

Das geheimnisvolle Krypteum

***Ein durch MS Teams begleiteter mebis-Kurs für den
Distanz- oder den digital gestützten Präsenzunterricht im
Lernfeld 9 der technischen IT-Berufe***

**Praktische Prüfung Mediengestaltung
im
Erweiterungsstudiengang Medienpädagogik
am**

13. Oktober 2022

Christian Endres

Agenda

1. Planung und Konzeption des Praxisprojekts
2. Aufbau und Inhalt des mebis-Kurses „Das geheimnisvolle Krypteum“
3. Einsatz des mebis-Kurses im Fachunterricht der Klasse IFA11A
4. Evaluation und Reflexion des durchgeführten Unterrichts

Agenda

1. Planung und Konzeption des Praxisprojekts

2. Aufbau und Inhalt des mebis-Kurses „Das geheimnisvolle Krypteum“

3. Einsatz des mebis-Kurses im Fachunterricht der Klasse IFA11A

4. Evaluation und Reflexion des durchgeführten Unterrichts

Überblick

1. Kryptologie ist **theorielastig** und mathematisch anspruchsvoll
2. Spielerische Vermittlung **abstrakter** kryptographischer Grundlagen hilft beim Verständnis weiterführender netzwerktechnischer Inhalte
3. Motivation durch „**konkurrierende**“ Arbeitstandems
4. Kursgestaltung als einfacher **eduBreakout**
5. Digitale **Kursbegleitung** durch Kollaborations-SW MS Teams

mebis-Lernplattform

Bedingtes Fortkommen
(positive **Verstärkung**,
Wiederholung und
Sicherung)

Flexibilität bei Lernort und Lernzeit
(digital gestützter **Präsenzunterricht**,
asynchroner/synchroner
Distanzunterricht)

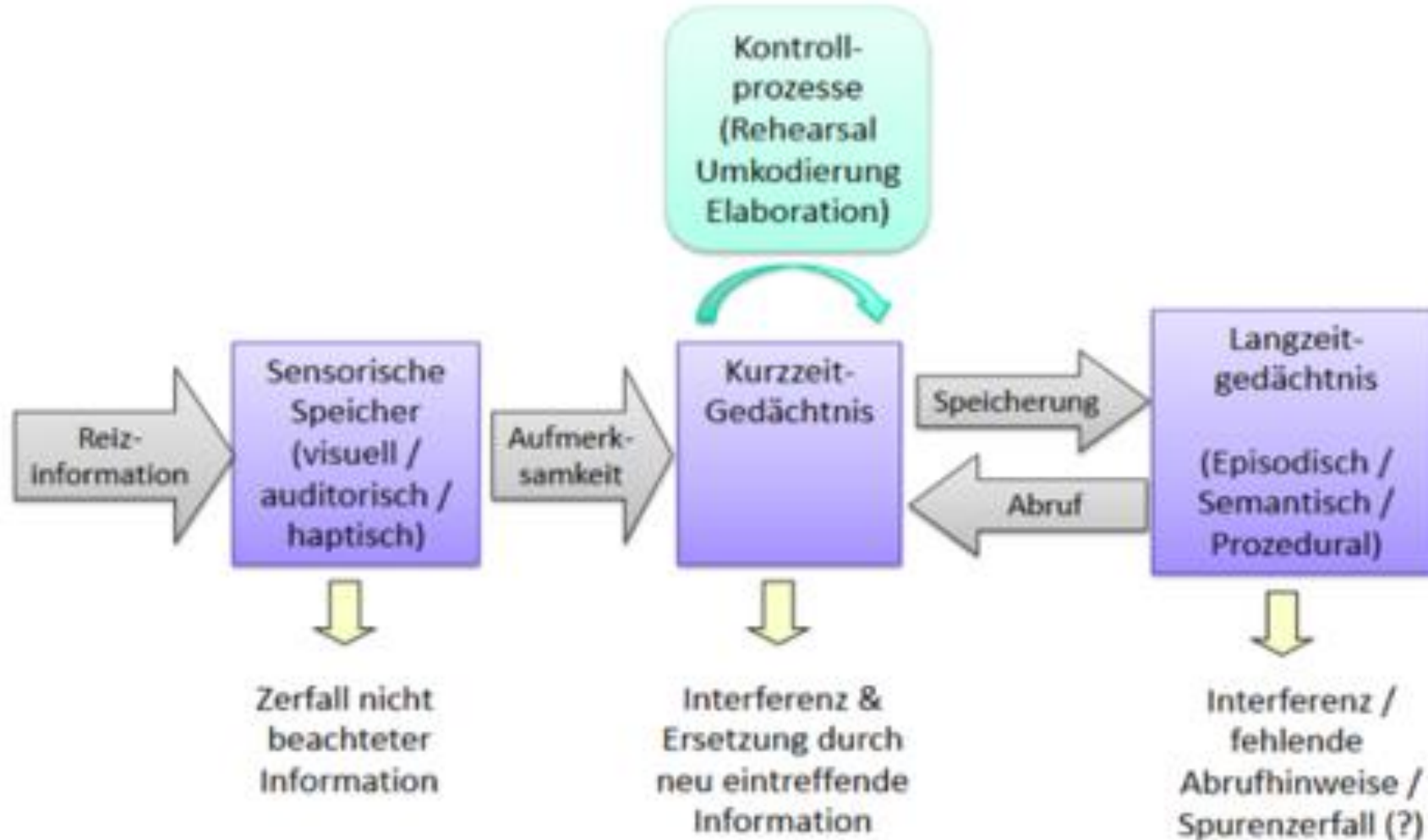
Anschaulichkeit durch
Multimedia
(**Erklärvideos, Simulationen**)

Selbststeuerung
(kontinuierliches **Feedback**,
eigenständige **Navigation**)

Behavioristisches E-Learning
(operantes Konditionieren
nach **B.F. Skinner**, digitale
Programmierte Unterweisung)

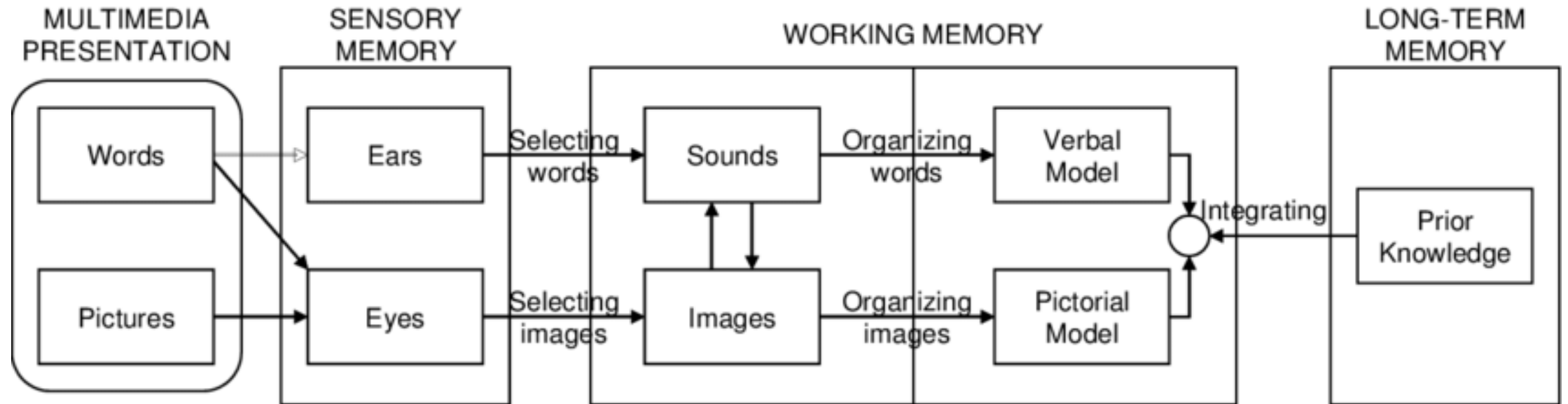
Lernmotivation
(**Storytelling, Competition**)

Kursgestaltung – 3-Speicher-Modell



Atkinson & Shiffrin,
1968

Kursgestaltung – CTML



Mayer, 2001

Kursgestaltungsprinzipien (Mayer)

Multimediaprinzip

Kombination von Grafik und Text

Kontiguitätsprinzip

Räumlich zusammenhängende
Präsentation

Kohärenzprinzip

Weglassen irrelevanter /
dekorativer Elemente

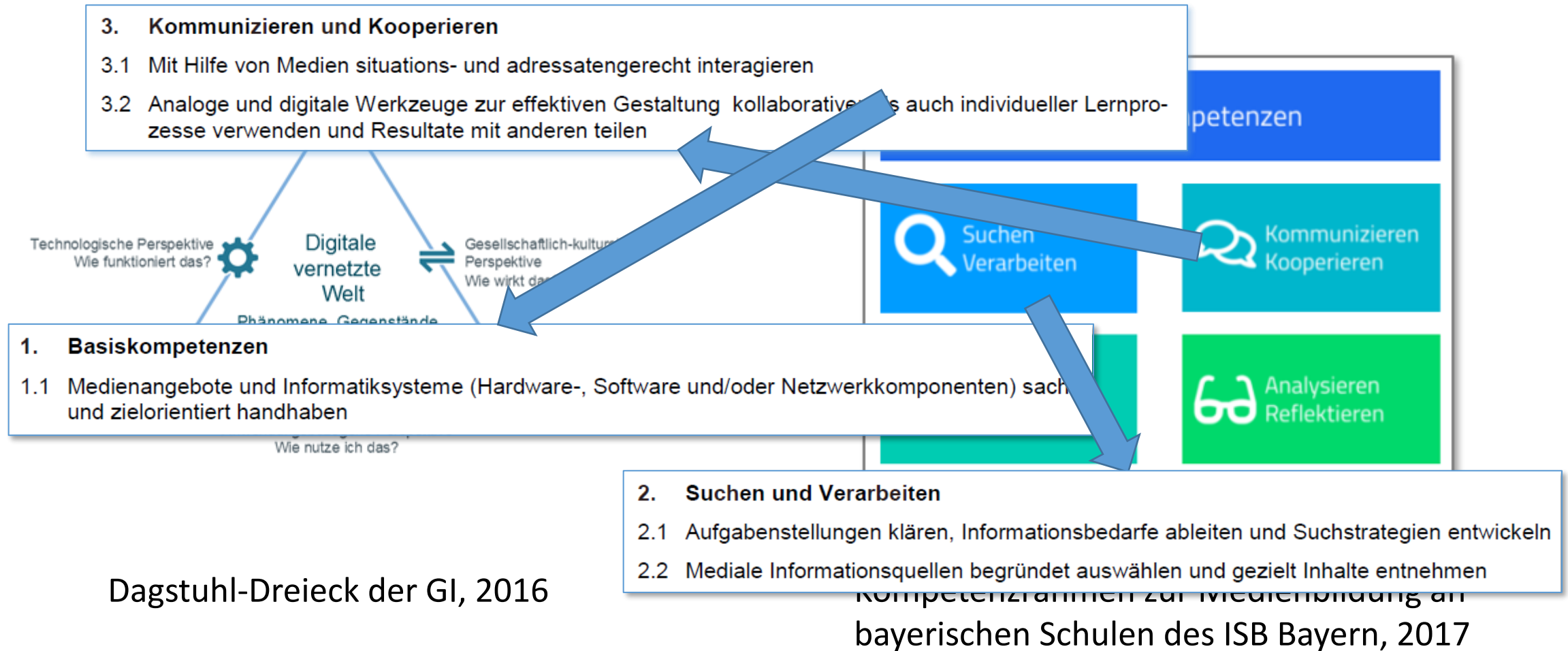
Hinweisprinzip

Hervorhebung zentraler
Informationen

Gamification Lite

1. eduBreakout als **schulische** Variante kommerzieller **Escape-Rooms**
2. Fortkommen im Kurs von Lösung kleiner Aufgaben und Rätsel abhängig (**mebis-Aktivität „Test“**)
3. Game-based-Learning kann **Motivation** zur Bearbeitung sperriger Unterrichtsinhalte sein
4. Story-Telling **zwingt** zur Auseinandersetzung mit **abstrakten** Lerninhalten
5. Instruktives **Coaching** gamifizierter Lernsettings durch Lehrkraft lernförderlich
6. Lernerfolg durch **Teamgedanken** in **kompetitiver** Lernsituation

Medienkompetenzen



Lehrplanbezug

	Lernfeld 0	Netzwerke und Dienste bereitstellen	
Erweiterungsstudien Berufsbildung	Inhaltliche Orientierung Allgemein <ul style="list-style-type: none">• Dämpfung, Leitungsreflexion, Messungen, Durchgangsprüfung• VLAN, Access Control Lists, Segmentierung, Subnetting, CIDR• IPv6 (versus IPv4, Dual-Stack)• Transportprotokolle (Portnummern, TCP, UDP, SCTP)• Services (z.B. DHCP, DNS etc.)• Kryptographie (Verschlüsselung, Hashfunktionen etc.)• Autorisierung und Authentifizierung, Zertifikate (z.B. X.509)• VPN, IPsec, SSH, TLS• VoIP, QoS• LDAP• RADIUS, Zwei-Faktor-Authentifizierung		e zu
Sie be fremd die IT.	deren Infrastruktur und die Dienste hinsichtlich der gestellten Anforderungen, Datensicherheit und Datenschutz.		

Unterrichtseinsatz

1. Einsatzmöglichkeiten des mebis-Kurses sowohl im (angeordneten) **synchronen Distanzunterricht** als auch im **digital gestützten Präsenzunterricht**
2. Verankerung von Distanzunterricht in der didaktischen Jahresplanung bei **pädagogischem / didaktischem Mehrwert** mit Steigerung der Lerneffektivität
3. Rahmung durch eine Kollaborationsplattform wie MS Teams zur **digitalen Begleitung** der Kursdurchführung (Coaching, Informationsverteilung, Austausch der Kursteilnehmer*innen etc.)

Agenda

1. Planung und Konzeption des Praxisprojekts
- 2. Aufbau und Inhalt des mebis-Kurses „Das geheimnisvolle Krypteum“**
3. Einsatz des mebis-Kurses im Fachunterricht der Klasse IFA11A
4. Evaluation und Reflexion des durchgeführten Unterrichts

Fachliche Kursinhalte

Nomenklatur,
mathematische
Notation

Kryptologie,
Kryptographie,
Kryptanalyse

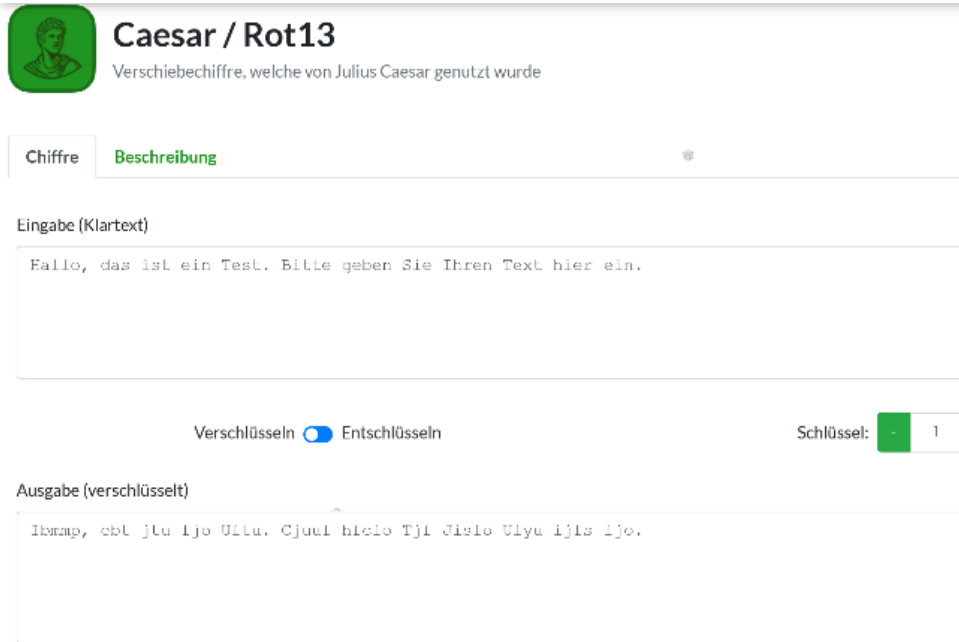
Klassische
Chiffren (Caesar,
Vigenère)

Symmetrische,
asymmetrische,
Hybridverschlüsselung

Hash-
funktionen

Digitale
Signatur

Das Simulationstool CrypTool



Caesar / Rot13
Verschiebechiffre, welche von Julius Caesar genutzt wurde

Chiffre **Beschreibung**


Eingabe (Klartext)
Hallo, das ist ein Test. Bitte geben Sie Ihren Text hier ein.

Verschlüsseln Entschlüsseln

Schlüssel: 1

Ausgabe (verschlüsselt)
Hkzmp, ebt jtu ljo Ullu. Cjuel hlclo Tji Jisio Ulyu ijls ljo.

Caesar-Chiffre in CrypTool-Online
<https://www.cryptool.org/de/cto/>



CrypTool 2.1 (Stable Build 9202.2) – caesar.cwm

Start Bearbeiten Kryptotutorien

Neu Öffnen Speichern Drucken Starten Stoppen Protokoll Startcenter CrypTool-Store CrypCloud Updates Einstellu

Komponenten

- Klassische Verfahren <<
- ADFGVX
- Caesar
- Chaocipher
- Enigma
- Fialka
- Klassische Verfahren
- Moderne Verfahren
- Steganografie
- Hash-Funktionen
- Kryptoanalyse
- Protokolle
- Werkzeuge

Texteingabe

HINTER DER LETZTEN TUER
DIESES MUSEUMS LIEGT EIN
SCHATZ VERBORGEN. GEHE MIT
DEM NEUNTEN WORT DIESER
INSCHRIFT AUF DIE SUCHE.

124 Zeichen, 1 Zeile
0%

Caesar

0%

Textausgabe

OPUALY KLY SLAGALU ABLY KPLZLZ
TBZLBTZ SPLNA LPU ZIOHAG CLIVYVNLU.
NLQL TPA KLT ULBUALLU DVVA KPLZLY
PUZJOYPMA HBM KPL ZBJOL.

124 Zeichen, 1 Zeile
0%

Caesar-Chiffre in CrypTool 2
<https://www.cryptool.org/de/ct2/>

mebis-Mehrthemenkurs

Blockchiffren

Eingeschränkt Nicht verfügbar, es sei denn: Die Aktivität **Weiter geht's, wenn Ihr diese Frage richtig beantwortet!** ist abgeschlossen und bestanden

Klasse! Alice und Bob sind auf ihrer Schatzsuche nicht mehr weit vom Ziel entfernt. Sie bekommen im nächsten Raum Informationen zu modernen Blockchiffren, bei deren Implementierung häufig die Boole'sche XOR-Operation zum Einsatz kommt.

Macht weiter wie bisher, löst die verbleibenden Aufgaben! Dann

Gebt hier das von Euch gefundene Schlüsselwort ein! Dann geht's weiter!

Operator



XOR-Operation



DE:

Mit Cryptool-Online könnt Ihr die Funktionsweise von AES anhand Auch die unterschiedlichen Betriebsarten wie ECB oder CBC kö

Hier ist der Link, um Euch mit AES vertraut zu machen:
<https://www.cryptool.org/de/cto/aes-step-by-step>

Frage 1

Bisher nicht beantwortet

Erreichbare Punkte: 10,00

Frage markieren

Frage bearbeiten

Wie lautet das Schlüsselwort?

Antwort:

Test-Navigation



Versuch abschließen ...

Neue Vorschau beginnen

Versuch abschließen ...

Kursgestaltung

Multimedia-
prinzip

Kohärenz-
prinzip

Hinweis-
prinzip

Kontiguitäts-
prinzip

Digitale Signatur

Unter der Voraussetzung, dass sowohl Alice als auch Bob die verwendeten Algorithmen für Hashing und Verschlüsselung kennen, läuft die digitale Signatur eines Dokuments unter Zuhilfenahme dessen kryptographischen Fingerabdrucks folgendermaßen ab:

1. Alice berechnet mit Hilfe einer Hash-Funktion (z.B. SHA-256) den **Hashwert des Dokuments M** : $f(M)$.
2. Alice **verschlüsselt den Hashwert $f(M)$** mit ihrem geheimen Schlüssel (z.B. RSA): $E_{SA}(f(M))$.
3. Alice sendet Klartext M und Hashwert-Chiffre an Bob.
4. Bob **entschlüsselt** den verschlüsselten Hashwert, $D_{PA}(E_{SA}(f(M)))$, und **berechnet selbst den Hashwert** von M .
5. Sind beide **Ergebnisse gleich**, ist Alice's Unterschrift **authentisch**.

Alice

Bob

$f(), PA$

$f(M); E_{SA}(f(M));$

$f(M) = D_{PA}(E_{SA}(f(M))) ?$

Agenda

1. Planung und Konzeption des Praxisprojekts
2. Aufbau und Inhalt des mebis-Kurses „Das geheimnisvolle Krypteum“
- 3. Einsatz des mebis-Kurses im Fachunterricht der Klasse IFA11A**
4. Evaluation und Reflexion des durchgeführten Unterrichts

Die Fachinformatiker-Klasse IFA11A

1. Fachklasse der 11. Jahrgangsstufe im Ausbildungsberuf **Fachinformatiker(in) (Fachrichtung: Anwendungsentwicklung)** an der Staatlichen Berufsschule Erlangen
2. 2 Schülerinnen und 22 Schüler im Alter von **17 bis 32** Jahren
3. Drei Ausbildungsbetriebe: **BA** (11 SuS) in Nürnberg, **ProLeit GmbH** (11 SuS) und **adidas AG** (2) in Herzogenaurach
→ Profunde Förderung der **Sozialkompetenz** der Azubis
4. Schulische Vorbildung: Überdurchschnittliche **mittlere Reife** (11), **Hochschulbefähigung** (13, davon 10 AH)
5. Drei bereits ältere, leistungsstarke Schülerinnen und Schüler mit **Flucht- oder Migrationshintergrund** mit sehr guten Deutschkenntnissen und Lebenserfahrung
6. 1 **schwerbehinderter** Schüler gut in die Klassengemeinschaft integriert
7. → **Kaum Störungen** des Unterrichts wegen fehlender Sozialkompetenz der Azubis bzw. notwendiger erzieherischer Maßnahmen

Unterrichtsablauf

1. Dauer: **4 Doppelstunden** inkl. Vorbereitung, Feedback und Nachbereitung (Anteil des Fachs IT-Systeme am Unterricht einer Blockwoche)
2. Unterrichtsraum: **iFU G056** an der Berufsschule Erlangen mit **SuS-Arbeitsplatzrechnern** sowie ticketgebundenes **WLAN (BYOD)**
3. Reibungslose Aufnahme der SuS in den mebis-Kurs (**BSA-Registrierung**) und Einteilung in **Tandems** zu Unterrichtsbeginn
4. Eigenständige paarweise Kursbearbeitung
5. Unterstützungsbedarf weniger bei fachlichen Fragestellungen als bei Unsicherheiten im Umgang mit der **mebis-Lernplattform** oder den verwendeten **digitalen Werkzeugen** wie CryptTool-Online
6. Nach Kursabschluss: Rekapitulation, Vertiefung, Ergebnissicherung auch im L-S-Gespräch
7. SuS-Feedback über **MS Forms-Abfrage** zu Lernmotivation, Lerneffizienz, Kursgestaltung und Sozialform



Agenda

1. Planung und Konzeption des Praxisprojekts
2. Aufbau und Inhalt des mebis-Kurses „Das geheimnisvolle Krypteum“
3. Einsatz des mebis-Kurses im Fachunterricht der Klasse IFA11A
- 4. Evaluation und Reflexion des durchgeführten Unterrichts**

Evaluation

1. Feedback der Auszubildenden über **MS Forms-Abfrage** (Auswertungs-Link):

[Krypteum SuS MS-Forms Feedback](#)

2. Fragen mit **Auswahloptionen**:

„Stimme voll zu“, „Stimme überwiegend zu“,
„Stimme teilweise zu“, „Stimme nicht zu“

3. Zusätzliche Kommentare, Lob, Kritik in **Freitextfeld**:

„Ich würde gerne noch anmerken, ...“

Fragen

Antworten 20

mebis-Kurs "Das geheimnisvolle Krypteum"

Bitte geben Sie anhand der folgenden Fragen ein Feedback zum mebis-Kurs "Das geheimnisvolle Krypteum" und Ihren damit einhergehenden Lernerfahrungen.

1. Der Kurs "Das geheimnisvolle Krypteum" war eine Abwechslung im Vergleich zum sonstigen Unterricht. *

- Stimme voll zu
- Stimme überwiegend zu
- Stimme teilweise zu
- Stimme nicht zu

Evaluation – Lernen mit mebis

1. Der Kurs "Das geheimnisvolle Krypteum" war eine Abwechslung im Vergleich zum sonstigen Unterricht.

● Stimme voll zu	16
● Stimme überwiegend zu	4
● Stimme teilweise zu	0
● Stimme nicht zu	0



9. Selbstgesteuertes Lernen über vorgefertigte Online-Kurse kann ich mir auch für andere Unterrichtsthemen vorstellen.

● Stimme voll zu	13
● Stimme überwiegend zu	7
● Stimme teilweise zu	0
● Stimme nicht zu	0



Evaluation - Gamification

2. Die Kursgestaltung als "Story" hat mich zur Bearbeitung des Inhalts motiviert.

● Stimme voll zu	5
● Stimme überwiegend zu	13
● Stimme teilweise zu	2
● Stimme nicht zu	0



3. Die spielerische Herangehensweise des Kurses hat mir das Erlernen der fachlichen Inhalte erleichtert.

● Stimme voll zu	10
● Stimme überwiegend zu	7
● Stimme teilweise zu	3
● Stimme nicht zu	0



4. Ich war mehr auf die Rätsel als auf den fachlichen Inhalt fokussiert.

● Stimme voll zu	4
● Stimme überwiegend zu	8
● Stimme teilweise zu	5
● Stimme nicht zu	3



Evaluation – Coaching/Sozialform

5. Für die Kursbearbeitung habe ich zusätzliche externe Webseiten benötigt (Google etc.).

● Stimme voll zu	9
● Stimme überwiegend zu	1
● Stimme teilweise zu	6
● Stimme nicht zu	4



8. Die Kursbearbeitung war im Wesentlichen ohne Unterstützung durch die Lehrkraft möglich.

● Stimme voll zu	8
● Stimme überwiegend zu	9
● Stimme teilweise zu	3
● Stimme nicht zu	0



7. Die Arbeit mit Partner(in) hat mich beim Erarbeiten der fachlichen Inhalte unterstützt.

● Stimme voll zu	16
● Stimme überwiegend zu	3
● Stimme teilweise zu	1
● Stimme nicht zu	0



Freitextantworten

1. *„... dass ich mir noch mehr praktische Rätsel gewünscht hätte.“*
2. *„Der Kurs ist inhaltlich interessant gestaltet. Die spielerische Herangehensweise erleichtert den Verständnis von komplexen Inhalten. Würde den Kurs gerne weiteren Mitschüler empfehlen. Diese Lernweise soll auch in anderen Unterrichten eingesetzt werden.“*
3. *„Es wäre gut, wenn Texte mit denen man Arbeiten muss kopierbar wären.“*

Fazit

1. Aufwändige Kurserstellung in Relation zur Dauer der Unterrichtseinheit
2. Aufwandsminderung durch **Kurspflege im LK-Team**
3. Vielfältige **Einsatzmöglichkeiten** des mebis-Kurses (RLFB, teachSHARE etc.)
4. **Kursoptimierung** anhand SuS-Feedback:
 - Ergänzendes **(Download-)Material** für Sicherung, Vertiefung, Übung
 - Zusätzliche **Offline-Plenumsphasen** zur Klärung von Fragen / Problemen
 - Integration weiterführender **Links** und Querverweise auf **Zusatzmaterial**
 - **Fachliche Erweiterung** der **Freischalt-Rätsel** des eduBreakouts

Quellenverzeichnis

1. BfJ [Bundesamt für Justiz] (2005). Berufsbildungsgesetz. Bonn: Kompetenzzentrum Rechtsinformationssystem des Bundes.
URL: https://www.gesetze-im-internet.de/bbig_2005/ [16. Februar 2022].
2. Cryptool Portal (2022). Cryptography for Everybody. Siegen: Institut für Wirtschaftsinformatik der Universität Siegen. URL: <https://www.cryptool.org/de/> [12. Januar 2022].
3. Endres, C. (2022). Das geheimnisvolle Krypteum. Erlangen: Staatl. BS Erlangen. URL: <https://lernplattform.mebis.bayern.de/course/view.php?id=1165681>,
Einschreibeschlüssel: **Krypteum**
4. GI [Gesellschaft für Informatik] (2016). Dagstuhl-Erklärung. Bildung in der digitalen vernetzten Welt. Berlin: Gesellschaft für Informatik.
URL: https://gi.de/fileadmin/GI/Hauptseite/Themen/Dagstuhl-Erklärung_2016-03-23.pdf [07. Januar 2022].
5. ISB [Staatsinstitut für Schulqualität und Bildungsforschung] (2020a). Berufsschule. Handreichung. Umsetzungshilfe für Lehrkräfte technischer IT-Ausbildungsberufe. München: ISB.
6. ISB [Staatsinstitut für Schulqualität und Bildungsforschung] (2020b). Lehrplanrichtlinien für die Berufsschule. Fachklassen Fachinformatiker/Fachinformatikerin. München: ISB
7. ISB – Referat Medienbildung (2017). Kompetenzrahmen zur Medienbildung an bayerischen Schulen. München: Staatsinstitut für Schulqualität und Bildungsforschung (ISB).
URL: <https://www.mebis.bayern.de/wp-content/uploads/sites/2/2017/03/Kompetenzrahmen-zur-Medienbildung-an-bayerischen-Schulen-1.pdf> [04. Januar 2022].
8. KMK [Kultusministerkonferenz] (2018). Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz. Berlin: Sekretariat der Kultusministerkonferenz.
URL: https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf [07. Januar 2022]
9. Mayer, R.E. (2015). Cognitive Theory of Multimedia Learning. in: Mayer, R.E. (Hrsg.): The Cambridge Handbook of Multimedia Learning. Cambridge: Cambridge University Press
10. mebis-Redaktion (2021). DigCompEdu Bavaria – Digitale und medienbezogene Lehrkompetenzen. in: mebis – Landesmedienzentrum Bayern.
URL: <https://www.mebis.bayern.de/p/71502> [04. Januar 2022].
11. Nieding, G., Ohler, P. & Rey, G.D. (2015). Lernen mit Medien. Paderborn: Ferdinand Schöningh
12. Schaumburg, H. & Prasse, D. (2019). Medien und Schule. Bad Heilbrunn: Verlag Julius Klinkhardt.
13. StMUK [Bayerisches Staatsministerium für Unterricht und Kultus] (2020). Lehrplanrichtlinien für die Berufsschule. Fachklassen Fachinformatiker/Fachinformatikerin. München: Staatsinstitut für Schulqualität und Bildungsforschung (ISB).
14. StMUK [Bayerisches Staatsministerium für Unterricht und Kultus] (2021). KMS. Distanzunterricht in Zeiten des Präsenzunterrichts. München.
15. StMUK [Bayerisches Staatsministerium für Unterricht und Kultus] (2022). mebis, Landesmedienzentrum Bayern. URL: <https://www.mebis.bayern.de> [05. Januar 2022].
16. Tulodziecki, G., Herzig, B. & Grafe, S. (2021). Medienbildung in Schule und Unterricht. Bad Heilbrunn: Verlag Julius Klinkhardt.