Studienreferendar: Christoph van Heteren-Frese
5. SPS Steglitz-Zehlendorf / Frau Gramlich
Schadow Gymnasium (06Y01)
Lerngruppe: in-Z2
Zeit: 8:45 Uhr – 9:30 Uhr
Raum: II-206

Berlin, den 28. Mai 2018

Unterrichtspraktische Prüfung im Rahmen des zweiten Staatsexamens für das Lehramt an Gymnasien und Integrierten Sekundarschulen

Entwurf einer Unterrichtsstunde im Fach Informatik

Thema der Unterrichtsreihe:
Verschlüsselung im Mobilfunknetz

Thema der Stunde:
Sicherer Schlüsselaustausch durch Falltürfunktionen

Prüfungskommission:
Prüfungsvorsitz: Fr. Spring
Fachseminarleiterin Informatik: Fr. Thalemann
Fachseminarleiterin Biologie: Fr.Jahn
Schulleiter: Hr. Krenz

Berlin, den 28. Mai 2018 Unterschrift:_____

1 Thema der Lehr- und Lernprozesse

1.1 Thema der Unterrichtsreihe

Thema der Unterrichtsreihe ist Verschlüsselung im Mobilfunknetz.

1.2 Darstellung der Unterrichtsreihe

Die Unterrichtsreihe kombiniert Teile eines Unterrichtsmodells zum Mobilfunknetz der Arbeitsgruppe *Didaktik der Informatik* (DDI) der Freien Universität Berlin (2015) mit Auszügen der Reihe „*E-Mail (nur?) für Dich*“ von Gramm u. a. (2011). Es werden u.a. die verbindlichen Inhalte Vertraulichkeit und Authentizität, die im Berliner Rahmenlehrplan im Themenfeld *Informatik, Mensch und Gesellschaft* genannt werden, behandelt (Senatsverwaltung für Bildung, Jugend und Sport Berlin 2010, S. 23). Fokussiert werden hier „*Aspekte der Datensicherheit bei der Kommunikation*“ am Beispiel einer verschlüsselten Mobilfunkverbindung (ebd., S. 16).

1.3 Thema der Unterrichtsstunde

Die Unterrichtsstunde fokussiert die praktische Planung eines asymmetrischen Verschlüsselungsverfahrens, dass mit Hilfe eines Rollenspiels auf mögliche Schwachstellen hin überprüft werden soll.

Std.	Thema/Inhalt der UE	Kompetenz und Standardbezug laut RLP
1	**Struktur Mobilfunknetz** - Aufbau des Mobilfunknetz - Funktion der Komponenten	**Informatiksysteme verstehen:**Die SuS diskutieren Funktionalität [...] von Informatiksystemen.
2	**Verbindungsaufbau im Mobilfunknetz**	**Kommunizieren und Kooperieren:** Die SuS dokumentieren, visualisieren, präsentieren und verteidigen Ergebnisse der Teamarbeit. (S.)
3-4	***Der ultimativer Abhöralptraum*** - Sicherheit im Mobilfunknetz	**Wechselwirkung zwischen Informatiksystemen, Mensch und Gesellschaft:** Die SuS bewerten Risiken und Chancen von Informatiksystemen. (RLP S. 17) **Kommunizieren und Kooperieren** Die SuS verwenden selbstständig Fachtexte [...]. (RLP S. 16)
6	**Verschlüsselungsverfahren** -	**Erkenntnisse gewinnen:** Die SuS können Hypothesen aufstellen, die auf naturwissenschaftlichen Fragestellungen basieren. (2.2.2) **Erkenntnisse gewinnen:** Die SuS können das Untersuchungsergebnis unter Rückbezug auf die Hypothese beschreiben. (2.2.2)

(Fortsetzung auf der nächsten Seite)

Tabelle 1: (Fortzsetzung)

Std.	Thema/Inhalt der UE	Kompetenz und Standardbezug laut RLP
7	**Symmetrische Verschlüsselungsverfahren** - Asymmetrische Verschlüsselung - Falltürfunktion	**Problemlösen** Die SuS wenden die Phasen des Problemlöseprozesses (informelle Problembeschreibung, formale Modellierung, Implementierung und Realisierung, Bewertung und Modellkritik) an. RLP (S. 16)
8	**Hybride Verschlüsselungsverfahren** -	**Problemlösen**

2 Kompetenzen und Standards

2.1 Angestrebte längerfristige Kompetenzentwicklung

Die SuS sollen durch die Unterrichtsreihe befähigt werden naturwissenschaftliche Untersuchungen selbstständig zu planen und durchzuführen.

Die in der vorliegenden Stunde angestrebte Förderung der Teilkompetenz ist in der Klasse bisher kaum vorhanden. Die SuS haben lediglich im Rahmen einer Einzelstunde unter Anleitung ein Experiment durchgeführt. Aufbau und die Durchführung waren vollständig vorgegeben, so dass es bisher keinen selbstständigen Planungsanteil gab. Eine Progression ist dementsprechend darin zu sehen, dass in dieser Stunde den SuS ein Teil der Planungsarbeit überlassen wird. Wenngleich die Versuchsplanung noch nicht gänzlich selbstständig durchgeführt wird, ist der Aufbau und die Durchführung in Teilen von den SuS selbst zu planen. Des weiteren ist eine Kompetenzentwicklung im Zuwachs praktischer Fähigkeiten (Performanz) zu sehen. Dazu zählen auch allgemeine Abseitsorganisation und Zeitmanagement.

2.2 Konkretisierung der Standards für die geplanten Lehr- und Lernprozesse

Standard(s) laut RLP	Stand der Kompetenzentwicklung	Standardkonkretisierung
„Die Schülerinnen und Schüler können Experimente zur Überprüfung von Hypothesen nach Vorgaben planen und durchführen.“ (*Rahmenlehrplan für die Sekundarstufe I: Biologie Teil C* 2015, S. 19)	Die Lernenden können einfache Versuche mit vorgegebenem Aufbau und vollständiger Durchführungsanleitung durchführen und in Teilen protokollieren.	Die Lernenden planen einen Modellversuch zum abiotischen Faktor Temperatur mit einer geeigneten Auswertung und erstellen dafür Teile eines Protokolls (Skizze des Versuchsaufbaus und Struktur für die geplante Auswertung).

2.3 Die individuelle Kompetenzentwicklung der Lernenden

Schüler/ Standard	**Stand der Kompetenzentwicklung**	**Maßnahmen zur Kompetenzförderung**	**Indikatoren des Kompetenzzuwachses**
Maximalstandard (A-Schüler)	*z.B: Eleni, Lilith, Paul:* - arbeiten zügig und selbstständig - können Versuchsaufbau beschreiben und erklären - haben noch kein Versuchsprotokoll vollständig selbstständig erstellt	wird aufgefordert Störfaktoren zu benennen und zu diskutieren	Kann die Skizze zum Versuchsaufbau selbstständig erstellen, den Versuch exakt beschreiben und zur Dokumentation eine Tabelle und eine grafische Darstellungsform vorschlagen. Die Hinweise werden nur zur Kontrolle verwendet. Wechselwirkungen und Störfaktoren werden im Versuch berücksichtigt.
Mittlerer Standard (B-Schüler)	*z.B: Lissi, Cäcilia, Mark:* - arbeiten größtenteils selbstständig - haben noch kein Versuchsprotokoll vollständig selbstständig erstellt	Es werden Hinweise zum Vorgehen gegeben	Kann die Skizze zum Versuchsaufbau mit Hilfe weniger Hinweise erstellen, den Versuch mit geringen Ungenauigkeiten beschreiben und zur Dokumentation der Beobachtungen eine Tabelle vorschlagen.
Minimalstandard (C-Schüler)	*z. B Len, Gregor, Piotr:* - können nur bedingt selbstständig arbeiten - sind teilweise abgelenkt - haben noch kein Versuchsprotokoll vollständig selbstständig erstellt	Es werden Hinweise zur Aufgabenverteilung (Gruppeneinteilung), zur Arbeitsweise und zur Nutzung der Hilfsmaterialien gegeben	kann Skizze unter Nutzung aller Hinweise erstellen und den Versuch oberflächlich, aber prinzipiell richtig beschreiben.

3 Sachstrukturanalyse

Grundlegend für die asymmetrische Kryptographie sind bestimmte Funktionen, die sich zwar leicht berechnen lassen, ihre Umkehrfunktion ohne weiteres hingegen nur sehr schwer berechnet werden kann. Diese sogenannten *Einwegfunktionen* mit Falltür (kurz: Falltürfunktion) verfügen aber über eine „Hintertür“. Mit Hilfe dieser „Hintertür“ kann die Umkehrfunktion wiederum leicht bestimmen werden. Beispielsweise lässt sich ein Briefkasten als Falltürfunktion betrachten (vgl. Gramm u. a. 2011, S. 11): Während das Einwerfen eines Briefes leicht geschieht, ist es schwer, ihn danach wieder herauszufischen – es sei denn, man hat den Schlüssel zum Briefkasten.

Im Unterricht werden Falltürfunktionen durch Vorhängeschlösser repräsentiert. Analog zu Falltürfunktion ist das Schließen eines Schlosses durch Zudrücken sehr einfach, während das Öffnen ohne Schlüssel sehr aufwendig ist.

In Abbildung 1 sind die fachlichen Inhalte der Sequenz im Kontext der umspannenden Reihe

in Form einer Mindmap dargestellt.

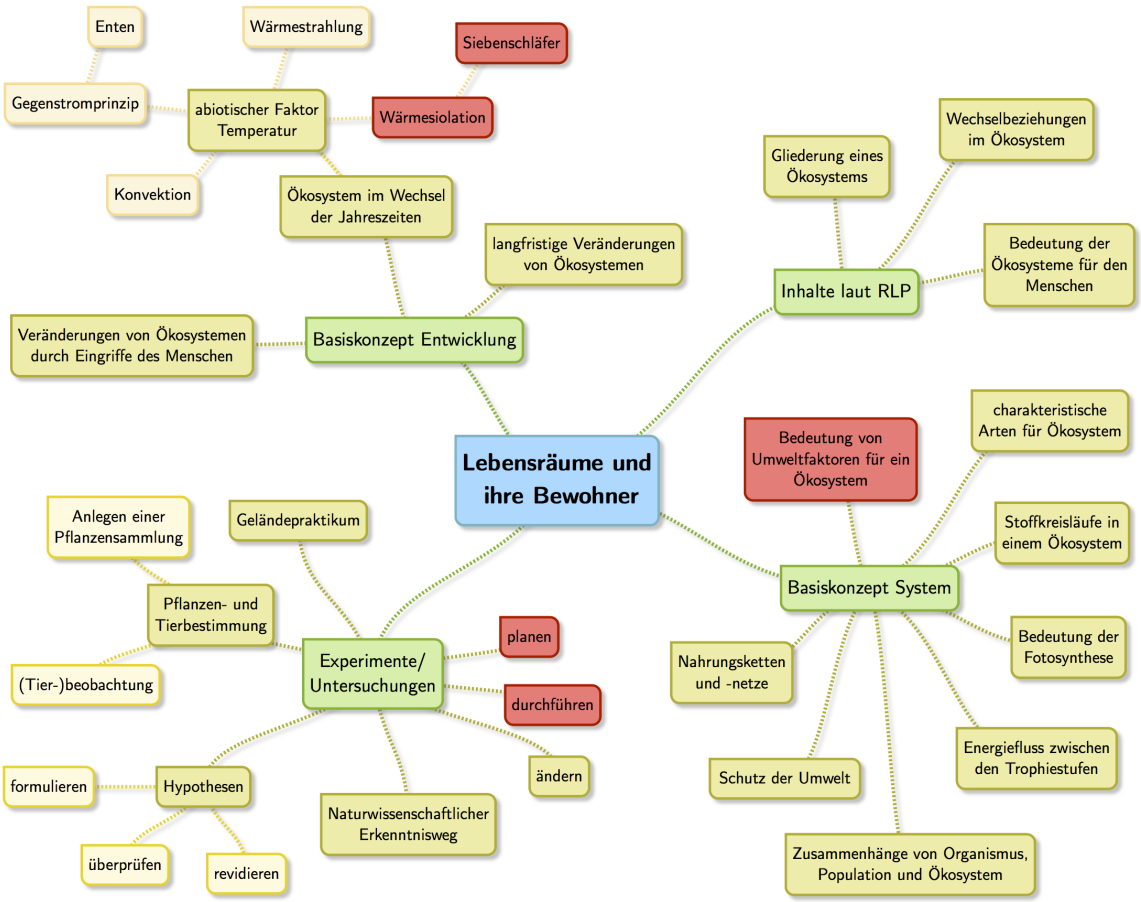

Abb. 1: Mindmap der wichtigsten fachlichen Inhalte. Die Schlagwörter sind so angeordnet, dass der Detailgrad nach außen hin zunimmt. Inhalte der vorliegenden Stunde sind rot eingefärbt.

4 Begründung der Lehr- und Lernstruktur

Ein Sachverhalt kann nach Bruner auf drei verschiedene Arten dargestellt werden: *enaktiv* (d.h. handelnd), *ikonisch* (d.h. bildlich) oder *symbolisch*, (d.h. verbal oder formal) (Brunner 1974, S. 49). Im Sinne eines nachhaltigen Lernens sollten im Unterricht möglichst alle drei Formen genutzt werden, da sie zusammen kohärente mentale Repräsentationen ermöglichen (Kiper und Mischke 2006, S. 56). Dabei sollte auf den Transfer zwischen den drei Repräsentationsmodi besonderer Wert gelegt werden.

Phase	Didaktische oder methodische Entscheidungen	Begründung bezogen auf den fachl.-inhalt. Schwerpunkt	Begründung bezogen auf die SuS (inkl. Lernpsychologie)	Mögliche Schwierigkeiten	Vorbeugende Maßnahmen/mögliche Alternativen
Einstieg	Informierender Einstieg: Transparenz durch Vorstellung des Stundenthemas. Festlegung von Fragestellung im Plenum, um einheitliche Ausgangslage zu schaffen.	Die Einstiegsphase wird zu Gunsten der Erarbeitungsphase bewusst kurz gehalten.	Ziel ist selbstständiges und ergebnisoffenes Arbeiten. Ergebnisse sollen dennoch vergleichbar sein.	SuS kommen zu spät.	Visualisierung von Szenario, Fragestellung & Regeln für das Rollenspiel.
Erarbeitung I		Planung des Verfahrens fördern unmittelbar die fokussierte Kompetenz. Die schriftlichen Notizen zum Ablauf des Verfahrens stellen das Arbeitsergebnis/Lernprodukt dar.	Aufgabenstellung und Material lassen handlungsorientiertes und forschendes Lernen zu.	Evtl. wird zu früh nach den Lösungskarten zum Abschreiben verlangt.	Der Zugriff ist nur am Lehrerpult möglich.
Sicherung I	Da eine Sicherung der Planung bereits mit Hilfe der Lösungskarten stattgefunden hat, wird hier die Darstellung der Ergebnisse fokussiert.	Refelexion der Durchführung ist Bestandteil der Präsentation, Beurteilung der Vermutung ist unverzichtbarer Teil der Erkenntnisgewinnung.		Gruppen brauchen lange zum Aufräumen	gesteuerte Auswahl der präsentierenden Gruppen
Erarbeitung II			Aufgabenstellung und Material lassen handlungsorientiertes und forschendes Lernen zu	Evtl. wird zu früh nach den Lösungskarten zum abschreiben verlangt.	Der Zugriff ist nur am Lehrerpult möglich.
Sicherung II				Gruppen brauchen lange zum Aufräumen	

5 Unterrichtsverlaufsplan

Tabelle 3: Unterrichtsverlaufplan.Abk.: SuS: Schülerinnen und Schüler, AB: Arbeitsblatt.

Phase/Zeit/ Dauer	**Geplantes Verhalten der Lehrkraft/*Leitimpulse***	**Antizipierte Aktivitäten der SuS**	**Sozialform/Medien/ Materialien**
Einstieg 08:045 – 08:50 5 Min.	L. knüpft an die letzte Stunde (Caesar) an und nennt die Fragestellung für die heutige Stunde: *Wie kann das Problem der Schlüsselübermittlung gelöst werden?*	Die SuS rufen sich die Problematik der letzten Stunde in Gedächtnis	Plenum/Beamer, Lehrervortrag, LS-Gespräch
Gelenkstelle: *Um...*			
Erarbeitung 08:50 – 09:05 15 Min.	**Entwickeln und Testen des Verfahrens:** L. teilt Material aus und teilt die SuS in Gruppen auf. L. erläutert die Aufgabenstellung des Rollenspiels. Während des Spiels versucht L, die übermittelte Nachricht zu lesen. Dies kann durch die SuS nur verhindert werden, wenn sie ein geschicktes Schlüsselaustauschverfahren nutzen.	Die in Gruppen aufgeteilten SuS entwickeln ein Verfahren, bei dem sie mittels ihrer Schlösser und einem Briefumschlag eine Nachricht sicher übermitteln können. Sie führen das Verfahren anschließend durch.	2 Vorhängeschlösser u. 1 Briefumschlag (jeweils), Gruppenarbeit
Sicherung 09:05 – 09:10 5 Min.	**Demonstration eines man-in-themiddle-Angriffs:** L. fordert die SuS auf, das Szenario noch einmal durchzuspielen, greift die Nachrichtenübermittlung an, indem er/sie 1. die Nachricht abfängt, mit einem eigenen Schloss versieht und wieder zurückschickt und 2. den Umschlag austauscht und weiter schickt	Entscheiden sich die SuS für das DiffieHellman-Verfahren, so führen Sie das Verfahren erneut durch und beobachten dabei, wie die Übermittlung der Nachricht durch L. angegriffen wird.	Rollenspiel, LS-Gespräch
Gelenkstelle: *Beendet...*			
Erarbeitung 09:10 – 09:20 10 Min.	L. erweitert die Situationsbeschreibung um die Möglichkeit, dass die Gruppen die Kommunikation in einem einmaligen Treffen vorbereiten.	Die SuS erarbeiten, ggf. durch geeignete Einhilfen von L, ein Verfahren mit vorangehendem Austausch der geöffneten Schlösser.	Gruppenarbeit, anschließend Plenum

(Fortsetzung auf der nächsten Seite)

Tabelle 3: (Fortzsetzung)

Phase/Zeit/ Dauer	**Geplantes Verhalten der Lehrkraft/*Leitimpulse***	**Antizipierte Aktivitäten der SuS**	**Sozialform/Medien/ Materialien**
Sicherung 09:20 – 09:10 10 Min.	L bittet eine(e) Schüler(in) die Schrittfolge des Verfahrens an der Tafel festzuhalten. L fragt nach der zentralen Idee des gewählten Lösungsansatzes.	Ein(e) Schüler(in) hält die Schrittfolge des Verfahrens an der Tafel fest, die anderen SuS unterstützen ihn / sie dabei. Die SuS halten die Schrittfolge auf dem AB fest. Die SuS benennen die Trennung von Schließ- und Öffnungsfunktion als Lösung.	Schülervortrag / Tafel

7 Literatur und Internetquellen

AG DDI Freie Universität Berlin (2015). *DDI / Unterrichtsmodell Mobilfunknetz*. URL: `https://git.imp.fu-berlin.de/ddi/unterrichtsmodellmobilfunknetz/wikis/home` (besucht am 02. 01. 2017).

Brunner, Jerome S. (1974). *Entwurf Einer Unterrichtstheorie*. Bearb. von Werner Loch, Harm Paschen und Gerhard Priesemann. Bd. 5. Sprache und Lernen. Internationale Studien zur pädagogischen Anthropologie. Berlin/Düsseldorf: Berlin Verlag/Schwann.

Gramm, Andreas, Malte Buchholz und Helmut Witten (2011). "E-Mail (nur?) für Dich". In: *LOG IN* 31 (169/170).

Kiper, Hanna und Wolfgang Mischke (2006). *Einführung in die Theorie des Unterrichts*. Beltz-Studium. OCLC: 179970006. Weinheim: Beltz. 199 S.

Meyer, Hilbert (2011). *Was ist guter Unterricht?* 8. Aufl. Frankfurt am Main: Scriptor.

Rahmenlehrplan für die Sekundarstufe I: Biologie Teil C (2015). Unter Mitarb. von Senatsverwaltung für Bildung Jugend und Familie Berlin. URL: `http://bildungsserver.berlin-brandenburg.de/fileadmin/bbb/unterricht/rahmenlehrplaene/Rahmenlehrplanprojekt/amtliche_Fassung/Teil_C_Biologie_2015_11_10_WEB.pdf`.

Senatsverwaltung für Bildung, Jugend und Sport Berlin (2010). *Rahmenlehrplan für die gymnasiale Oberstufe: Informatik*. URL: `http://www.berlin.de/imperia/md/content/sen-bildung/unterricht/lehrplaene/sek2_informatik.pdf`.

8 Anlagen

8.1 Sitzplan

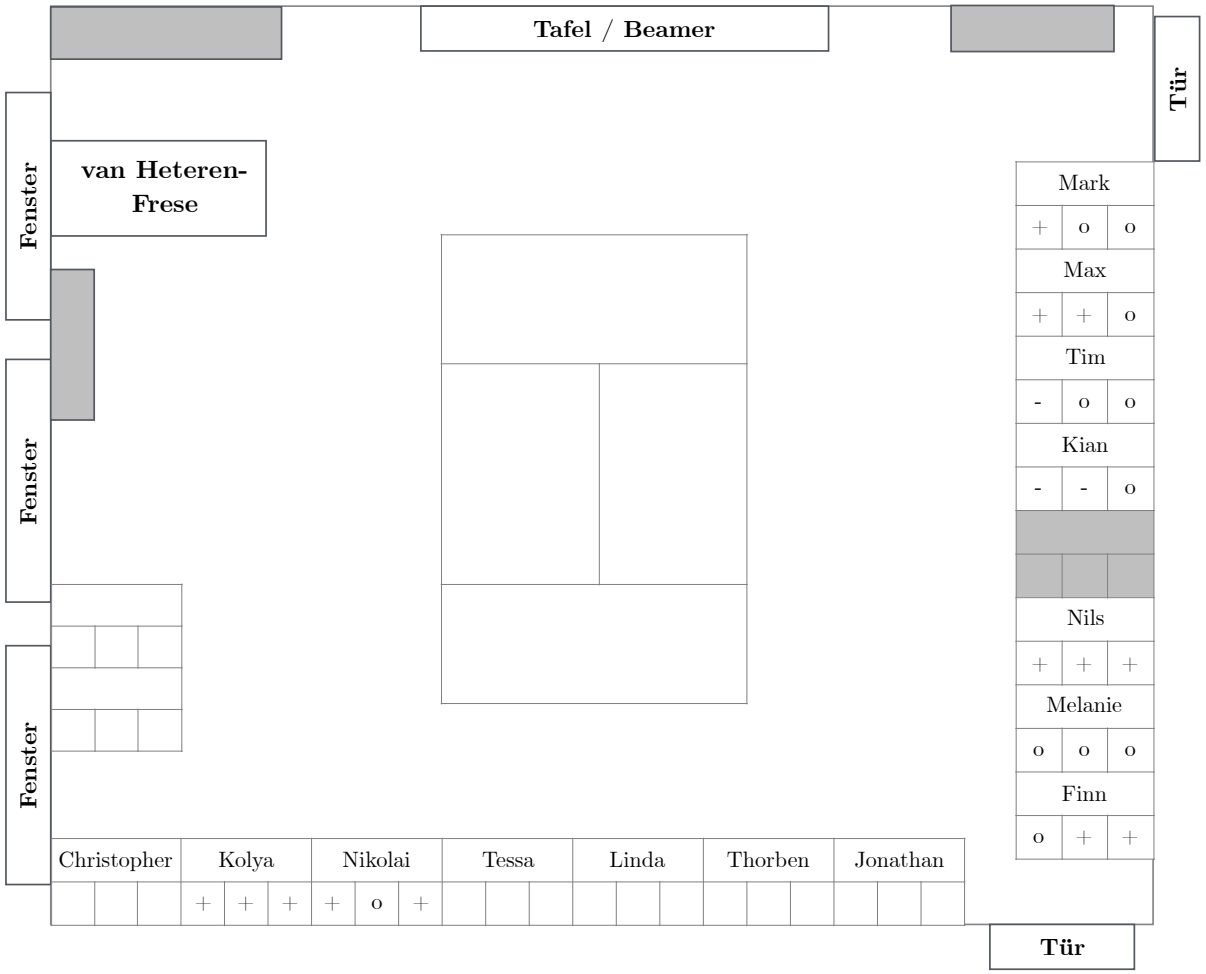

Abb. 2: Sitzplan mit Leistungseinschätzung. Reihenfolge der Bewertung: *Bezug zum Kompetenzschwerpunkt* | *Mitarbeit* | *Kooperation*.

8.2 Einschätzung der Niveaus

	Bezug zum Konpetenzschwerpunkt	**Mitarbeit**	**Kooperation**
+	kann selbstständig planen und durchführen	regelmäßig, konstruktiv	verantwortungsvoll, zeigt Initiative
o	kann mit Hilfestellungen planen und durchführen	phasenweise, meist konstruktiv	erfüllt Aufgaben zielgerichtet, erwartet Zuweisung
-	kann nur unter Anleitung und Unterstützung der Gruppe arbeiten	selten, reproduzierend	ohne eigene Aktivität