IT-Sicherheit 2 (Einführung Kryptographie) – Zusammenfassung mit IHK-Bezug

Klartext & Chiffrat, ROT-13, Transposition, Steganographie

🔐 IT-Sicherheit 2 – Einführung Kryptographie

📘 Grundlage: Folien „Entschlüsseln Sie das mal …“ (GBS Fachschule, 13 Folien).

🧭 So liest du dieses Dokument

- **Fett** = Prüfungs-Schlagwort. 🎯 = eigene Einschätzung der IHK-Relevanz.
- Die alten Verfahren (ROT-13, Transposition) kommen selten direkt in der Prüfung vor. Sie erklären aber die **Begriffe**, die später wichtig sind: Klartext, Chiffrat, Algorithmus, Schlüssel.
- ✏️ Übungsfragen am Ende jedes Blocks, Lösungen ganz am Ende. 🔎 = Ergänzung.

📖 Block 1: Die Grundbegriffe

🎯 IHK-Relevanz: **hoch** – die Begriffe musst du sicher benutzen können.

Begriff	Bedeutung	Beispiel
Klartext	die lesbare Nachricht	„Wir verwenden Cookies …“
Chiffrat (= Geheimtext, Kryptogramm, Ciphertext)	die verschlüsselte Nachricht	„Jve irejraqra Pbbxvrf …“
Verschlüsseln	Klartext → Chiffrat	
Entschlüsseln	Chiffrat → Klartext	

🕵️ Wie knackt man ein Chiffrat? – „Educated Guesses“

Nicht wild raten, sondern **begründet vermuten**. Das spart Zeit, Geld und Rechenleistung.

1. **Was ist es?** → vermutlich ein Text.
2. **Welche Sprache?** → vermutlich Deutsch.

3. **Welches Verfahren?** → vermutlich einfache Buchstabenvertauschung.

Dann nach **Merkmalen** suchen:

- **Häufigkeit**: Der häufigste Buchstabe im Deutschen ist **e**.
- **Muster**: typische Paare wie „ch“, „sch“, „st“, „nd“.
- **Kurze Wörter**: 2–3 Buchstaben → um, zu, in, der, die, das, ein, und.
- Je **länger** das Chiffrat, desto besser funktioniert das.

💡 Genau das nennt man **Häufigkeitsanalyse**. Sie knackt jede einfache Buchstabenvertauschung.

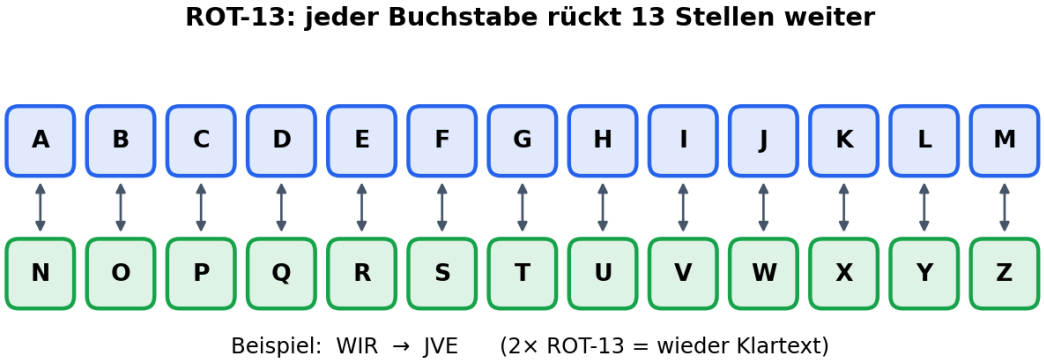
✏️ Übungsfragen Block 1

Ü1.1 Nennen Sie drei andere Wörter für „Chiffrat“.

Ü1.2 Warum ist ein langes Chiffrat leichter zu knacken als ein kurzes?

🔄 Block 2: ROT-13 – Buchstaben ersetzen (Substitution)

🎯 IHK-Relevanz: **mittel** – als Beispiel für ein unsicheres Verfahren.



ROT-13

- Jeder Buchstabe wird durch den Buchstaben **13 Stellen weiter** im Alphabet ersetzt.
- Fachbegriff: **monoalphabetische Substitution** (ein Buchstabe wird immer durch denselben ersetzt).
- Verwandt: **Cäsar-Chiffre** (beliebige Verschiebung, z. B. um 3).
- Besonderheit: Das Alphabet hat 26 Buchstaben. 13 + 13 = 26. Darum gilt: **zweimal ROT-13 = wieder Klartext**.

Beispiel: W → J, I → V, R → E. Also **WIR → JVE**.

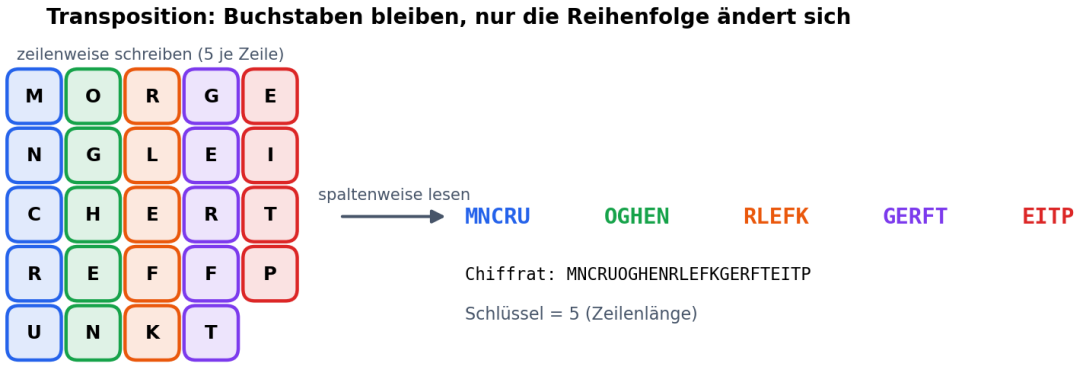
✏️ Übungsfragen Block 2

Ü2.1 Verschlüsseln Sie „IHK“ mit ROT-13.

Ü2.2 Warum knackt eine Häufigkeitsanalyse ROT-13 sofort?

🔀 Block 3: Transposition – Buchstaben umsortieren

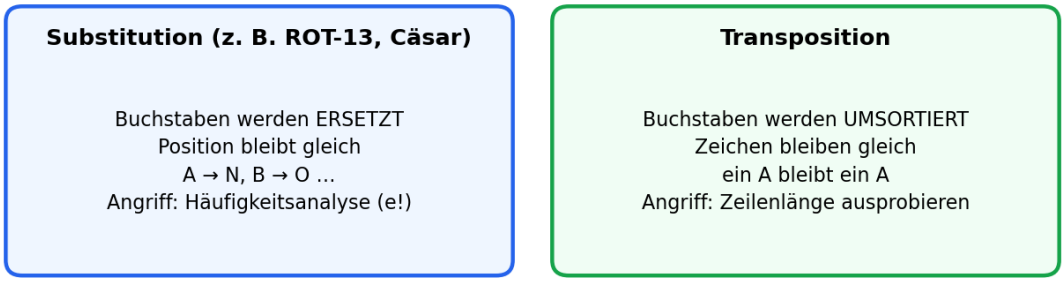
🎯 IHK-Relevanz: **gering bis mittel**.



Transposition

- Die Zeichen **bleiben gleich** (ein A bleibt ein A). Nur die **Reihenfolge** ändert sich.
- Vorbereitung (**Normieren**): alles groß schreiben, ä → ae, Leer- und Satzzeichen weg.
- Text in Zeilen fester Länge schreiben (hier 5), dann **spaltenweise** ablesen.
- Kennt man die Zeilenlänge (= den **Schlüssel**), kann man zurückrechnen. Leer- und Satzzeichen ergänzt man dann leicht.

Beispiel aus dem Unterricht: „Morgen, gleicher Treffpunkt“ → **MNCRUOGHENRLEFKGERFTEITP**



Substitution vs. Transposition

✏️ Übungsfragen Block 3

Ü3.1 Was ist der Unterschied zwischen Substitution und Transposition?

Ü3.2 Entschlüsseln Sie **HLAOL** (Zeilenlänge 3, der Klartext hat 5 Buchstaben).

🖼️ Block 4: Steganographie – Nachrichten verstecken

🎯 IHK-Relevanz: **gering** – gut als Abgrenzung zur Kryptographie.

- Von griechisch „steganós“ + „gráphein“ = **verstecktes Schreiben**.
- Die Nachricht wird **in anderen Daten versteckt** (dem **Container**), meist Bilder oder Musik.
- Die Änderung liegt **unter der Wahrnehmungsschwelle**. Niemand sieht oder hört sie.
- Der Container wirkt völlig harmlos. Man merkt nicht einmal, **dass** etwas versteckt ist.

	Kryptographie	Steganographie
Ziel	Inhalt **unlesbar** machen	Existenz der Nachricht **verbergen**
Angreifer sieht	„Da ist etwas Geheimes“	„Nur ein Urlaubsgruß“

Beispiel aus dem Unterricht („Liebe Kolleginnen! Wir genießen nun endlich …“): Man zählt die Buchstaben jedes Wortes. **Gerade Länge = 1, ungerade = 0**. Je 8 Wörter ergeben ein Byte:

Binär	Dezimal	ASCII
01010011	83	**S**
01001111	79	**O**
01010011	83	**S**

→ Versteckte Botschaft: **SOS**

⚠️ Auf der Folie steht die Spalte „Hex“, die Werte 83 / 79 sind aber **Dezimal**zahlen. Hexadezimal wären es 53 / 4F.

💡 Beides lässt sich kombinieren: erst verschlüsseln, dann verstecken.

✏️ Übungsfragen Block 4

Ü4.1 Worin unterscheiden sich Kryptographie und Steganographie?

Ü4.2 Welches Zeichen ergibt die Bitfolge 01000001 (ASCII)?

✅ Lösungen

Ü1.1 Geheimtext, Kryptogramm, Ciphertext.

Ü1.2 Mehr Text = mehr Buchstaben. Dann treten Häufigkeiten und Muster deutlicher hervor.

Ü2.1 I → V, H → U, K → X. Also **VUX**.

Ü2.2 Jeder Buchstabe wird immer gleich ersetzt. Die Häufigkeiten bleiben erhalten. Der häufigste Chiffrat-Buchstabe ist vermutlich „e“ – damit ist die Verschiebung bekannt.

Ü3.1 Substitution ersetzt Zeichen (Position bleibt). Transposition vertauscht Positionen (Zeichen bleiben).

Ü3.2 5 Buchstaben in Zeilen zu 3 → Zeile 1 hat 3, Zeile 2 hat 2 Buchstaben. Die Spalten sind also 2 + 2 + 1 Zeichen lang: **HL | AO | L**. Zeilenweise lesen: H A L / L O → **HALLO**.

Ü4.1 Kryptographie macht den Inhalt unlesbar, man sieht aber, dass etwas verschlüsselt ist. Steganographie versteckt die Nachricht so, dass niemand merkt, dass es sie gibt.

Ü4.2 01000001 = 65 = **A**.