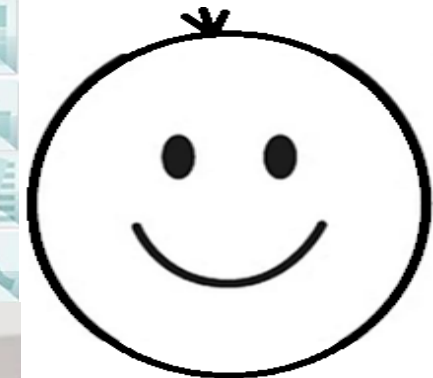
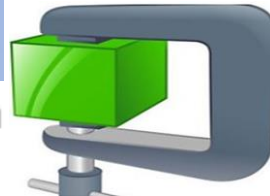


Rückblick

Kunst ist Weglassen

* Bewertung Ihrer gelösten fünf Arbeiten



* Vektorengrafiken wurde erarbeitet! → **B09**
- Die 5 Aufgaben wurden erledigt!

Stoff → Block 10

- * Definierte Lernziele
- * Ziele beim Schutz von Informationen
- * Steganographie
- * Geschichte der Verschlüsselung
- * Symmetrische und asymmetrische Verschlüsselung
- * Hinweise auf zusätzliches Lernmaterial



Übungen bzw. Aufgaben

- * Persönlich gelöste und besprochene 2. Arbeit zu Unterrichtsblock 05..08 korrigieren!
- * Block 10 "Verschlüsselung – Geschichte und Grundsätzliches" wird persönlich erarbeitet und vorhandene Fragen bzw. Unklarheiten werden notiert bzw. gemeldet und die 5 Aufgaben dazu werden sauber und vollständig gelöst!

Ausblick

Fr. 15. Dez.: - Verschlüsselungsverfahren erkennen → **B11**

Fr. 22. Dez.: - Rückblickarbeiten erledigen → **B09..11 (A3)**

Weihnachtsferien

Fr. 12. Jan.: - Kryptographie und Seganographie definieren und anwenden → **B12**

Fr. 19. Jan.: - Arbeiten zu den erarbeiten M114-Modulidentifikationen! → **B1..B12**

Fr. 26. Jan.: - Arbeiten zu den erarbeiten M114-Modulidentifikationen! → **B1..B12**
- Modul 114 abschliessen

M114

Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Berufsbildungszentrum
Wirtschaft, Informatik und Technik

bbzw.lu.ch

Freitag:	KW	SW	Themen (Theorie und Übungen)	Stoffplan
25.08.2023	34	01	00 Begrüssung und Einleitung 01 Die Zahlensysteme BIN, HEX und DEZ kennenlernen	
01.09.2023	35	02	02 Arithmetische und logische Grundoperationen binär	
08.09.2023	36	03	Rückblickübungen zu Block 01 und 02 lösen	
15.09.2023	37	04	03 Die Logik und den Prozessor verstehen	
22.09.2023	38	05	Prüfung Block 01 und 02 04 Grosse Zahlen in kleinen Variablen ablegen, wie geht das?	P1
29.09.2023	39	06	Rückblickübungen zu Block 03 und 04 lösen	
			Herbstferien	
20.10.2023	42	07	05 Fehler in der Datenübertragung finden und korrigieren	
27.10.2023	43	08	Arbeit zu Block 02 bis und mit 04 schreiben	A1
03.11.2023	44	09	06 Speicherplatz als rares Gut – Dateien und ihr Platzbedarf	
10.11.2023	45	10	07 Speicherplatz als rares Gut – Dateien und ihr Platzbedarf, Kompression	
17.11.2023	46	11	08 Speicherplatz als rares Gut – Reduktion	
24.11.2023	47	12	Arbeit zu Block 06 bis und mit Block 08 schreiben 09 Vektorgrafiken – Eine Alternative zu den Pixeln	A2
01.12.2023	48	13	10 Verschlüsselung – Geschichte und Grundsätzliches	
08.12.2023	49	14	Maria Empfängnis	
15.12.2023	50	15	11 Verschlüsselung – Moderne Verfahren	
22.12.2023	51	16	Arbeit zu Block 09 bis und mit Block 11 schreiben	A3
			Weihnachtsferien	
12.01.2024	02	17	12 Kryptographie und Steganographie definieren und anwenden	
19.01.2024	03	18	Rückblickübungen über erarbeitete M114-Themen lösen	
26.01.2024	04	19	Rückblickübungen über erarbeitete M114-Themen abschliessen Modul abschliessen	



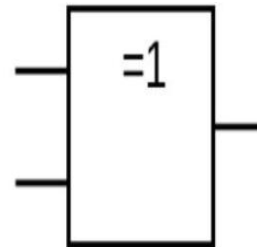
00 Einleitung für
Lehrpersonen und Lernende



01 Die Zahlensysteme BIN,
HEX und DEZ kennenlernen
Zahlenwerte darstellen, Zahlenwerte
umrechnen.

$$\begin{array}{r} 1010 \\ + 111 \\ \hline 10001 \end{array}$$

02 Arithmetische und
logische Grundoperationen
bin...



03 Die Logik und den
Prozessor verstehen



04 Grosse Zahlen in kleinen
Variablen ablegen, wie...



05 Fehler in der
Datenübertragung finden
und korri...



06 Speicherplatz als rares
Gut – Dateien und ihr P...



07 Speicherplatz als rares
Gut – Kompression



08 Speicherplatz als rares
Gut – Reduktion



09 Vektorgrafiken – Eine
Alternative zu den Pixeln



10 Verschlüsselung –
Geschichte und
Grundsätzliche...



11 Verschlüsselung –
Moderne Verfahren

Rückblick

➔ **Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen** → **Merke, Vorgehen, Ablauf, Bewertung, Hilfen**

Sie erledigten 5 Aufträge zu den erarbeiteten und angewendeten Unterrichtsböcken 05 bis und mit 08! Das Prinzip zum Lösen solcher arbeiten wendeten Sie an ähnlichen Aufgaben bereits an.



05 Fehler in der Datenübertragung finden und korri...



06 Speicherplatz als rares Gut - Dateien und ihr P...



07 Speicherplatz als rares Gut - Kompression



08 Speicherplatz als rares Gut - Reduktion

Anzahl Punkte	Note	G INKM23a 3 / 3	INF 22aL 11 / 12	INF 22dL 9 / 10	INF 22bL 7 / 7
30..32	6.0			1	
29	5.9				1
28	5.8		1 1		1
27	5.7				
26	5.6	1			1
25	5.5	1 1 1			
24	5.4				
23	5.2				
22	5.0				
21	4.8				1
20	4.6			1	2
19	4.4				1
18	4.2		1 1	1 1	
17	4.0	1	1 1	1 1	
16	3.8		1	2	
15	3.6				
14	3.4			1	
13	3.2		1 1	1	
12	3.0				
11	2.8				
10	2.6		1		
4	1.4				
Durchschnitt:		4.5			

73%

27%

- Merke:** - Bei jeder Aufgabe wird wie gelernt nicht nur das Endresultat, sondern auch die **Vollständigkeit** des Lösungsweges und die **Klarheit, Sauberkeit und Normeinhaltung** bewertet.
- Falls Sie Lösungsteile von einer Ausgabe auf Ihre BYOD lösten, speichern Sie schlussendlich dieses File mit dem Namen 'INF22xL A2 IhrName_IhrVornae.pdf' bzw. wenn Sie diese Arbeiten in einer 2er-Grupper erledigten 'INF22xL A2 Name1_Name2.pdf' unter dem bei Teams geöffneten Arbeit '23-11-24 M114 A2 Daten, Kompression, Reduktion' ab.

Maximal: 32 Punkte

Fach: M114	Thema: Daten, Kompression, Reduktion (B5..B8!)	Punkte: 30	INF22xL	Note: 6.0
-------------------	---	-------------------	---------	------------------

M114

Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Berufsbildungszentrum
Wirtschaft, Informatik und Technik

bbzw.lu.ch

Rückblick

* Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen → **Merke, Vorgehen, Ablauf, Bewertung, Hilfen**

Sie erledigten 5 Aufträge zu den erarbeiteten und angewendeten Unterrichtsböcken 05 bis und mit 08! Das Prinzip zum Lösen solcher arbeiten wendeten Sie an ähnlichen Aufgaben bereits an.

→ Weitere Test:

19.12.23 Arbeit Vektorgrafiken und Verschlüsselung
xxxx Blitzprüfung

Anzahl Punkte	Note	GINKM23a 3 / 3	INF 22aL 11 / 12	INF 22dL 9 / 10	INF 22bL 7 / 7
30..32	6.0			1	
29	5.9				1
28	5.8		1 1		1
27	5.7				
26	5.6	1			1
25	5.5	1	1 1		
24	5.4				
23	5.2				
22	5.0				
21	4.8				1
20	4.6			1	2
19	4.4				1
18	4.2		1 1	1	
17	4.0	1	1	1 1	
16	3.8		1	2	
15	3.6				
14	3.4			1	
13	3.2		1 1	1	
12	3.0				
11	2.8				
10	2.6		1		
4	1.4				
Durchschnitt:		4.5			

73%

27%

Merke: - Bei jeder Aufgabe wird wie gelernt nicht nur das Endresultat, sondern auch die **Vollständigkeit** des Lösungsweges und die **Klarheit, Sauberkeit und Normeinhaltung** bewertet.
- Falls Sie Lösungsteile von einer Ausgabe auf Ihre BYOD lösten, speichern Sie schlussendlich dieses File mit dem Namen 'INF22xL A2 IhrName_IhrVornae.pdf' bzw. wenn Sie diese Arbeiten in einer 2er-Grupper erledigten 'INF22xL A2 Name1_Name2.pdf' unter dem bei Teams geöffneten Arbeit '23-11-24 M114 A2 Daten, Kompression, Reduktion' ab.

Maximal: 32 Punkte

Fach: M114	Thema: Daten, Kompression, Reduktion (B5..B8!)	Punkte: 30	INF22xL	Note: 6.0
-------------------	---	-------------------	---------	------------------

M114 Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Berufsbildungszentrum
Wirtschaft, Informatik und Technik

bbzw.lu.ch

Rückblick

* Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!

→ Vektorengrafiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
- Lernziele und Materialien sind klar!

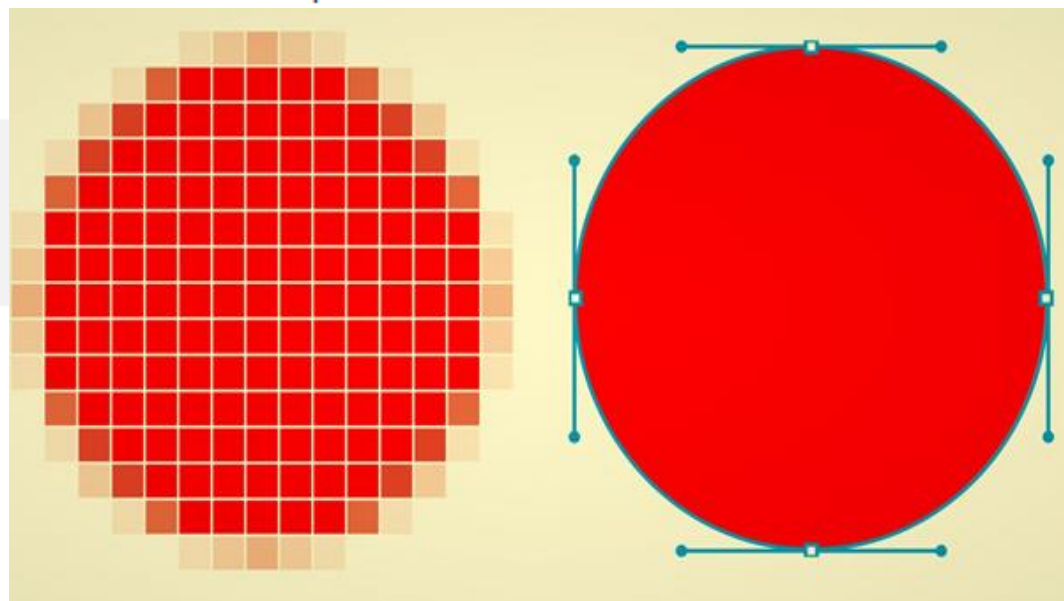
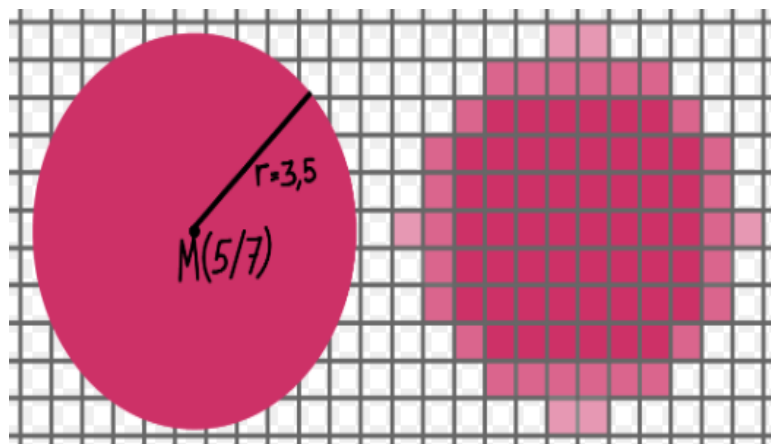
Lernziele zu dieser Lerneinheit

Ich kann...

- Den Unterschied zwischen Bitmap- und Vektorgrafiken erklären.
- Darlegen, wie SVG-Grafiken aus Scripts aufgebaut werden.
- Selber einfache Grafiken in Form eine SVG-Scripts erstellen.

Materialien

- 📄 Präsentation "Vektorgrafiken"
- 📄 Aufgaben "Vektorgrafiken"
- 📄 Musterlösungen



Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
 - * Vektorengragiken wurde erarbeitet! → Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?
 - Lernziele und Materialien sind klar!
- Der andere Ansatz erkennen! → Vektorgrafik statt Pixel!

Bild	Zeile Nr.	Bitwerte	Hexadezimalwerte
	1	0000 0000 0000 0000	0x0000
	2	0000 0001 0000 0000	0x0100
	3	0000 0010 1000 0000	0x0280
	4	0000 0100 0100 0000	0x0440
	5	0000 1000 0010 0000	0x0820
	6	0001 0000 0001 0000	0x1010
	7	0010 0000 0000 1000	0x2008
	8	0100 0000 0000 0100	0x4004
	9	1000 0000 0000 0010	0x8002
	10	0100 0000 0000 0100	0x4004
	11	0010 0000 0000 1000	0x2008
	12	0001 0000 0001 0000	0x1010
	13	0000 1000 0010 0000	0x0820
	14	0000 0100 0100 0000	0x0440
	15	0000 0010 1000 0000	0x0280
	16	0000 0001 0000 0000	0x0100

In Abbildung oben sehen wir, dass die SVG-Grafiken in einem html-ähnlichen Code definiert werden:

- Mit dem **svg-Tag** wird eine Zeichnungsfläche mit Koordinatensystem definiert. Der Ursprung des Koordinatensystems befindet sich dabei oben links.
- Der Befehl **path** eröffnet einen Linienstrang, **d** setzt den Zeichenstift aufs "Papier", **M** bewegt den Cursor zum Startpunkt und **L** zieht die gerade Linie zum nächsten Punkt.
- Mit **fill** wird gewählt, ob und mit welcher Farbe die Zeichnung gefüllt werden soll, **stroke** wählt die Stift-Farbe aus.
- Mit dem **/svg**-Tag wird die Zeichnung abgeschlossen.

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
 - * Vektorengrafiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Lernziele und Materialien sind klar!
 - Der andere Ansatz erkennen! → *Vektorgrafik statt Pixel!*
- Vorteile von vektorbasierten Grafiken erkennen! → *Skalierbarkeit, Dateigrösse*



Dateigrösse

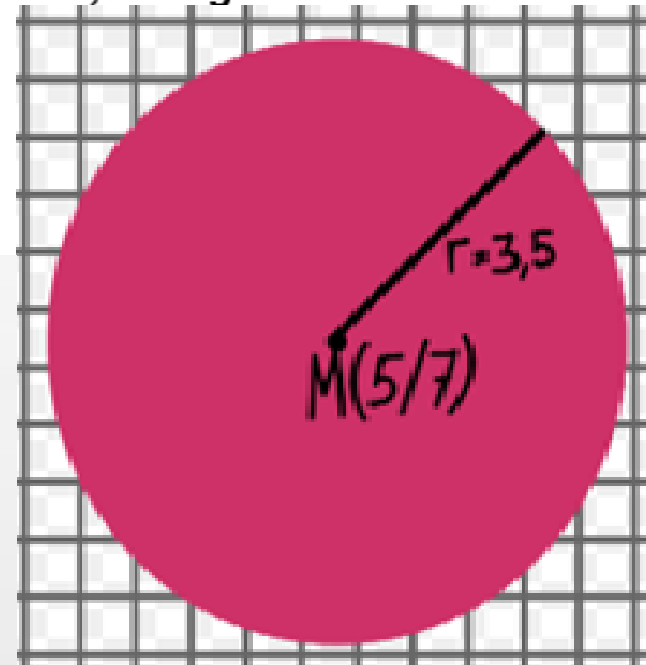
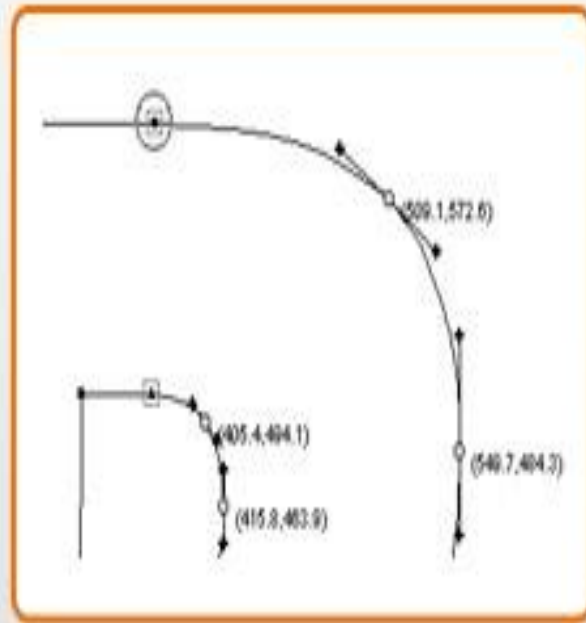
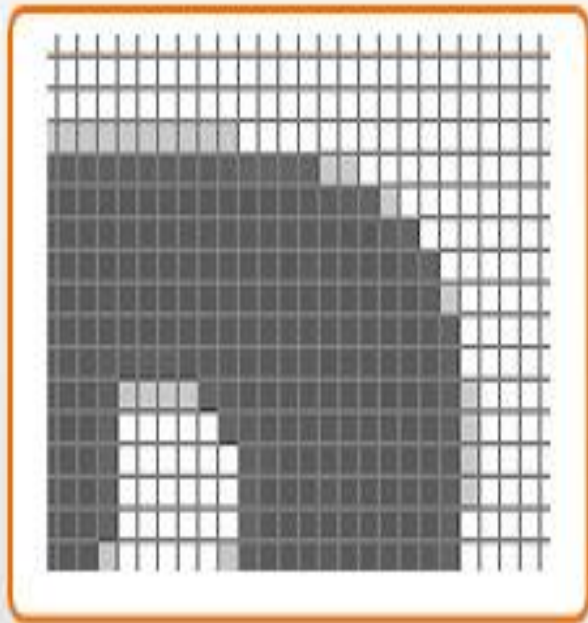
Je nach Komplexität der Grafik sind die SVG-Textfiles sehr viel kleiner, als die komplette Rastergrafik.

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Lernziele und Materialien sind klar!
 - Der andere Ansatz erkennen! → *Vektorgrafik statt Pixel!*
 - Vorteile von vektorbasierten Grafiken erkennen! → *Skalierbarkeit, Dateigrösse*
 - Nachteile von vektorbasierten Grafiken kennen!

Vektorbasierte Grafiken eignen sich für Darstellungen im Sinne von "Zeichnungen", Plänen, Logos.

Für komplexere Bilder mit unklaren Konturen und/oder grosser Farbvielfalt sind sie nicht geeignet.



Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
 - * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Lernziele und Materialien sind klar!
 - Der andere Ansatz erkennen! → *Vektorgrafik statt Pixel!*
 - Vorteile von vektorbasierten Grafiken erkennen! → *Skalierbarkeit, Dateigrösse*
 - Nachteile von vektorbasierten Grafiken kennen!
- Hinweis auf zusätzliches Lernmaterial!

⇒ [SVG Tutorial und Online-Editor](#)

What is SVG?

- SVG stands for Scalable Vector Graphics
- SVG is used to define vector-based graphics for the Web
- SVG defines the graphics in XML format
- Every element and every attribute in SVG files can be animated
- SVG is a W3C recommendation
- SVG integrates with other W3C standards such as the DOM and XSL

Rückblick

* Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!

* Vektorengrafiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*

- Lernziele und Materialien sind klar!
- Der andere Ansatz erkennen! → *Vektorgrafik statt Pixel!*
- Vorteile von vektorbasierten Grafiken erkennen! → *Skalierbarkeit, Dateigrösse*
- Nachteile von vektorbasierten Grafiken kennen!
- Hinweis auf zusätzliches Lernmaterial!

→ Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Sie lösen die folgenden 6 Aufgaben 9.1 bis 9.5 und mindestens die Zusatzaufgaben und melden alle Ihre Probleme bzw. Unklarheiten spätestens bei der Besprechung!

Aufgabe 9.1: SVG-Editor installieren

Installieren Sie die Software «Scribus» (Modulunterlagen) auf Ihren vmWP1

Aufgabe 9.2: Ein einfaches SVG-Script analysieren

Öffnen Sie die Datei «SVG-Beispiel.txt» (Modul-Share) im Editor.

Analysieren Sie den Code. Wie müsste die Zeichnung als Bild aussehen?

Aufgabe 9.3: Ein einfaches SVG-Script erstellen

Speichern Sie die Datei SVG-Beispiel aus dem Editor unter der Dateiendung .svg.

Öffnen Sie nun «SVG-Beispiel.svg» in Scribus und überprüfen Sie Ihre Vermutungen aus Aufgabe 9.2.

Ergänzen Sie das Script nun so, dass es nebenstehendes Smiley abbildet.

Hilfe dazu finden Sie im Dokument «SVG Path».



Aufgabe 9.4: Bézier-Kurven

Etwas komplizierter wird es, wenn wir das Smiley lächeln lassen wollen.

Experimentieren Sie dazu mit Hilfe der Anleitung «SVG Path».

Im schlimmsten Fall finden Sie weitere Hilfe in den Musterlösungen.



Aufgabe 9.5: Eigenschaften von Vektorgrafiken

Zeichnen Sie nun direkt in Scribus Ihr eigenes Logo. Die Bedienung der Software ist etwas gewöhnungsbedürftig. Exportieren Sie nun Ihr Logo sowohl als BMP wie auch als SVG-Datei. Welchen Unterschied stellen Sie punkto Speicherplatz fest? Begründung?

Zusatzaufgabe für Interessierte:

Kreativität Lassen Sie Ihrer Kreativität freien Lauf und experimentieren Sie weiter 😊

Zum Vergleichen mit Ihren Lösungen finden Sie wie immer auf Teams Musterlösungen!

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse*
- * Symmetrische und asymmetrische Verschlüsselung, als auch Hybridverfahren kennen!
- * Hinweise auf zusätzliches Lernmaterial geben!



10 Verschlüsselung – Geschichte und Grundsätzliche...

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → *Block 10: Verschlüsselung – Geschichte und Grundsätzliches*

→ Definierte Lernziele und vorhandene Materialien erläutern!

Lernziele zu dieser Lerneinheit

- Ich kann...
- Den Begriff «Steganographie» erklären.
 - Exemplarisch monoalphabetische Chiffren dechiffrieren.
 - Den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung erklären.

Materialien

- 📄 Präsentation "Verschlüsselung 1"
- 📄 Aufgaben "Verschlüsselung 1"
- 📄 Musterlösungen

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*

Vertraulichkeit (Confidentiality)

Die Informationen können von Unbefugten nicht eingesehen werden (wird erreicht durch eine sichere **Verschlüsselung**).

Integrität (Integrity)

Die Informationen sind unverfälscht und vollständig (wird erreicht durch eine gute **Hash-Funktion**).

Authentizität (Authenticity)

Sender und Empfänger sind einander klar bekannt (wird erreicht mit einer guten Funktion für **digitale Signatur**).

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- **Steganographie definieren!** → *Siehe beispielsweise Wikipedia!*

Die Steganographie (auch Steganografie) ist die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container).

Kurz gesagt geht es also um das Verstecken von Informationen. Als "Schlüssel" braucht der Empfänger dann nur noch die Anleitung zum auffinden der Information, während Dritte bei der Betrachtung des Trägermediums keinen Verdacht schöpfen (sollten).

Einige Beispiele für das Verstecken von Informationen sind:

- Text in Text
- Bilder in Bildern
- First Letter Messages
- Bitströme in Dateien
- Skytalen (Abbildung unten)



Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*

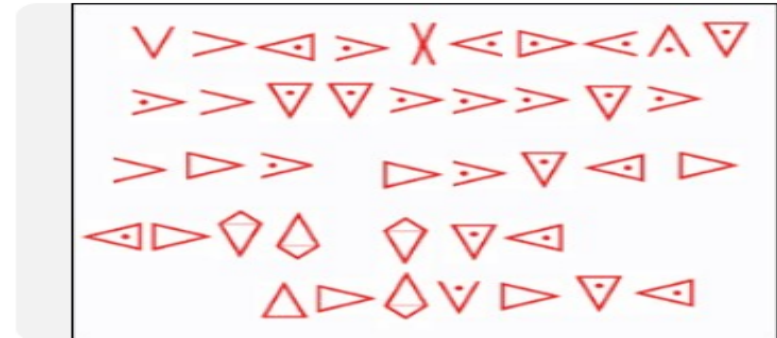
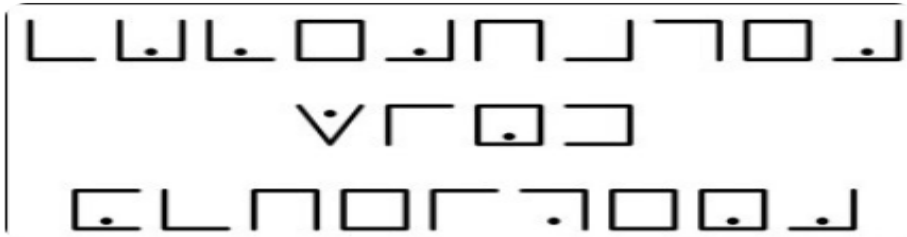
→ **Geschichte der Verschlüsselung kennen!** → *Monoalphabetische-Chiffren,*

Die Verschlüsselung ist wahrscheinlich fast ebenso alt, wie die Schrift.

Über lange Zeit hinweg scheint dabei die **monoalphabetische Chiffrierung** genügend sicher gewesen zu sein.

Typisch für diese Art der Verschlüsselung ist, dass für jeden Buchstaben des Alphabets **genau ein Zeichen** der Geheimschrift verwendet wird - und zwar immer dasselbe.

Zwei Beispiele solcher Geheimschriften sehen wir unten. Die linke Abbildung zeigt einen Text in der sogenannten Freimaurer-Chiffre, diejenige rechts in der Tempelritter-Chiffre:



Im Arbeitsblatt zu dieser Lerneinheit können Sie sich eingehender mit diesen Geheimschriften auseinandersetzen.

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*

→ **Geschichte der Verschlüsselung kennen!** → *Monoalphabetische- und Ceasar-Chiffren*, ←

Die bekannteste monoalphabetische Chiffre ist die Caesar-Chiffre.

Die Buchstaben eines Textes werden dabei einfach um eine bestimmte Anzahl Stellen im Alphabet verschoben.

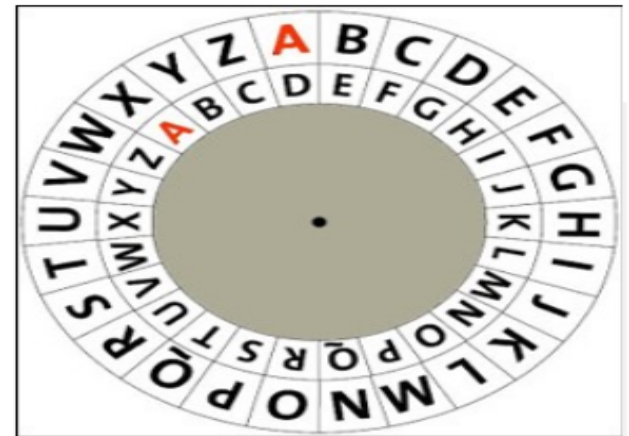
Der Schlüssel ist dann derjenige Buchstabe, der angibt, um wie viele Stellen geschoben wurde (A: keine Verschiebung, B: Verschiebung um eine Stelle, C: Verschiebung um zwei Stellen, und so weiter).

In den Abbildungen unten sehen Sie ein Beispiel und die sogenannte Caesar-Scheibe, deren innerer Ring drehbar ist, damit man den Schlüsselbuchstaben unter "A" drehen kann und so eine einfache Verschlüsselungshilfe erhält.

DAS IST STRENG GEHEIM

GDV LVW VWUHQJ JHKHLP

(Verschlüsselt mit Schlüssel «3» oder «D»)

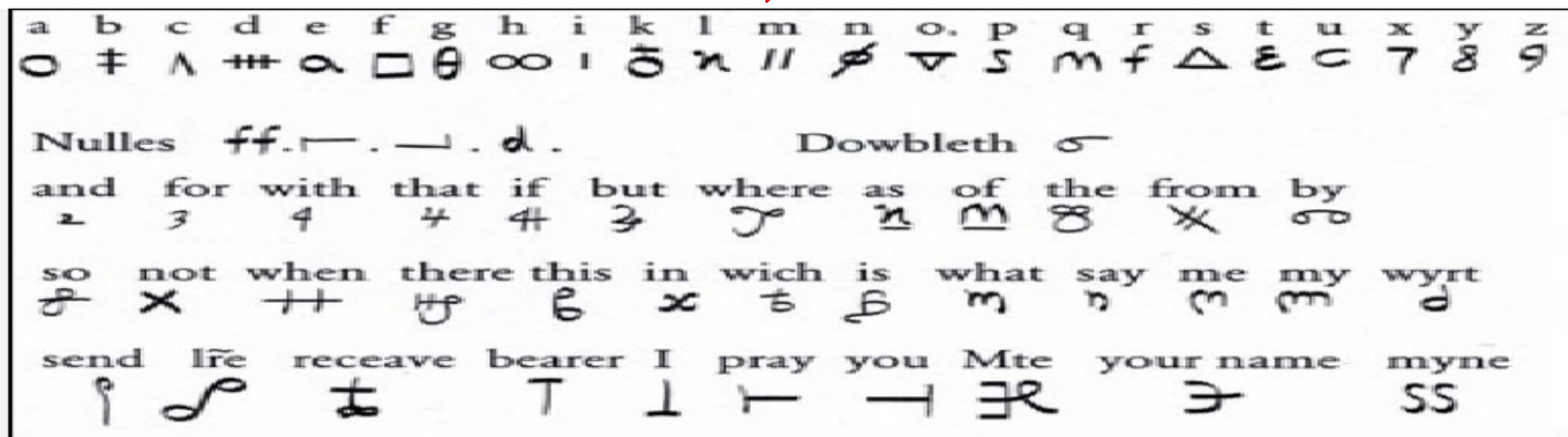


Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren,*
→ *Geheimschrift der Mary Stuart,*



Um es den Dechiffrierern schwieriger zu machen, wurden folgende Hürden eingebaut:

- Zeichen ohne Bedeutung
- Zeichen, dass der folgende Buchstabe doppelt kommt (Dowbleth)
- Eigene Zeichen für häufig vorkommende Wörter

Letztlich half dies Mary Stuart aber auch nicht weiter. Wie alle monoalphabetischen Chiffren wurde auch die Ihre geknackt und sie wurde wegen Verschwörung hingerichtet...

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse* ←

Der Begriff **Kryptoanalyse** meint das "knacken" von Verschlüsselungen.

Das ist bei monoalphabetischen Chiffren meistens sehr einfach: Sobald man weiss, in welcher Sprache der Geheimtext geschrieben wurde, kann man sich der Buchstabenhäufigkeit bedienen. Praktisch jede Sprache hat diesbezüglich einen eigenen "Fingerabdruck".



Rückblick

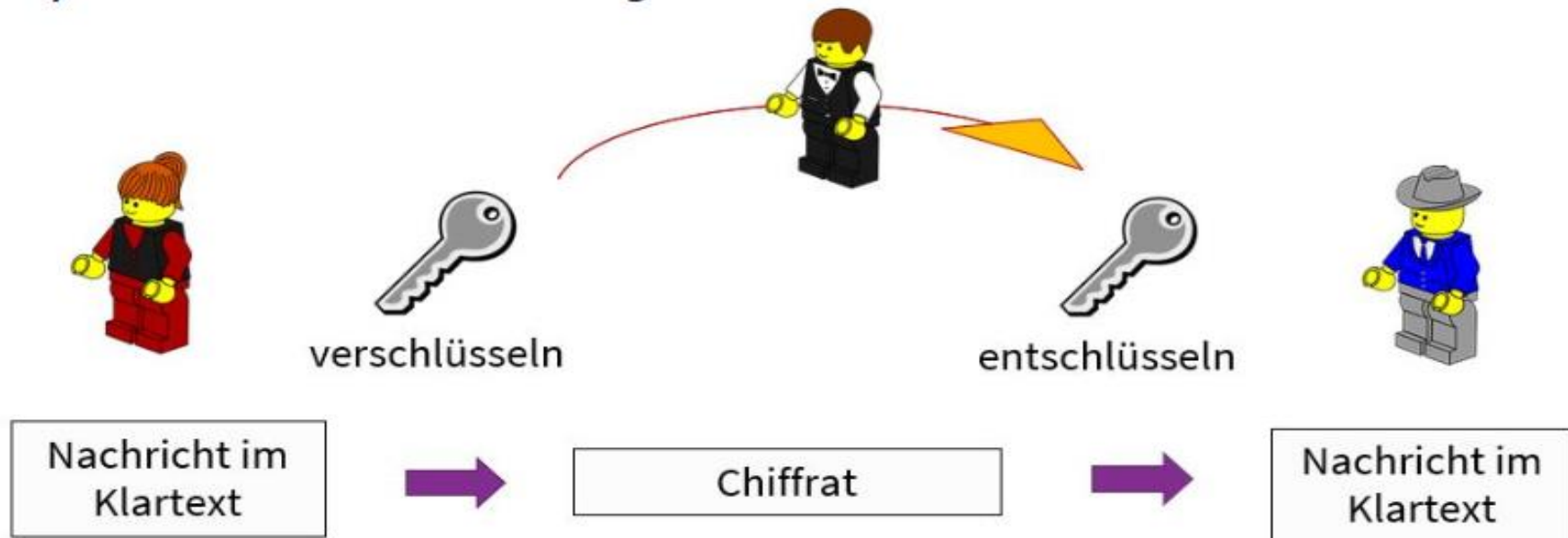
- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse*

→ Symmetrische Verschlüsselung

Weil sowohl Sender als auch Empfänger denselben Schlüssel verwenden, spricht man von **symmetrischer Verschlüsselung**.



Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengraphiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse*

→ Symmetrische und asymmetrische Verschlüsselung

Es reicht also für sicheren Nachrichtenaustausch, wenn jeder Teilnehmer seinen Public Key veröffentlicht und sehr gut auf seinen Private Key aufpasst.

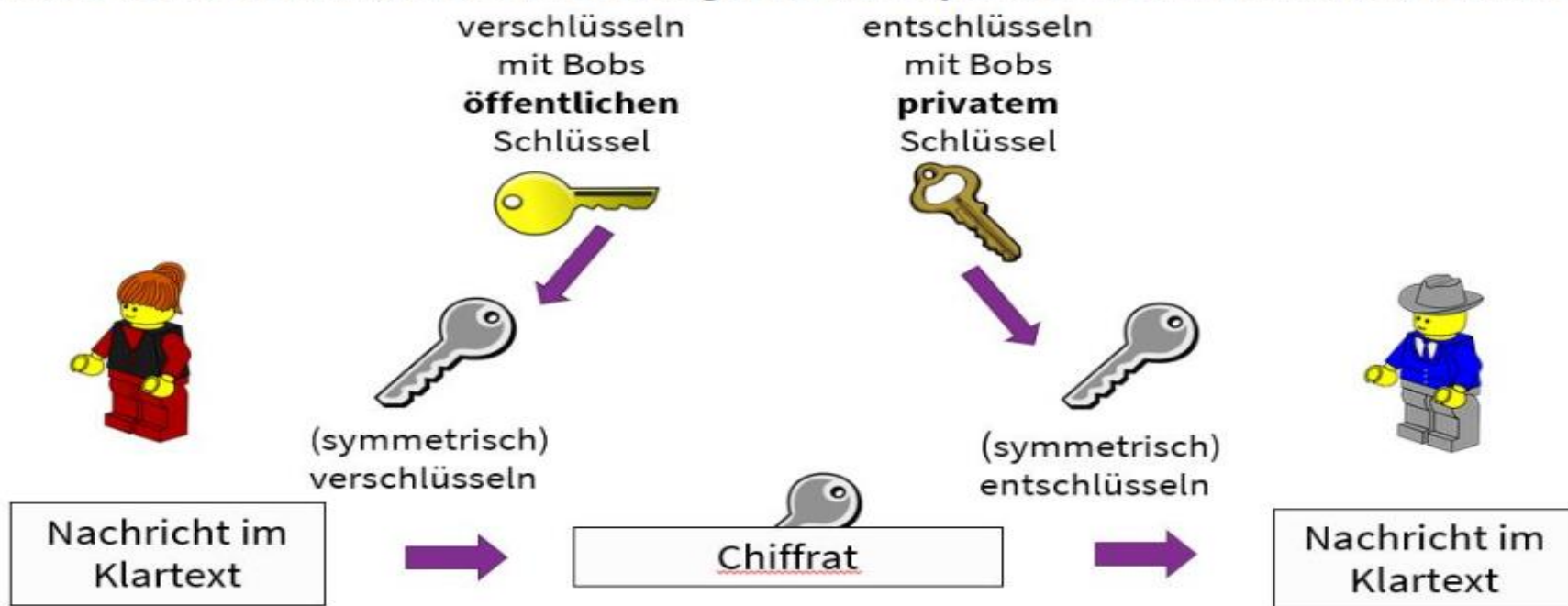


Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse*
- * **Symmetrische und asymmetrische Verschlüsselung, als auch Hybridverfahren kennen!** ←
- Deshalb versucht man, beide Arten in sogenannten **hybriden Verfahren** zu kombinieren:



Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
 - * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
 - * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
 - * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse*
 - * Symmetrische und asymmetrische Verschlüsselung, als auch Hybridverfahren kennen!
- Hinweise auf zusätzliches Lernmaterial geben!

Zusätzliches Lernmaterial

↪ [Video zur Caesar-Verschlüsselung](#)

↪ [Buchempfehlung "Geheime Botschaften"](#)

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen!
- * Vektorengragiken wurde erarbeitet! → *Probleme bzw. Fragen zum Inhalt bzw. zu den Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren, Geheimschrift der Mary Stuart, Kryptoanalyse*
- * Symmetrische und asymmetrische Verschlüsselung, als auch Hybridverfahren kennen!
- * Hinweise auf zusätzliches Lernmaterial geben!

Übungen bzw. Aufgaben

- * Persönlich gelöste und besprochene 2. Arbeit zu Unterrichtsblock 05..08 korrigieren!

→ Block 10 "Verschlüsselung – Geschichte und Grundsätzliches" wird persönlich erarbeitet und vorhandene Fragen bzw. Unklarheiten werden notiert bzw. gemeldet und die 5 Aufgaben dazu werden sauber und vollständig gelöst!



**10 Verschlüsselung –
Geschichte und
Grundsätzliche...**

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen → *Merke, Vorgehen, Ablauf, Bewertung, Hilfen*
- * Vektorengrafiken wurde erarbeitet! → *B09: Probleme bzw. Fragen zu Inhalt und Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren,...*
- * Symmetrische und asymmetrische Verschlüsselung, als auch Hybridverfahren kennen!
- * Hinweise auf zusätzliches Lernmaterial geben!

Übungen bzw. Aufgaben

- * Persönlich gelöste und besprochene 2. Arbeit zu Unterrichtsblock 05..08 korrigieren!
- * Block 10 "Verschlüsselung – Geschichte und Grundsätzliches" wird persönlich erarbeitet und vorhandene Fragen bzw. Unklarheiten werden notiert bzw. gemeldet und die 5 Aufgaben dazu werden sauber und vollständig gelöst!

Ausblick

→ Fr. 15. Dez.: - Verschlüsselungsverfahren erkennen → *B11*



**11 Verschlüsselung -
Moderne Verfahren**

Rückblick

- * Bewertung Ihrer gelösten fünf Arbeiten zu Unterrichtsblock B05 Datenübertragung, B06 Dateien, B07 Kompression und B08 Reduktion besprechen → *Merke, Vorgehen, Ablauf, Bewertung, Hilfen*
- * Vektorengrafiken wurde erarbeitet! → *B09: Probleme bzw. Fragen zu Inhalt und Aufträgen?*
 - Die 5 Aufgaben wurden erledigt! → *Fragen, Unklarheiten, Probleme?*

Stoff → Block 10: Verschlüsselung – Geschichte und Grundsätzliches

- * Definierte Lernziele und vorhandene Materialien erläutern!
- * Ziele beim Schutz von Informationen definieren! → *Vertraulichkeit, Integrität, Authentizität*
- * Steganographie definieren! → *Siehe beispielsweise Wikipedia!*
- * Geschichte der Verschlüsselung kennen! → *Monoalphabetische- und Ceasar-Chiffren,...*
- * Symmetrische und asymmetrische Verschlüsselung, als auch Hybridverfahren kennen!
- * Hinweise auf zusätzliches Lernmaterial geben!

Übungen bzw. Aufgaben

- Persönlich gelöste und besprochene 2. Arbeit zu Unterrichtsblock 05..08 korrigieren!
- Block 10 "Verschlüsselung – Geschichte und Grundsätzliches" wird persönlich erarbeitet und vorhandene Fragen bzw. Unklarheiten werden notiert bzw. gemeldet und die 5 Aufgaben dazu werden sauber und vollständig gelöst!

Ausblick

- Fr. 15. Dez.: - Verschlüsselungsverfahren erkennen → *B11*
- Fr. 22. Dez.: - Rückblickarbeiten erledigen → *B09..11 (A3)*
Weihnachtsferien
- Fr. 12. Jan.: - Kryptographie und Seganographie definieren und anwenden → *B12*
- Fr. 19. Jan.: - Arbeiten zu den erarbeiten M114-Modulidentifikationen! → *B1..B12*
- Fr. 26. Jan.: - Arbeiten zu den erarbeiten M114-Modulidentifikationen! → *B1..B12*
 - Modul 114 abschliessen

Freitag:	KW	SW	Themen (Theorie und Übungen)	Stoffplan
25.08.2023	34	01	00 Begrüssung und Einleitung 01 Die Zahlensysteme BIN, HEX und DEZ kennenlernen	
01.09.2023	35	02	02 Arithmetische und logische Grundoperationen binär	
08.09.2023	36	03	Rückblickübungen zu Block 01 und 02 lösen	
15.09.2023	37	04	03 Die Logik und den Prozessor verstehen	
22.09.2023	38	05	Prüfung Block 01 und 02 04 Grosse Zahlen in kleinen Variablen ablegen, wie geht das?	P1
29.09.2023	39	06	Rückblickübungen zu Block 03 und 04 lösen	
			Herbstferien	
20.10.2023	42	07	05 Fehler in der Datenübertragung finden und korrigieren	
27.10.2023	43	08	Arbeit zu Block 02 bis und mit 04 schreiben	A1
03.11.2023	44	09	06 Speicherplatz als rares Gut – Dateien und ihr Platzbedarf	
10.11.2023	45	10	07 Speicherplatz als rares Gut – Dateien und ihr Platzbedarf, Kompression	
17.11.2023	46	11	08 Speicherplatz als rares Gut – Reduktion	
24.11.2023	47	12	Arbeit zu Block 06 bis und mit Block 08 schreiben 09 Vektorgrafiken – Eine Alternative zu den Pixeln	A2
01.12.2023	48	13	10 Verschlüsselung – Geschichte und Grundsätzliches	
08.12.2023	49	14	Maria Empfängnis	
15.12.2023	50	15	11 Verschlüsselung – Moderne Verfahren	
22.12.2023	51	16	Arbeit zu Block 09 bis und mit Block 11 schreiben	A3
			Weihnachtsferien	
12.01.2024	02	17	12 Kryptographie und Steganographie definieren und anwenden	
19.01.2024	03	18	Rückblickübungen über erarbeitete M114-Themen lösen	
26.01.2024	04	19	Rückblickübungen über erarbeitete M114-Themen abschliessen Modul abschliessen	