



Westfälische Wilhelms-Universität Münster

Institut der Didaktik für Mathematik und Informatik

Arbeitsbereich Didaktik der Informatik

Wintersemester 2016/2017

Digitale Medien und Informatische Bildung (DigiMed)

Dozent: Marco Thomas und Alexander Best

schriftliche Arbeit im Fach Informatik

- Kryptologie -

Birte Dieckmeyer



Master of Education (MEd) für das Lehramt an Grundschulen

1. Fachsemester

I. Inhaltsverzeichnis

Vorlage / Langentwurf / Unterrichtsstunde

Schriftliche Planung des Unterrichts

1. Ziele und angestrebte Kompetenzen.....	1
2. Didaktische Schwerpunkte	2
3. Geplanter Verlauf des Unterrichts	9
4. Artikulationsschema/ Synopse	11

Literaturverzeichnis.....	13
---------------------------	----

II. Anhang

Folie für den OHP.....	15
Arbeitsblatt	16
Kontrollblatt.....	19
Hausaufgabe	21
Erwartungshorizont: Hausaufgabe	22

Vorlage / Langentwurf / Unterrichtsstunde¹

Erstellt von:

Birte Dieckmeyer

Matrikelnummer:

■■■■■

Zeitumfang (Min.):

90

Klasse:

3

Thema der Stunde:

Das Prinzip des Ver- und Entschlüsselns anhand der Quadratschrift erlernen.

Thema der Reihe:

Kryptologie

¹ Diese Vorlage basiert auf dem Dokument „Schriftliche Arbeit mit Kommentar“ (Stand 03/2013) des Zentrums für schulpraktische Lehrerbildung Krefeld (ZfsL) / Seminar für das Lehramt an Gymnasien und Gesamtschulen.

1. Ziele und angestrebte Kompetenzen

Der vorliegende Unterrichtsentwurf wurde für eine dritte Grundschulklasse konzipiert und umfasst eine Doppelstunde. Das Thema der gesamten Reihe lautet *Kryptologie*, das Prinzip der Ver- und Entschlüsselung von Botschaften. Die Unterrichtsstunde thematisiert dieses Prinzip angewandt auf die Quadratschrift, eine Geheimschrift, mit der Botschaften für Dritte unleserlich gemacht werden können. Das Stundenziel lautet wie folgt: Die *Schülerinnen und Schüler*² sollen mit Hilfe der Quadratschrift das Prinzip der Ver- und Entschlüsselung erläutern können. Sie zeigen dies, indem sie verschlüsselte Botschaften der Quadratschrift entschlüsseln und Botschaften in die Quadratschrift verschlüsseln und dies mit eigenen Worten erklären können. Ferner sind vier Teilziele definiert: Die SuS sollen die Begriffe „Verschlüsseln“ und „Entschlüsseln“ erläutern können. Sie zeigen dies, indem sie anhand eines Beispiels das Prinzip der Ver- und Entschlüsselung erläutern können (1). Die SuS sollen unter Verwendung der Quadratschrift das Prinzip der Ver- und Entschlüsselung anwenden können. Sie zeigen dies, indem sie aus einer Botschaft eine Geheimbotschaft und umgekehrt aus einer Geheimbotschaft eine Botschaft erstellen können (2). Die SuS sollen erläutern können, wie das von ihnen verwendete Verschlüsselungsverfahren funktioniert. Dies zeigen sie, indem sie die Quadratschrift mit dem Prinzip des Ver- und Entschlüsselns sowie den vier Funktionen Borys erklären können (3). Die SuS sollen erläutern können, welchen Vorteil eine verschlüsselte Botschaft gegenüber einer unverschlüsselten Botschaft hat. Dies zeigen sie, indem sie sich mit dem Prinzip der Ver- und Entschlüsselung kritisch auseinandersetzen und dieses Prinzip auf ihre Lebenswelt beziehen (4). Nach den Bildungsstandards Informatik für den Primarbereich [BS17] ergibt sich folgende Kompetenzerwartung am Ende der Klasse vier: Die SuS kennen ein exemplarisches Verschlüsselungsverfahren. Dabei umfasst die inhaltsbezogene Kompetenz den Bereich der *Information und Daten*. Die durch die Quadratschrift entstehenden Zahlenfolgen und Worte sollen von den SuS als Information wahrgenommen und interpretiert werden. Dazu müssen sie mit den unterschiedlichen Darstellungsformen dieser Daten, einerseits in der Alphabetschrift und andererseits in Form einer bestimmten Zahlennotation, operieren und diese in Sachzusammenhänge bringen. Die SuS wenden Informatik auf konkrete Aufgabenstellung an, indem sie informatische Kenntnisse und Fähigkeiten nutzen. Sie setzen sich mit dem Modell der Quadratschrift auseinander und arbeiten damit. Die prozessbezogenen Kompetenzen *Modellieren und Implementieren* werden somit gefördert [BS17].

² Im Folgenden werden *Schülerinnen und Schüler* mit *SuS* abgekürzt.

2. Didaktische Schwerpunkte

Im Folgenden werden die einzelnen Elemente der Unterrichtsstunde didaktisch begründet. Bei den jeweiligen Entscheidungen wird stets versucht, die Vermittlungsabsicht zu berücksichtigen und die fachlichen Aspekte mit der Lernerperspektive in Einklang zu bringen. Dazu ist eine kritische Auseinandersetzung mit dem Thema *Kryptologie* unausweichlich, ebenso eine Analyse der Lernvoraussetzungen der SuS [Ku07]. Da es sich im vorliegenden Fall um eine allgemeine Unterrichtskonzeption handelt, die sich nicht explizit an eine spezielle Klasse richtet, werden grundlegende Fähigkeiten und Fertigkeiten in Schrift und Sprache sowie Kenntnisse in der Partnerarbeit vorausgesetzt.

Kryptologie, also das Ver- und Entschlüsseln von Botschaften, spielt eine große, wenn auch meist unbemerkte Rolle in der Lebenswelt der SuS. Sei es durch das Nutzen von WLAN-Netzwerken, Türcodes und der EC-Karte oder beim Surfen im Internet. In all diesen Situationen werden kodierte Botschaften verwendet. Beispielsweise befindet sich auf der EC-Karte ein Chip mit einem Hardware-Sicherheitsmodul, welcher einen Schlüssel erzeugt und speichert. Dieser Schlüssel wird durch die Eingabe des Pins freigegeben und die Karte nutzbar gemacht. Viele Computer kommunizieren mittels des Secure Sockets Layer. Dabei verbinden sich zwei Computer, erzeugen einen individuellen Fingerabdruck und können so Nachrichten untereinander ver- und entschlüsseln. Diese Geheimsprachen sind vielen SuS nicht bewusst. Stattdessen verbinden sie mit diesem Begriff eher Schriften aus Zitronensäure oder Morsezeichen. Oft vereinbaren Kinder untereinander Sprachen oder Zeichen, um miteinander zu kommunizieren, ohne dass Dritte sie verstehen. Kryptologie umfasst damit sowohl bewusste, als auch unbewusste Bereiche in der Lebenswelt der SuS.

Lehr- und
Lernaus-
gangslage
der SuS

Neben der Aktualität weckt das Thema die kindliche Neugier, Geheimnisse aufzudecken und die Freude daran, selber geheime Botschaften für andere zu erstellen. Ferner entspricht die Methode der Quadratschrift dem kreativen und forschenden Geist von Kindern, Regelmäßigkeiten zu entdecken und eigene Strategien zu entwickeln [Mk10]. Sie ermöglicht differenziertes Üben aufgrund der Berücksichtigung des individuellen Lerntempos der SuS sowie der Berücksichtigung sprachlicher und kreativer Fähigkeiten durch unterschiedliche Niveaus der zu ver- und entschlüsselten Botschaften. Durch den Austausch über die Funktionen der Quadratschrift wird die Ausdrucksfähigkeit der SuS gefördert. Zudem ist die Quadratschrift auf weitere Bereiche der Informatik übertragbar, z.B. dem Kodieren von Daten und bietet eine Grundlage für anschlussfähigen Informatikunterricht.

Die Kryptologie umfasst die Wissenschaft der Datenverschlüsselung und lässt sich in zwei Teilbereiche gliedern: die Kryptographie und die Kryptoanalyse. Unter der Kryptographie versteht sich das Absichern von Informationen durch Chiffrierung, wobei eine Botschaft mittels eines bestimmten Schlüssels für Dritte unleserlich gemacht wird. Die Kryptoanalyse beschreibt die Kunst des Entschlüsselns, der Dechiffrierung: Die Geheimbotschaft wird in einen Klartext kodiert und so für den Empfänger lesbar gemacht. Dies funktioniert nur, wenn der gleiche Schlüssel zum Dechiffrieren der Botschaft benutzt wird, welcher auch zum Chiffrieren angewendet wurde. Dieses Vorgehen wird symmetrisches Verfahren genannt. Ein asymmetrischen Verfahren beschreibt einen Angriff durch eine dritte Person – ohne Einverständnis von Sender und Empfänger –, dabei ist der Schlüssel zum Dechiffrieren nicht bekannt und muss zunächst entwickelt werden [Ba15] [Bt11] [Bj16].

Durch die Kryptologie sollen laut Borys vier Funktionen geschaffen werden:

- (1) Die Authentizität der Botschaft, also dass die Nachricht von mindestens einer Person als „echt“ nachgewiesen werden und sich der Empfänger vom Ursprung dieser überzeugen kann.
- (2) Die Integrität, welche besagt, dass die Nachricht nicht durch Dritte verändert werden kann.
- (3) Die Verbindlichkeit der Botschaft, wodurch die unmittelbare Sendung an den Empfänger beschrieben wird.
- (4) Die Anonymität, welche verborgene Kommunikation gewährleistet und das Mitlegen der Nachrichten durch Dritte verhindert [Bt11].

In Bezug auf die Vermittlungsabsicht muss an dieser Stelle die Lernerperspektive berücksichtigt werden. Das Prinzip der Kryptologie – das Ver- und Entschlüsseln von Botschaften – sowie die einzelnen Funktionen sollen den Kindern verständlich dargestellt werden. Dazu muss das Thema an die Lebenswelt der SuS angepasst und Fachtermini geklärt werden [Ku07]. Der Begriff *Kryptologie* wird durch die Wörter „Verschlüsseln“ und „Entschlüsseln“ ersetzt, wodurch die Differenzierung *Kryptographie* und *Kryptoanalyse* entfällt. Diese beiden Wörter umfassen zudem Begriffe wie „chiffrieren“ (verschlüsseln), „dechiffrieren“ (entschlüsseln) oder „(de-)kodieren“. Um die vier Funktionen Borys nachzuvollziehen, ist es sinnvoll, diese an einer exemplarischen Geheimschrift deutlich zu machen. In dem vorliegenden Fall wurde die Quadratschrift ausgewählt. Diese ist wie ein Polybios-Quadrat aufgebaut: In der oberen Reihe befinden sich die Zahlen eins bis fünf, am linken Rand die Zahlen sechs bis null und im Quadrat die 25 Buchstaben, ausschließ-

lich das J.³ Folglich bilden zwei Zahlen einen Buchstaben, indem zuerst eine Zahl des linken Rands und anschließend eine des oberen Rands ermittelt wird [Rg]. Mit Hilfe der Quadratschrift können das Prinzip und die Funktionen der Ver- und Entschlüsselung von Botschaften veranschaulicht und eingeübt werden. Den Kindern wird deutlich gemacht, dass sie selber geheime Nachrichten erstellen können und diese durch die Eigenproduktion echt bzw. authentisch sind. Ferner soll von den SuS erkannt werden, dass eine Botschaft zwar entschlüsselt, jedoch nicht mehr verändert werden kann und unmittelbar, beispielsweise an den Partner, gesendet wird. Durch die Unleserlichkeit der geheimen Botschaften für die Nachbarklasse wird die Anonymität der Nachrichten dargestellt. Somit werden alle vier Funktionen der Kryptologie berücksichtigt und schülerorientiert vermittelt. Ein Vorteil der Quadratschrift ist zudem die Erweiterung auf Buchstaben. So können anstatt der Zahlen bestimmte Buchstaben gewählt werden, wodurch eine neue Geheimschrift entsteht und den Kindern die Möglichkeit geboten wird, sich noch ausführlicher mit der Methode auseinanderzusetzen. Auch können im Anschluss an diese Stunde weitere Geheimschriften analysiert werden.

Durch das Verstehen des Prinzips der Ver- und Entschlüsselung unter Berücksichtigung der vier Funktionen Borys wird eine Grundlage für Kodierungsvorgänge in der Informatik geschaffen und das Interesse für das Fach Informatik bei den SuS geweckt.

Die Bildungsstandards der Informatik für den Primarbereich fordern informatische Allgemeinbildung und das Nutzen von Elementen der Fachsprache [BS17]. Durch das Thema Kryptologie werden den SuS Grundlagen der Datenverschlüsselung nähergebracht und das Wissen im Bereich der Informatik erweitert. Die Verwendung von Begriffen wie Ent- und Verschlüsselung und der aktive Austausch über das Prinzip der Quadratschrift fördern den fachlichen Ausdruck der Kinder. Der direkte und indirekte Zusammenhang von Geheimschriften in der Lebenswelt der Kinder (siehe 2.1) führt dazu, dass die SuS ihre informatische Sichtweise auf die Welt ausbauen und diese dadurch besser verstehen und gestalten können. Auch wird die Aufmerksamkeit der SuS auf Gefahren von Datensicherung gelenkt und ein kritischer und bewusster Umgang damit angeleitet. Dies stärkt zudem das Selbstbild der Kinder im Bereich der Informatik, wodurch ebenfalls die Forderungen der Bildungsstandards erfüllt werden [BS17].

Zudem sollen – laut Lehrplan und Bildungsstandards – die SuS möglichst entdeckend und problemlösend lernen. Das Prinzip der Ver- und Entschlüsselung, welches die Quadrat-

Legitimation des Vorhabens durch curriculare Vorgaben

³ siehe Anhang.

schrift umfasst, kann selbstständig geübt und erweitert werden. Die SuS können Modelle und Strategien entwickeln, Botschaften zu kodieren und somit für Dritte unleserlich zu machen. Dieses Vorgehen erfordert Kreativität, was sich wiederum positiv auf das Selbstkonzept der Kinder auswirken kann. Die Anknüpfung an die Lebenswelt, beispielsweise bei der Nutzung des Internets, kann Chancen und Gefahren der Kryptologie aufdecken, die den SuS bislang verborgen geblieben sind. Somit ist auch die geforderte Anwendungs- und Strukturorientierung gewährleistet. Durch die Vernetzung verschiedener Darstellungsformen, beispielsweise durch den Wechsel der Alphabet- und Zahlennotation, das Visualisieren der Quadratschrift am OHP sowie das Rollenspiel zu Beginn der Unterrichtsstunde, wird eine Verständnisgrundlage geschaffen. Mit Hilfe unterschiedlicher Niveaus der Übungsaufgaben bzw. der Schwierigkeitssteigerung dieser werden Differenzierungsmöglichkeiten gewährleistet [BP17] [LP08].

Ferner wird eine anschlussfähige Grundlage für die weitere Informatikbildung geschaffen. Beispielsweise sollen sich SuS laut dem Lehrplan die Sekundarstufe I mit Algorithmen auseinandersetzen, Strukturen und Beziehungen zwischen Objekten erkennen oder den Einsatz von Informatiksystemen in der Gesellschaft bewerten. Das Auseinandersetzen mit dem Thema *Kryptologie* schafft dafür ein erstes Fundament [LP15].

Das Thema Kryptologie spielt, wie in Kapitel 2.1 bereits erläutert, einen kardinalen Aspekt im Leben der SuS. Oft wird eine Ver- und Entschlüsselung von Daten nicht bewusst von den Kindern ausgeführt. Durch den vorliegenden Unterricht soll neben informatischen Kenntnissen und Fertigkeiten Kryptologie im Alltag deutlich gemacht werden. Gerade im Internet werden viele Daten verschlüsselt und gespeichert, ohne dass die Nutzer dies bemerken. So wird der Blick der SuS geschult, um Datenverschlüsselung zu erkennen und sich eventuell vor möglichen Gefahren, wie das Mitlesen privater Nachrichten, zu schützen. Im weiteren Verlauf der Unterrichtsreihe wird eine Diskussion über Vor- und Nachteile verschlüsselter Botschaften stattfinden, wodurch die SuS zu einem sensibleren Umgang mit Daten in ihrer Lebenswelt geschult werden. Ferner soll durch das Nutzen einer Geheimschrift deutlich gemacht werden, dass persönliche Daten geschützt werden können, indem die vier Funktionen Borys eingehalten werden. So besteht beispielsweise die Möglichkeit, eine Botschaft an einen Empfänger zu übermitteln, ohne dass ein Dritter diese Nachricht lesen kann.

Relevanz
für die SuS

Die Aktualität des Themas, die zukünftigen Konsequenzen der Datennutzung der SuS und die Forderungen der Bildungsstandards sowie des Lehrplans rechtfertigen das Behandeln von Kryptologie in der Grundschule.

Da die vorliegende Unterrichtsplanung die Einführung der Unterrichtsreihe zum Thema *Kryptologie* darstellt, ist ein ausführlicher Einstieg in diese Thematik notwendig und sinnvoll. So soll durch ein Rollenspiel das Vorwissen der SuS zum Ver- und Entschlüsseln von Botschaften geweckt werden. Durch den direkten Bezug zur Lebenswelt der Kinder – das Nutzen von Türcodes – wird eine Situation geschaffen, die jedes Kind kennt und versteht. Dadurch kann leicht ein für die SuS nachvollziehbarer Bezug zur Datenverschlüsselung dargestellt werden. Ferner soll die kleine Inszenierung die Motivation und das Interesse der SuS wecken, genau zu beobachten und Besonderheiten zu entdecken. Es soll an dieser Stelle bereits verdeutlicht werden, wie sehr Datenverschlüsselung den Alltag berührt – wenn auch meist unbemerkt. Um nun einen reibungslosen Übergang zu der in der Unterrichtsstunde behandelnden Quadratschrift zu ermöglichen, werden Ideen und Möglichkeiten verschiedener Geheimschriften und –sprachen gesammelt. Es wird ein Austausch angeleitet, der zur Wissensaktivierung anregt und erste Vermutungen zum Thema Ver- und Entschlüsselung von Botschaften einfordert.

Begründung der wichtigsten Entscheidungen des geplanten Unterrichts

Anschließend wird an der Tafel in der Zahlennotation eine für die SuS noch unleserliche Botschaft geschrieben. Dadurch wird eine weitere Art der Geheimschrift dargestellt, die es in der Stunde zu untersuchen und anzuwenden gilt. Es folgt eine kurze Erläuterung seitens der Lehrkraft, wie der nachfolgende Verlauf des Unterrichts aufgebaut ist. Dabei soll den SuS das Stundenziel – das Verstehen und das Anwenden der Quadratschrift – deutlich gemacht werden. Gerade schwächere Kinder bedürfen starker Strukturierungshilfen, was durch die Studententransparenz ermöglicht werden soll [Mk10]. Auch aus diesem Grund wird im ersten Teil der Erarbeitungsphase mit der gesamten Klasse die Quadratschrift eingeführt. Mit Hilfe des OHPs wird diese visualisiert dargestellt und je nach Leistungsniveau der SuS die dahinterstehende Strategie von der Lehrkraft oder von den Kindern erläutert. Dadurch wird zusammen eine Verständnisgrundlage geschaffen und mögliche Fachtermini geklärt, sodass alle SuS auf einer Ebene kommunizieren. Dies wird durch das gemeinsame Entschlüsseln einer exemplarischen Botschaft erreicht. An dieser Stelle muss die Lehrkraft individuell auf die Klasse abgestimmte Hilfestellungen geben und eventuell das Lösen der Aufgabe übernehmen [V178]. Im Anschluss daran wird der Arbeitsauftrag erklärt: Die SuS sollen im zweiten Teil der Erarbeitung in Partnerarbeit verschiedene Botschaften ent- und

verschlüsseln. Das Arbeitsmaterial ist so aufgebaut, dass sich die Schwierigkeit der Aufgaben steigert und eine Zusatzaufgabe angeboten wird, die nicht gelöst werden muss.⁴ Somit soll eine Differenzierung gewährleistet werden. Zur Ergebniskontrolle liegen Kontrollblätter zur Selbstkontrolle aus, um das eigene Lern- und Arbeitstempo zu gewährleisten.⁵ Ferner ermöglicht dies der Lehrkraft Zeit, um individuell einzelnen Gruppen Unterstützung bei Problemen zu bieten. Durch die Methode der Partnerarbeit sollen sich die SuS über ihre Lösungswege austauschen und diese eventuell revidieren. Ziel dieser Methode ist es, dass die SuS Verständnisschwierigkeiten durch die Kommunikation untereinander lösen und sich gegenseitig helfen. Hilfestellungen der Lehrkraft sind somit nur bei großen Hindernissen erwünscht. Es wird deutlich, dass durch den Austausch der SuS kommunikative und kooperative Kompetenzen geschult werden. Auch ist das gemeinsame Auseinandersetzen mit einer neuen Materie motivierend und steigert die Effizienz [Mk10]. Nachdem die SuS die vorgegebenen Botschaften erfolgreich ver- und entschlüsselt haben, sollen sie für ihren Partner eine Nachricht verschlüsseln. Dabei können die SuS selbstständig entscheiden, ob die geheime Botschaft lediglich ein Wort oder einen ganzen Satz umfasst. Auch hier entsteht Raum für Differenzierung und die Schwierigkeit kann individuell auf den Partner abgestimmt werden. An dieser Stelle wird neben der Vertiefung des Verständnisses der Quadratschrift auch die Kreativität der Kinder gefördert. Das kann sich positiv auf das Selbstbild der SuS auswirken und damit auch auf das Fach Informatik. Um die Leistungen der Kinder zu würdigen, werden nach der Gruppenarbeitsphase einzelne Botschaften über den Visualizer dargestellt und von den SuS entschlüsselt. Bei Bedarf können auch Lösungswege von Aufgaben des Arbeitsblattes vorgestellt werden. So entsteht eine gemeinsame Grundlage, welche anschließend im Lehrer-Schüler-Gespräch erweitert wird: Das Prinzip der Ver- und Entschlüsselung wird auf die Quadratschrift übertragen und die Funktionen Borys anhand dieser erklärt. Es soll deutlich hervorgehoben werden, dass mittels dieser Geheimschrift Botschaften für Dritte unleserlich gemacht werden können und diese nur für Personen nutzbar ist, die Wissen über den Schlüssel der Kodierung haben.

Als Verständnishilfe bietet sich hier der Bezug zur Nachbarklasse an. So sollen gemeinsam mit den SuS die vier Funktionen nach Borys (siehe Kapitel 2.2) erarbeitet und kindgerecht auf einem Plakat zusammengefasst werden. Dazu werden die von den Kinder verwendeten Ausdrücke benutzt, um ihren Denkweisen gerecht zu werden. Aufgrund dessen kann dieser Bereich des Unterrichts nicht explizit vorbereitet werden und die Lehrkraft muss flexibel

⁴ siehe Anhang.

⁵ siehe Anhang.

auf die Reaktionen der SuS eingehen. Wichtig ist neben der Berücksichtigung der Lernerperspektive auch die fachliche Korrektheit des Plakats, da dieses als Ergebnissicherung dient und für den weiteren Verlauf der Unterrichtssequenz genutzt wird. Um nun das neu erworbene Wissen über das Ver- und Entschlüsseln von Daten auf einen Bereich der Lebenswelt der Kinder zu beziehen, wird ein Bezug zu dem anfangs inszenierten Rollenspiel hergestellt. Dieses Beispiel einer Kodierung im Alltag soll erweitert werden, indem weitere Einsatzmöglichkeiten von Datenverschlüsselung gesucht werden. Dabei sollen erste Gefahren der Nutzung verdeutlicht werden, beispielsweise das Ausschließen von Mitschülern oder das heimliche Mitlesen Dritter.

Als Hausaufgabe soll das gesamte Wissen der Unterrichtsstunde zusammengefasst dargestellt werden, indem die SuS für ihre Nachbarklasse ein übersichtliches Merkblatt erstellen, mit dessen Hilfe sie kurz die Quadratschrift erläutern und daran das Prinzip der Ver- und Entschlüsselung erklären.⁶ Dadurch wird der Inhalt der Unterrichtsstunde wiederholt und gefestigt sowie mögliche Verständnisschwierigkeiten sowohl für die SuS selber als auch für die Lehrkraft sichtbar, die es in der nächsten Stunde zu klären gilt. Die Position des Erklärers in dieser Aufgabe soll zudem motivierend wirken und gleichzeitig die Fähigkeit zur Perspektivübernahme fördern. So müssen sich die SuS in die Lage der Nachbarkinder hineinversetzen und verständlich ihr Wissen darstellen. Auch wird an dieser Stelle die Kreativität und Ausdrucksfähigkeit der SuS gefördert.

Zusammenfassend ist zu sagen, dass das Nutzen der Quadratschrift im Unterricht eine förderliche Methode zum Erreichen der in Kapitel 1 angestrebten Ziele und Kompetenzen darstellt. So werden neben der Kompetenzerwartung der Bildungsstandards, dass die SuS ein exemplarisches Verschlüsselungsverfahren kennen, auch die inhaltbezogenen und prozessbezogenen Kompetenzen gewährleistet: Die SuS kennen am Ende der Doppelstunde den Zusammenhang zwischen den Informationen – also einer geheimen Botschaft – und den Daten – den einzelnen Zahlen – und wenden das Modell der Quadratschrift an, indem sie Botschaften ver- und entschlüsseln. Ferner können die SuS das Prinzip der Ver- und Entschlüsselung unter Berücksichtigung der vier Funktionen Borys auf die vorliegende Geheimschrift beziehen, wodurch das Stundenziel erreicht wurde.

⁶ siehe Anhang.

3. Geplanter Verlauf des Unterrichts

Erstellt von:

Birte Dieckmeyer

Zeitumfang (Min.):

90

Klasse:

3

**Das Stundenziel/
Kernanliegen mit Indi-
kator:**

Die Schülerinnen und Schüler sollen...

- mit Hilfe der Quadratschrift das Prinzip der Ver- und Entschlüsselung erläutern können.

Sie zeigen dies, indem sie...

- verschlüsselte Botschaften der Quadratschrift entschlüsseln und Botschaften in die Quadratschrift verschlüsseln und dies mit eigenen Worten erklären können.

Teilziele mit Indikator:

Die Schülerinnen und Schüler sollen...

- die Begriffe „Verschlüsseln“ und „Entschlüsseln“ erläutern können.

Sie zeigen dies, indem sie...

- anhand eines Beispiels (Rollenspiel, Tafelbild) das Prinzip der Ver- und Entschlüsselung erläutern können.

Die Schülerinnen und Schüler sollen...

- unter Verwendung der Quadratschrift das Prinzip der Ver- und Entschlüsselung anwenden können.

Sie zeigen dies, indem sie...

- aus einer Botschaft eine Geheimbotschaft (Verschlüsselung) und umgekehrt aus einer Geheimbotschaft eine Botschaft (Entschlüsselung) erstellen können.

Die Schülerinnen und Schüler sollen...

- erläutern können, wie das von ihnen verwendete Verschlüsselungsverfahren funktioniert.

Dies zeigen sie, indem sie...

- die Quadratschrift mit dem Prinzip des Ver- und Entschlüsseln sowie den vier Funktionen Borys er-

Hierdurch sollen folgende Kompetenzen laut Lehrplan [MSW08] gefördert werden:

<p>klären können.</p> <p>Die Schülerinnen und Schüler sollen</p> <ul style="list-style-type: none">• erläutern können, welchen Vorteil eine verschlüsselte Botschaft (Geheimbotschaft) gegenüber einer unverschlüsselten Botschaft hat. <p>Dies zeigen sie, indem sie...</p> <ul style="list-style-type: none">• sich mit dem Prinzip der Ver- und Entschlüsselung kritisch auseinandersetzen und dieses Prinzip auf ihre Lebenswelt beziehen.
<p>inhaltsbezogene Kompetenz:</p> <ul style="list-style-type: none">• Information und Daten <p>prozessbezogene Kompetenz:</p> <ul style="list-style-type: none">• Modellieren und Implementieren <p>Kompetenzerwartung Ende Klasse 4:</p> <ul style="list-style-type: none">• Die Schülerinnen und Schüler kennen ein exemplarisches Verschlüsselungsverfahren.

4. Artikulationsschema/ Synopse

Dauer (Min.)	Unterrichtsphase	Unterrichtsinhalte	Sozial-/Aktionsformen	Material/Medien/Werkzeug	didaktisch-methodischer Kommentar
5	Einstieg	Rollenspiel: - vier SuS (davon ein/e Türsteher/in) - Türsteher/in „verschlüsselt“ die Tür mit einem Codewort - Lehrkraft gibt den drei SuS Codewörter vor, wovon ein Kind das Wort erhält, bei dem sich die Tür „entschlüsselt“	Sitzkreis	Sitzkreis	Vorwissen zu Kryptologie aktivieren - die Begriffe „Verschlüsseln“ und „Entschlüsseln“ veranschaulichen - Motivation wecken
5	Hinführung	- Ideensammlung zu Geheimschriften in der Lebenswelt der SuS - Verdeutlichen des Themas durch verschlüsselte Botschaft an der Tafel: 72657365748293637392747194 (GEHEIMSCHRIFT)	Plenum	Tafel	- Verdeutlichen, dass Buchstaben durch Zahlen ersetzt werden können - Stundentransparenz → Quadratschrift anwenden und Prinzip der Ver- und Entschlüsselung kennen.
10	Erarbeitung Teil I	- Quadratschrift visualisieren und erklären (lassen) - je nach Leistungsniveau der Klasse: Die LP entschlüsselt exemplarisch eine Botschaft. oder: Die SuS entschlüsseln gemeinsam (mit Hilfe der anderen SuS und der LP) exemplarisch eine Botschaft.	Plenum	OHP, Folie mit Abbildung der Quadratschrift	Einführung in die Quadratschrift - Vorgehen bei der Aufgabenbearbeitung (Ver- und Entschlüsseln der Quadratschrift) verstehen

30	Erarbeitung Teil II	<ul style="list-style-type: none"> - Arbeitsblatt mit jeweils fünf Botschaften zum Ver- und Entschlüsseln - Selbstkontrolle - Eigenständig eine verschlüsselte Botschaft für einen Partner entwickeln - Botschaften mit dem Partner austauschen, entschlüsseln und Lösung besprechen 	Partnerarbeit	OHP, Arbeitsblatt, Kontrollblätter zur Selbstkontrolle	Anwenden der Quadratschrift <ul style="list-style-type: none"> - Prinzip der Ver- und Entschlüsselung von Botschaften verstehen und anwenden
10	Auswertung/ Präsentation	<ul style="list-style-type: none"> - Zusammenfassen der Ergebnisse - ausgewählte Botschaften vorstellen und von der Klasse entschlüsseln lassen 	Plenum	Visualizer	<ul style="list-style-type: none"> - Verständniskontrolle - selbstentwickelte Aufgaben vorstellen
20	Sicherung	<p>Verdeutlichen des Prinzips des Ver- und Entschlüsselns</p> <ul style="list-style-type: none"> - Warum kann Schüler/in x die Nachricht von Schüler/in y lesen? Warum kann es Schüler/in z der Nachbarklasse nicht? → vier Funktionen Borys → Rückblick/ Bezug Türsteher <p>Weiterführende Frage: Wann und wo braucht man Geheimschriften?</p>	Sitzkreis	Plakat	<p>Ergebnissicherung</p> <ul style="list-style-type: none"> - verallgemeinernde Erklärung finden - vier Funktionen auf Plakat festhalten - Prinzip des Ver- und Entschlüsselns auf Anfangsbeispiel übertragen und darauf anwenden Lebensweltbezug herstellen - Bewusstmachen von Geheimschriften im Alltag - Nützlichkeit und Gefahren von Geheimschriften
5	Hausaufgabe	<p>Entwickeln eines Merkblattes für die Nachbarklasse, in dem</p> <ul style="list-style-type: none"> - die Quadratschrift kurz erklärt wird. - das Verschlüsseln und Entschlüsseln von Botschaften dargestellt wird. 	Einzelarbeit		<p>Ergebnissicherung und Verständniskontrolle</p> <p>Auseinandersetzen mit verschlüsselten Botschaften</p>
5	Zeitpuffer				Zeitpuffer, falls Probleme oder Unerwartetes auftreten

Literaturverzeichnis

- [Ba15] Beutelspacher, Albrecht: Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. 10. Aufl. Wiesbaden: Springer Spektrum, S.10, 18-20, 72f., 80f., 157-160, 2015
- [Bt11] Borys, Thomas: Codierung und Kryptologie. Facetten einer anwendungsorientierten Mathematik im Bildungsprozess. Wiesbaden: Vieweg + Teubner Verlag, S.61-63, 2011
- [Bj16] Buchmann, Johannes: Einführung in die Kryptographie. 6. Aufl. Berlin, Heidelberg: Springer-Verlag, S.73-77, 2016
- [Ku07] Kattmann, U.: Didaktische Rekonstruktion. In: Krüger, D./ Vogt, H. (Hrsg.): Theorien der biologiedidaktischen Forschung. Ein Handbuch für Lehramtsstudenten und Doktoraten. Berlin: Springer, S.93-98, 2007
- [Mk10] Möller, K.: Lernen von Naturwissenschaften heißt: Konzepte verändern. In: Labudde, P. (Hrsg.): Fachdidaktik Naturwissenschaft. 1.- 9. Schuljahr. Stuttgart: Hauptverlag, S.64-68, 2010
- [VI78] Vygotsky, L.: Mind in Society. The Development of Higher Psychological Processes. Cambridge, MA: Harvard University Press, S.86, 1978
- [Rg] Reinschmidt, Günter: Geheimschriften, S.9
- [BS17] Arbeitskreis »Bildungsstandards Primarbereich« der Gesellschaft für Informatik (GI) e.V.: Bildungsstandards Informatik für den Primarbereich – zur Diskussion, S.1-10, 2. Januar 2017 – Version 414
- [LP08] Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen: Richtlinien und Lehrpläne für die Grundschule in Nordrhein-Westfalen. Düsseldorf, S.55f., 2008
- [LP15] Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen: Richtlinien und Lehrpläne für die Gesamtschule und Sekundarschule in Nordrhein-Westfalen. Düsseldorf, S.12-20, 2015

Anhang

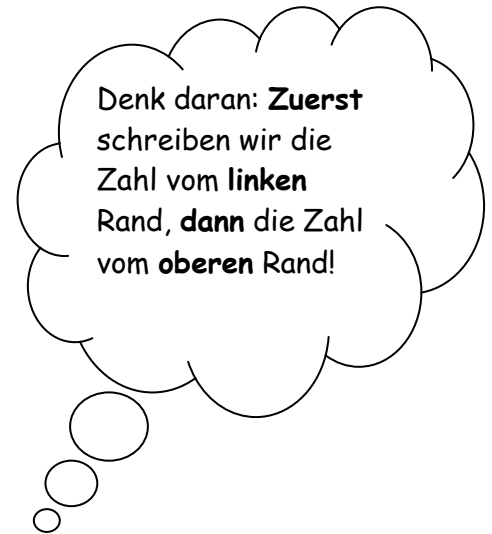
Folie für den OHP

Die Quadratschrift

	1	2	3	4	5
6	A	B	C	D	E
7	F	G	H	I	K
8	L	M	N	O	P
9	Q	R	S	T	U
0	V	W	X	Y	Z

Arbeitsblatt: Wir erforschen die Quadratschrift!

	1	2	3	4	5
6	A	B	C	D	E
7	F	G	H	I	K
8	L	M	N	O	P
9	Q	R	S	T	U
0	V	W	X	Y	Z



Was steht denn da? Entschlüssel die geheimen Botschaften!



Schau dir die geheimen Botschaften und die Tabelle ganz genau an!



Welcher Buchstabe wird durch welche Zahlen ersetzt?



Schreibe die gesuchte Botschaft auf!

73 61 81 81 84

64 95 83 75 65 81

82 95 94 74 72

64 65 94 65 75 94 74 01

72 65 71 61 73 92

★93 85 95 65 92 83 61 93 65

Jetzt andersherum! Verschlüssel in geheime Botschaften!

S P I O N

S C H L A U

G R U S E L I G

R A E T S E L

G R U S E L I G

★ W I E G E H T ' S ?

Verschicke eine geheime Botschaft an deinen Partner!



Überlege dir eine kleine Botschaft für deinen Partner!



Schreibe die Botschaft verschlüsselt auf!



Tauscht eure Botschaften und entschlüsselt sie!

geheime Botschaft: _____

Lösung: _____

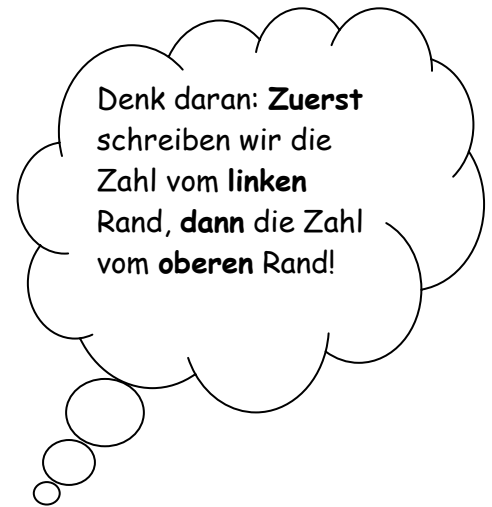
★

geheime Antwort
für den Partner: _____

Lösung: _____

Kontrollblatt: Wir erforschen die Quadratschrift!

	1	2	3	4	5
6	A	B	C	D	E
7	F	G	H	I	K
8	L	M	N	O	P
9	Q	R	S	T	U
0	V	W	X	Y	Z



Was steht denn da? Entschlüssel die geheimen Botschaften!



Schau dir die geheimen Botschaften und die Tabelle ganz genau an!



Welcher Buchstabe wird durch welche Zahlen ersetzt?



Schreibe die gesuchte Botschaft auf!

73 61 81 81 84

HALLO

64 95 83 75 65 81

DUNKEL

82 95 94 74 72

MUTIG

64 65 94 65 75 94 74 01

DETEKTIV

72 65 71 61 73 92

GEFAHR

★93 85 95 65 92 83 61 93 65

SPUERNASE

Jetzt andersherum! Verschlüssel in geheime Botschaften!

S	P	I	O	N
93	85	74	84	83

S	C	H	L	A	U
93	63	73	81	61	72

G	R	U	S	E	L	I	G
72	92	95	93	65	81	74	72

R	A	E	T	S	E	L
92	61	65	94	93	65	81

G	R	U	S	E	L	I	G
72	92	95	93	65	81	74	72

★	W	I	E		G	E	H	T	'	S?
02	74	65			72	65	73	94	'	93?

Hausaufgabe:

Du hast heute ganz viel über *Geheimschriften* gelernt: Du hast geheime Botschaften lesbar gemacht und sogar selber geheime Botschaften erstellt!

Das sollst du nun der 3b beibringen. Dazu sollst du ein **Merkblatt** erstellen, in dem du die *Quadratschrift* kurz erklärst. Am besten guckst du dir die Tabelle dazu noch einmal ganz genau an und überlegst, wie eine Botschaft gebildet wird. Gehe auch auf die vier Funktionen ein, die wir auf dem Plakat gesammelt haben.

Dann können wir bald geheime Botschaften mit der Klasse 3b austauschen!

Erwartungshorizont: Hausaufgabe

a) inhaltliche Leistung

	die Schülerin/ der Schüler	Max.	Err.
1	beschreibt den Aufbau der Quadratschrift, etwa <ul style="list-style-type: none"> - oberer Rand: Zahlen 1-5 - linker Rand: Zahlen 6-0 - im Quadrat: Buchstaben des Alphabets, außer J 	4	
2	erläutert das Bilden einer geheimen Botschaft mittels der Quadratschrift, etwa <ul style="list-style-type: none"> - zuerst die Zahl des linken Rands, dann die Zahl des oberen Rands ermitteln - zwei Zahlen ergeben einen Buchstaben 	2	
3	gibt die Hauptfunktionen der Quadratschrift wieder, etwa <ul style="list-style-type: none"> - Ausgangspunkt: Geheimschrift, um Nachrichten zu verschlüsseln/ für Dritte unleserlich zu machen - Prinzip der Ver- und Entschlüsselung von Nachrichten - 4 Funktionen Borys: <ol style="list-style-type: none"> 1) Echtheit der Nachricht 2) Unveränderbarkeit 3) Unmittelbarkeit 4) Anonymität 	6	
	Summe	12	

b) Darstellungsleistung

	die Schülerin/ der Schüler	Max.	Err.
1	strukturiert seinen Text schlüssig	1	
2	nutzt fachsprachliche Formulierungen, etwa <ul style="list-style-type: none"> - Prinzip der Ver- und Entschlüsselung - ver- und entschlüsseln - geheime Botschaft - Anonymität 	2	
3	berücksichtigt die Leserperspektive	1	
4	schreibt sprachlich richtig	1	
	Summe	5	

Versicherung:

„Ich versichere, dass ich den Unterrichtsentwurf eigenständig verfasst, keine anderen Quellen und Hilfsmittel als die angegebenen benutzt und die Stellen des Unterrichtsentwurfs, die anderen Werken dem Wortlaut oder Sinn entnommen worden sind, in jedem einzelnen Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe. Das Gleiche gilt auch für beigegebene Zeichnungen, Kartenskizzen und Darstellungen. Anfang und Ende von wörtlichen Textübernahmen habe ich durch An- und Abführungszeichen, sinngemäße Übernahmen durch direkten Verweis auf die Verfasserin oder den Verfasser gekennzeichnet.“

Ort, Datum

Unterschrift

Verwertungsrechte:

„Ich erkläre mich damit einverstanden, dass der von mir verfasste Unterrichtsentwurf durch den Arbeitsbereich Didaktik der Informatik der Westfälischen Wilhelms-Universität Münster verwertet werden darf. Dazu gehören die Nutzung und/oder die Veränderung in zukünftigen Lehrveranstaltungen sowie für zukünftige digitale und/oder gedruckte Veröffentlichungen.

Dabei soll folgende Einschränkung gelten (bitte ankreuzen):

Der Unterrichtsentwurf soll anonymisiert werden (Vor- und Nachname).“

Die folgenden Daten werden unabhängig von dieser Einschränkung grundsätzlich aus dem Dokument entfernt: E-Mail Adresse, Anschrift und Matrikelnummer.

Ort, Datum

Unterschrift