



Würden Sie die Erpressungsgebühr zahlen?

Symmetrische Verschlüsselungsverfahren

- 🔑 Derselbe **Schlüssel** zur Ver- und Entschlüsselung

Symmetrische Verschlüsselungsverfahren

- 🔑 Derselbe **Schlüssel** zur Ver- und Entschlüsselung
- 🤫 Sender und Empfänger müssen sich auf einen Schlüssel einigen, ohne dass ein Dritter mithören kann

Symmetrische Verschlüsselungsverfahren

- 🔑 Derselbe **Schlüssel** zur Ver- und Entschlüsselung
- 🤫 Sender und Empfänger müssen sich auf einen Schlüssel einigen, ohne dass ein Dritter mithören kann
- 🔐 Analogie: Schatzkiste versenden

Einführungsaufgabe 1

Der Geheimtext lautet:

AMEHT SEGITHCIW NIE TSI EIGOLOTPYRK

Stellen Sie den ursprünglichen Text wieder her.

Lösung der Einführungsaufgabe 1

Geheimtext:
AMEHT SEGITHCIW NIE TSI EIGOLOTPYRK

ursprünglicher Text:
KRYPTOLOGIE IST EIN WICHTIGES THEMA

Der Geheimtext entspricht dem von rechts nach links (rückwärts) gelesenen ursprünglichen Text.

Einführungsaufgabe 2

Der Geheimtext lautet:

1. RKPYOTOLIGEEMREOLGCITHEGEHMIINSSE
2. HCSFIRILTAHCZFUEBUHAWNERDNUKUZMMOINUEIZNER

Stellen Sie den ursprünglichen Text wieder her.

Lösung Einführungsaufgabe 2

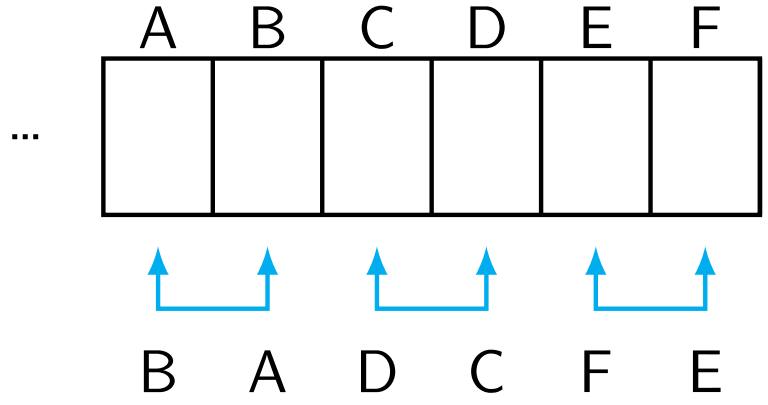
Geheimtext:

1. RKPYOTOLIGEEMREOLGCITHEGEHMIINSSE
2. HCSFIRILTAHCZFUEBUHAWNERDNUKUZMMOINUEIZNER

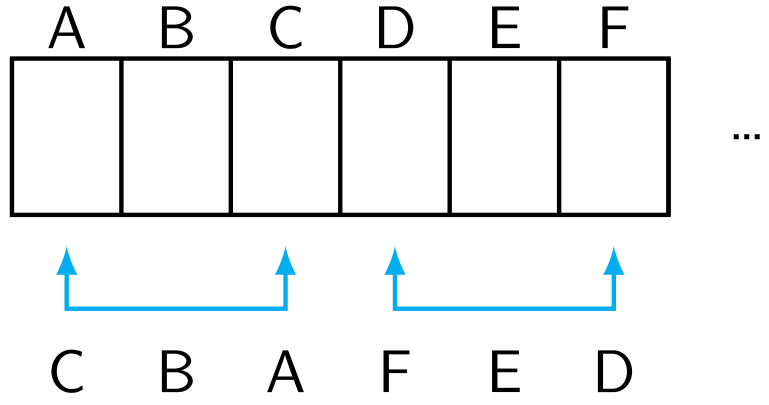
Ursprünglicher Text:

1. KRYPTOLOGIE ERMOEGLICHT GEHEIMNISSE
2. SCHRIFTLICH AUFZUBEWAHREN UND ZU KOMMUNIZIEREN

Der Geheimtext entsteht durch Austauschen der Positionen der Buchstaben.



(a) „Zweiertausch“



(b) „Dreiertausch“

Stock-und-Streifen-Verschlüsselung

🧩 Wer löst das Rätsel zuerst?

Stock-und-Streifen-Verschlüsselung

→ **Skytale** (von altgriechisch *skytálē* = „Stock“, „Stab“)

- Ältestes bekanntes militärisches Verschlüsselungsmethode der Welt!

Stock-und-Streifen-Verschlüsselung

→ **Skytale** (von altgriechisch *skytálē* = „Stock“, „Stab“)

- Ältestes bekanntes militärisches Verschlüsselungsmethode der Welt!
- Von Spartanern vor 2500 Jahren verwendet

Skytale

- Schreibe den Klartext zeilenweise in eine Tabelle (Matrix) von links nach rechts.
- Der Geheimtext erhalten wir, indem wir die Buchstaben Spalte für Spalte von links nach rechts lesen.

S	P	A	R	T	A	W
A	R	I	N	D	E	R
A	N	T	I	K	E	D
E	R	H	A	U	P	T
O	R	T	D	E	R	L
A	N	D	S	C	H	A
F	T	L	A	K	O	N
I	E	N	X	K	M	G

Skytale

- Falls der Klartext die Tabelle nicht vollständig ausfüllt, so füllt man die leeren Felder mit beliebigen Buchstaben auf (rot markiert).

S	P	A	R	T	A	W
A	R	I	N	D	E	R
A	N	T	I	K	E	D
E	R	H	A	U	P	T
O	R	T	D	E	R	L
A	N	D	S	C	H	A
F	T	L	A	K	O	N
I	E	N	X	K	M	G

Auftrag

Skript (auf Moodle)

- Aufgaben 1.2, 1.3
- Challenge: Aufgabe 1.4

Zeichen Ersetzen

Welche Methoden kennen wir bereits?

ASCII (Auszug)

Dezimal	Hexadezimal	Binär	Zeichen
0	00	00000000	NUL
1	01	00000001	SOH
2	02	00000010	STX
3	03	00000011	ETX
4	04	00000100	EOT
…	…	…	…
36	24	00100100	$
37	25	00100101	%
38	26	00100110	&
39	27	00100111	'
40	28	00101000	(
41	29	00101001	)
…	…	…	…
48	30	00110000	0
49	31	00110001	1
50	32	00110010	2
51	33	00110011	3
52	34	00110100	4
…	…	…	…
65	41	01000001	A
66	42	01000010	B
67	43	01000011	C
68	44	01000100	D
69	45	01000101	E
…	…	…	…

Kerkhoffs'sches Prinzip der Sicherheit

„Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi."
– Auguste Kerckhoffs, La cryptographie militaire (1883)

Kerkhoffs'sches Prinzip der Sicherheit

„Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi."
– Auguste Kerckhoffs, La cryptographie militaire (1883)

Kein Geheimhaltung $\rightarrow$ **Open Source**!

Anforderungen an kryptographische Systeme

1. **Vertraulichkeit**: Es soll sichergestellt sein, dass wirklich nur diejenige eine Nachricht lesen kann, für die diese bestimmt ist.

Welche dieser Anforderungen werden durch Skytale und Caesar erfüllt?

Anforderungen an kryptographische Systeme

1. **Vertraulichkeit**: Es soll sichergestellt sein, dass wirklich nur diejenige eine Nachricht lesen kann, für die diese bestimmt ist.
2. **Integrität**: Die Empfängerin soll feststellen können, ob die Nachricht nach ihrer Erzeugung verändert wurde.

Welche dieser Anforderungen werden durch Skytale und Caesar erfüllt?

Anforderungen an kryptographische Systeme

1. **Vertraulichkeit**: Es soll sichergestellt sein, dass wirklich nur diejenige eine Nachricht lesen kann, für die diese bestimmt ist.
2. **Integrität**: Die Empfängerin soll feststellen können, ob die Nachricht nach ihrer Erzeugung verändert wurde.
3. **Authentizität**: Der Verfasser einer Nachricht soll identifizierbar sein, bzw. die Empfängerin soll nachprüfen können, wer der Verfasser ist.

Welche dieser Anforderungen werden durch Skytale und Caesar erfüllt?

Anforderungen an kryptographische Systeme

1. **Vertraulichkeit**: Es soll sichergestellt sein, dass wirklich nur diejenige eine Nachricht lesen kann, für die diese bestimmt ist.
2. **Integrität**: Die Empfängerin soll feststellen können, ob die Nachricht nach ihrer Erzeugung verändert wurde.
3. **Authentizität**: Der Verfasser einer Nachricht soll identifizierbar sein, bzw. die Empfängerin soll nachprüfen können, wer der Verfasser ist.
4. **Verbindlichkeit**: Der Verfasser soll nicht abstreiten können, dass er der Verfasser der Nachricht ist.

Welche dieser Anforderungen werden durch Skytale und Caesar erfüllt?

Zusammenfassung

- Verschlüsselung betrifft viele persönliche, soziale sowie politische Bereiche

Zusammenfassung

- Verschlüsselung betrifft viele persönliche, soziale sowie politische Bereiche
- Daten sollen verschlüsselt übertragen werden, um Einblick durch fremde Personen zu vermeiden (Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit)

Zusammenfassung

- Verschlüsselung betrifft viele persönliche, soziale sowie politische Bereiche
- Daten sollen verschlüsselt übertragen werden, um Einblick durch fremde Personen zu vermeiden (Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit)
- Mono- sowie polyalphabetische Kryptosysteme sind einfach zu knacken $\rightarrow$ Häufigkeitsanalyse (nächstes Mal)!