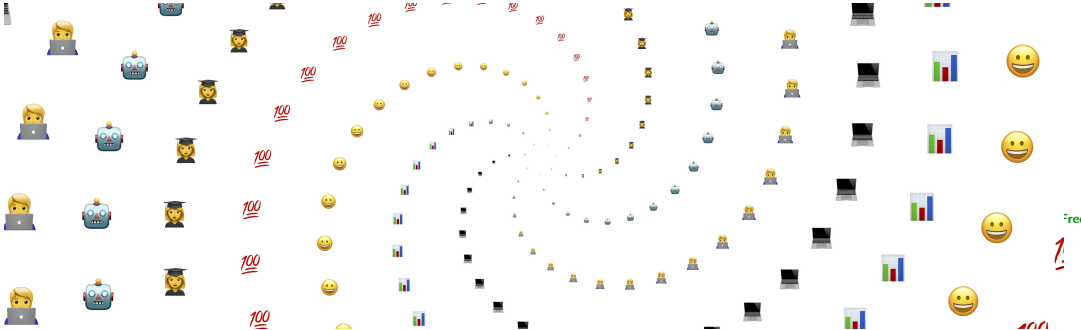
Kryptologie

Einführung

Cyril Blum

Fachschaft Informatik
Kantonsschule im Lee



Internet = *offene* Technologie

Was machen Sie alles im Internet?

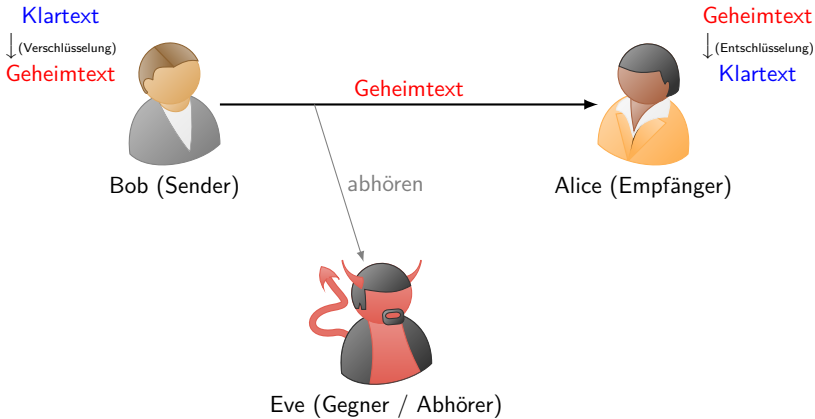


Internet = *offene* Technologie

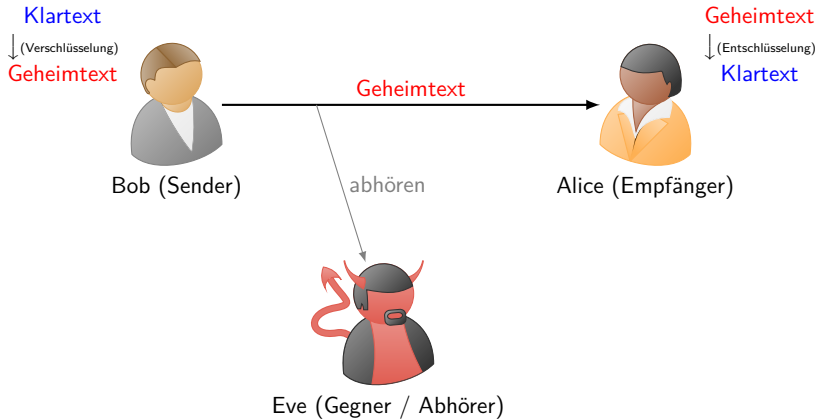
Z.B.: Sie schreiben eine Nachricht an Ihr 💕...
...und ich kann alles mitlesen! 🤓



Geheime Kommunikation zwischen Bob und Alice



Geheime Kommunikation zwischen Bob und Alice



Würden Sie die Erpressungsgebühr zahlen?

FreeFlower

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



FreeFlower

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



FreeFlower

Einführungsaufgabe 1

Der Geheimtext lautet:

AMEHT SEGITHCIW NIE TSI EIGOLOTPYRK

Stellen Sie den ursprünglichen Text wieder her.



FreeFlower

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

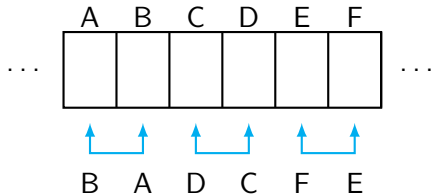
Geheimtext:

1. RKPYOTOLIGEEMREOLGCITHEGEHMIINSSE
2. HCSFIRILTAHCZFUEBUHAWNERDNUKUZMMOINUEIZNER

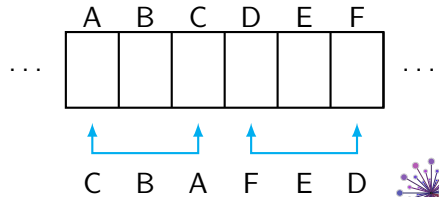
Ursprünglicher Text:

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



Foto: Luringen, Wikimedia Commons, CC BY-SA 3.0

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

- Ältestes bekanntes militärisches Verschlüsselungsmethode der Welt!

FreeFlower

Stock-und-Streifen-Verschlüsselung



Foto: Luringen, Wikimedia Commons, CC BY-SA 3.0

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

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

FreeFlower

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 1.1 - 1.4

