Seminar 11

Kryptologie – RSA und das Spiralcurriculum

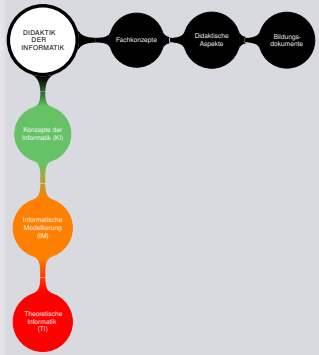
Informatikfachdidaktik

Cemre Tayyar

Seminar Didaktik der Informatik vom 11. Januar 2016

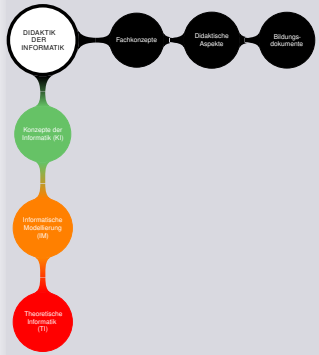
Version: 6ff982f
Stand: 2016-01-27 16:40
Bearbeitet von: Cemre Tayyar

Fachgebiet Didaktik der Informatik
Bergische Universität Wuppertal

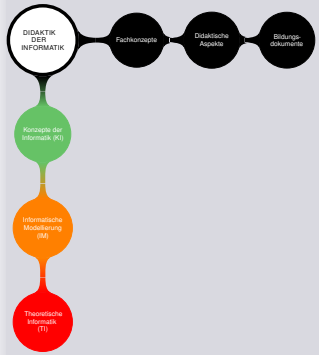


Kompetenzen – Seminar 11

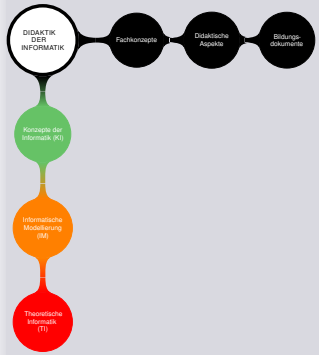
1. Stellenwert des allgemeinen Nachrichtenaustauschs in Alltagssituationen einordnen und die Wichtigkeit ihrer Verschlüsselung auf Basis der Notwendigkeit erkennen und beurteilen.
2. Bildungsdokumente bezüglich der Kryptologie – speziell des RSA-Verfahrens – untersuchen und ihre Kompetenzen erarbeiten.
3. Kryptologie in verschiedenen Schulstufen auf einem fachlich ausgewiesenem Niveau schulisch aufbereiten, einordnen und anhand von Beispielen konkretisieren und beurteilen.
4. Kriterien für den Unterrichtseinsatz von Kryptoverfahren – speziell des RSA-Verfahrens – entwickeln.



Gliederung – Seminar 11



Einführung - Was ist Kryptologie?

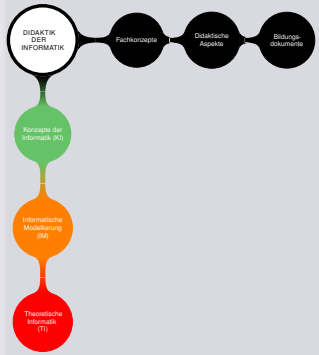


Frage

Was verstehen Sie unter *Kryptologie*?

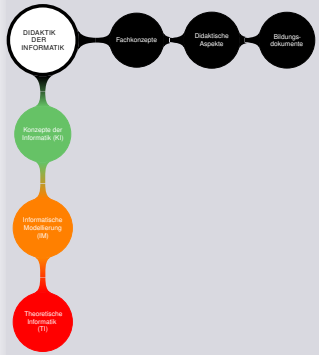
Einführung - Was ist Kryptologie?

Das Wort *Kryptologie* entstand aus dem griechischen Wort *Kryptos*, was soviel wie »versteckt«, »verborgen« und »geheim« bedeutet und aus dem Suffix *-logie*, das im Altgriechischen »Wort« oder »Sinn« bedeutet.



Definition:

Kryptologie ist die Wissenschaft der Ver- und Entschlüsselung von Nachrichten, um diese vor Dritten geheim zu halten.



Einführung - Was ist Kryptologie?

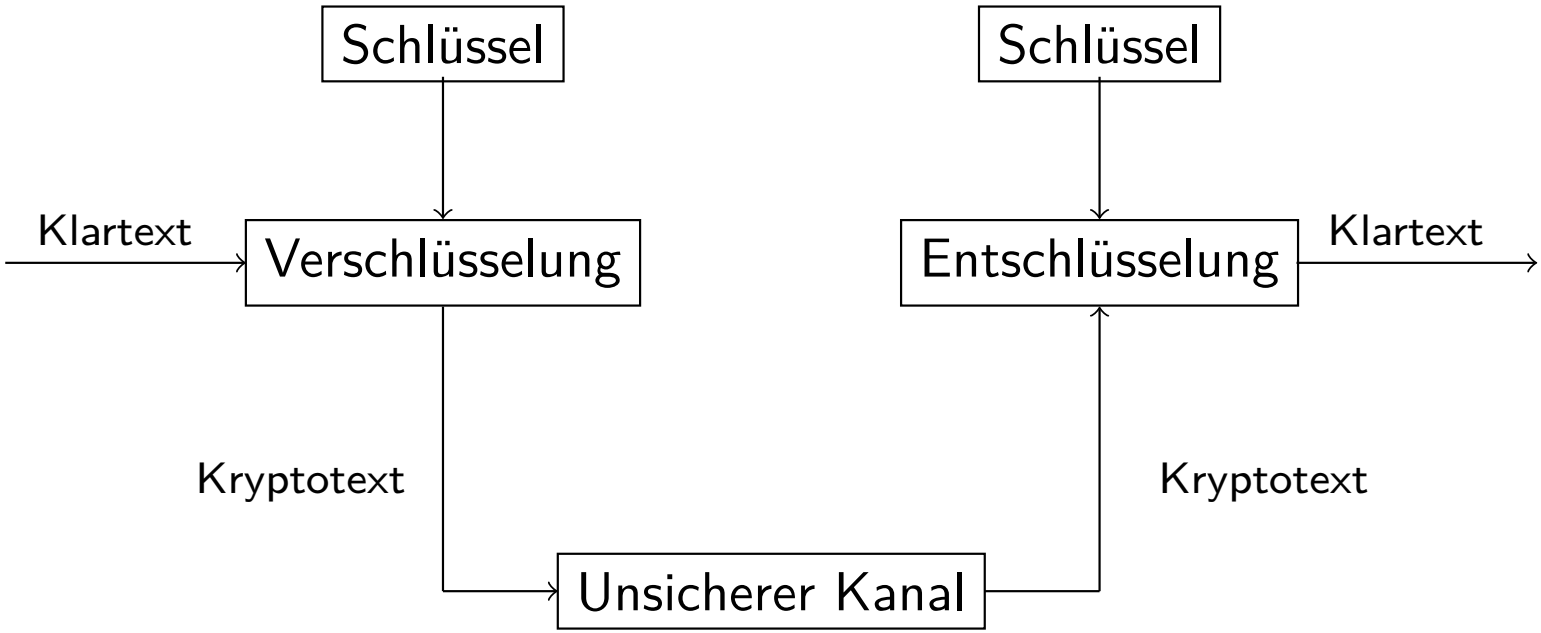
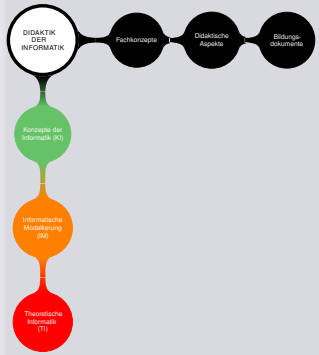


Abbildung: Prinzip eines Kryptosystems

(**Berendt1994**)



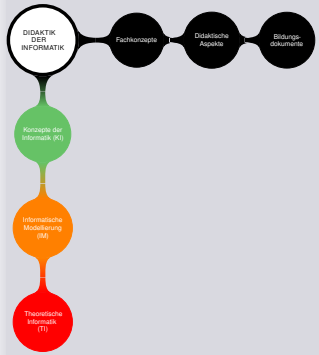
- **Symmetrische Kryptoverfahren:**

  Es gibt nur einen einzigen Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung dient, welcher über einen sicheren Kanal transportiert werden muss.

- **Asymmetrische Kryptoverfahren (Public-Key):**

  Besteht aus einem Schlüsselpaar, öffentlicher und privater Schlüssel. Der öffentliche Schlüssel dient der Verschlüsselung von Nachrichten für mich und der private der Entschlüsselung meiner Nachrichten.

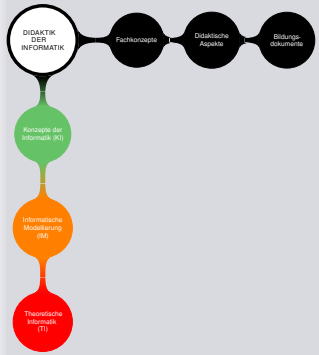
(**BongartzUnger2006**)



Kryptologie im Alltag

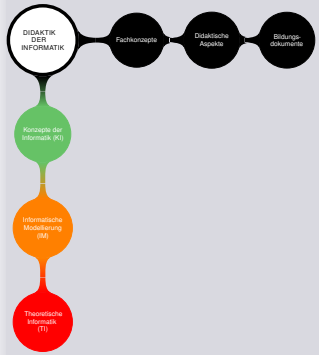
»If you think technology can solve your security problems, then you don't understand the problems and you dont't understand the technology.« Bruce Schneier

(**Schneier2000**)



Stellenwert des Nachrichtenaustauschs im Alltag

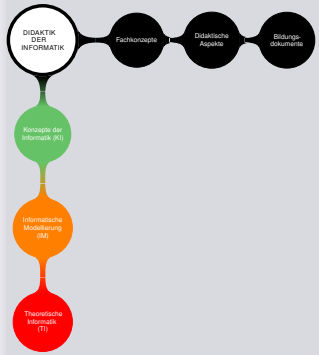
- In vielen Bereichen im Alltag findet Kommunikation statt, es werden Daten und Nachrichten ausgetauscht.
- Nicht nur in Informatiksystemen findet man Kryptoverfahren für die Verschlüsselung von Nachrichten und Daten.
- Schon Jahrhunderte v. Chr. gab es Kryptoverfahren, wie die *Skytale* und die *Cäsar-Chiffre*, für die Geheimhaltung von Botschaften, (**Berendt1994**).
- Heutzutage sind wir von Situationen umgeben, bei denen die Datensicherheit täglich eine wichtige Rolle spielt.



Stellenwert der Kryptologie im Alltag

Arbeitsauftrag

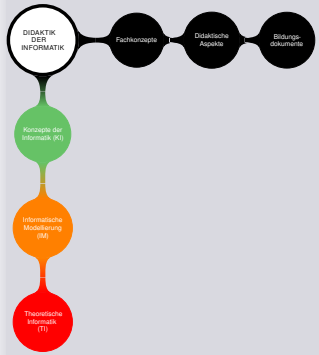
1. Nennen Sie konkrete Beispielsituationen in denen die Verschlüsselung der Daten eine wichtige Rolle spielt.
2. Was möchte *Bruce Schneier* damit sagen? Nehmen Sie Stellung zu der Aussage.

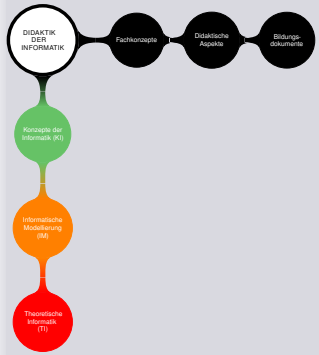


Das RSA-Verfahren

- Das RSA-Verfahren wurde von *Rivest*, *Shamir* und *Adleman* im Jahr 1977 entwickelt.
- Dieses Verfahren kann man sowohl für die Verschlüsselung, als auch für die digitale Signatur verwenden.
- Es beruht auf das Problem der Primfaktorzerlegung, und zwar darauf, dass zwei Primzahlen p, q nur mit sehr großem Aufwand aus dem Produkt n zurückzugewinnen sind.

(**Berendt1994**)





Die Schlüsselerzeugung

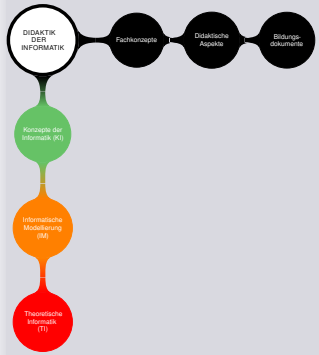
Alice möchte Bob eine verschlüsselte Nachricht versenden.

Bob

- wählt genügend große Primzahlen p und q, $p \neq q$.
- berechnet $n = p \cdot q$ und $\varphi(n) = (p-1) \cdot (q-1)$.
- wählt ein e, sodass $e < \varphi(n)$ und $\text{ggT}(e, \varphi(n)) = 1$.
- bestimmt $d < \varphi(n)$ mit $d \cdot e \equiv 1 \mod ((p-1) \cdot (q-1))$.

Bob's privater Schlüssel ist d und öffentlicher Schlüssel ist (n, e).

Die Verschlüsselung



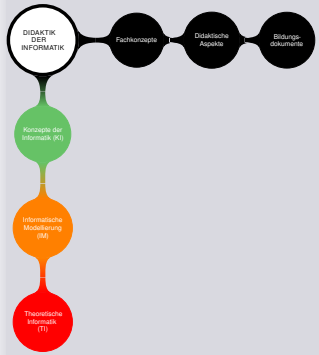
Alice

- kennt das Schlüsselpaar (n, e).
- möchte einen Klartext k $(0 \leqslant k \leqslant n)$ verschlüsseln.
- bestimmt $c := k^e \bmod n$.
- schickt Kryptotext c an Bob.

Die Entschlüsselung

Bob

- kennt n, c und seinen privaten Schlüssel d.
- berechnet $c^d \equiv k \mod n$.
- kann nun die entschlüsselte Nachricht von Alice lesen.



Die RSA-Signatur

Alice möchte die verschlüsselte Nachricht c signieren.

Signatur

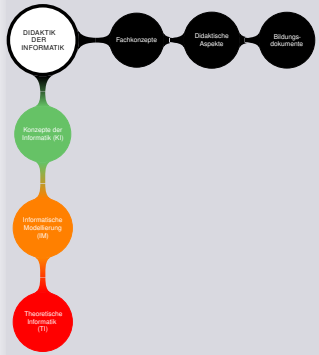
Alice

- hat ihren eigenen öffentlichen Schlüssel (m, t) und ihren privaten Schlüssel r.
- bestimmt $s := c^r \equiv k \mod m$ und schickt den signierten Kryptotext an Bob.

Verifikation

Bob

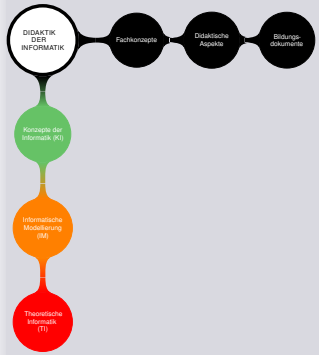
- kennt (m, t) und s.
- berechnet $s^t \equiv c \mod m$.
- muss den Kryptotext c nur noch entschlüsseln und einen sinnvollen Klartext erhalten.

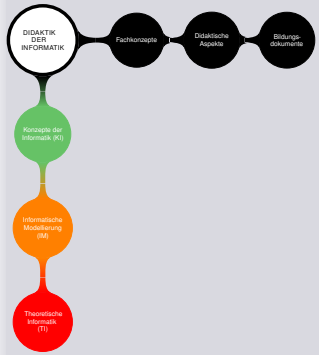


Die RSA-Signatur

Diskussion

Welches Risiko besteht beim Verwenden der RSA-Signatur bzw. welche Gefahr besteht generell bei einer beliebigen digitalen Signatur? Welche Möglichkeiten gibt es um diese Gefahr zu umgehen?





RSA in der Kryptoanalyse

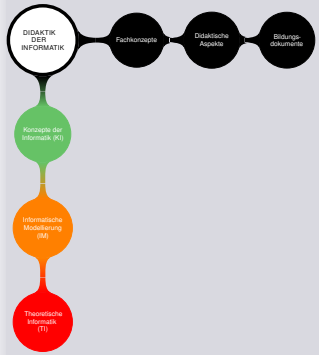
Der *Index-Calculus* ist ein Algorithmus zur Berechnung der diskreten Logarithmen. Der *Index-Calculus*-Algorithmus war für viele Verfahren eine Inspiration und wird heute als ein Oberbegriff für die, in der Tabelle sich befindenden, Algorithmen verwendet. Die folgende Tabelle zeigt den Zeitaufwand für das Brechen der *RSA-Verschlüsselung* in Abhängigkeit von vier verschiedenen *Index-Calculus*-Verfahren, (**Lange2014Bernstein**):

Angriff	**Jahr**	**RSA-1024**	**RSA-2048**
Kettenbruchme (CFRAC)	1975	2^{120}	2^{170}
Lineares Sieb (LS)	1977	2^{110}	2^{160}
Quadratisches Sieb (QS)	1982	2^{100}	2^{150}
Zahlkörpersieb (NFS)	1990	2^{80}	2^{112}

Ein Vergleich von RSA und ECC

- *Elliptic Curve Cryptography* ist ein asymmetrisches Kryptoverfahren, bei dem der diskrete Logarithmus auf eine elliptische Kurve übertragen wird.
- Der diskrete Logarithmus in einer Elliptischen Kurve ist nicht mit dem *Index-Calculus* berechenbar.
- Dennoch gibt es andere Verfahren der Kryptoanalyse, die aber noch lange nicht so schnell sind, wie z. B. *Lineare Sieb* oder *Zahlkörpersieb*.

(**Avanzi2005**)

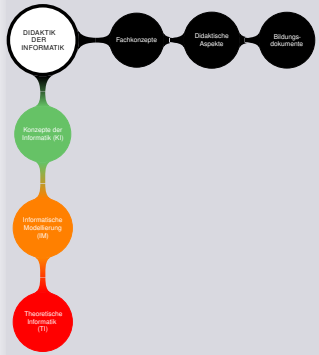


Ein Vergleich von RSA und ECC

Die folgende Tabelle gibt je nach Länge des Klartext an, wie viel Aufwand die einzelnen Verfahren benötigen, um RSA (NIST) bzw. ECC zu knacken:

Aufwand	**RSA (Bits)**	**ECC (Bits)**
2^{80}	1024	160
2^{112}	2048	224
2^{128}	3072	256
2^{192}	7680	384
2^{256}	15360	512

(**BlueKrypt2015**)



Bildungsstandards Informatik, Mensch und Gesellschaft

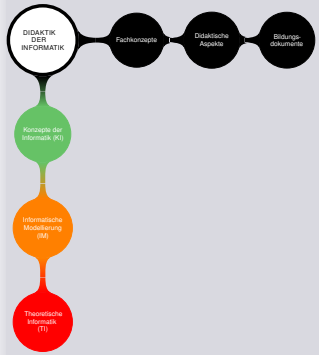
Schülerinnen und Schüler der Jahrgangsstufe 5 bis 7

- wissen, dass digitale Daten leicht manipulierbar sind.
- lernen die potenziellen Gefahren bei der Nutzung digitaler Medien an Beispielen kennen.

Schülerinnen und Schüler der Jahrgangsstufen 8 bis 10

- wenden Kriterien an, um Seriosität und Authentizität von Informationen aus dem Internet zu beurteilen.
- beschreiben an ausgewählten Beispielen, wann und wo personenbezogene Daten gewonnen, gespeichert und genutzt werden.
- bewerten Situationen, in denen persönliche Daten weitergegeben werden.
- erkennen die Unsicherheiten einfacher Verschlüsselungsverfahren.

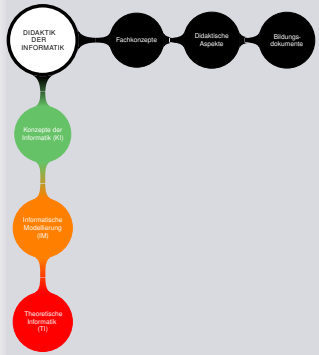
(**InformatikBildungsStandards2008**)



Interaktion mit und von Informatiksystemen Datenschutz und Datensicherheit (z. B. Kryptologie, Zugriffskontrolle).
Unterrichtliche Voraussetzungen:

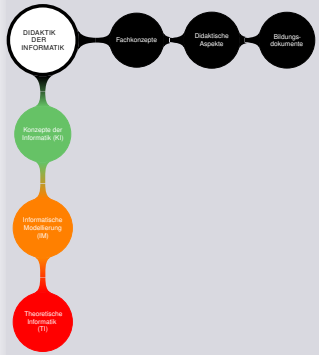
- Im Unterricht wurden symmetrische und asymmetrische Verschlüsselungsverfahren behandelt.
- Bezüglich des *RSA-Verfahrens* sind die Algorithmen zur Schlüsselerzeugung, zum Ver- und Entschlüsseln von Nachrichten und zur Authentifizierung bekannt, geübt und implementiert worden.
- Sie kennen Verfahren zur Kryptoanalyse und die Komplexität des Faktorisierungsproblems.
- Aktuelle Einsatzbereiche von Kryptographie sind im Unterricht behandelt und diskutiert worden.

(**KMK_EPA_IF2003**)



Inhaltsfeld 5: *Informatik, Mensch und Gesellschaft*
Die Schülerinnen und Schüler

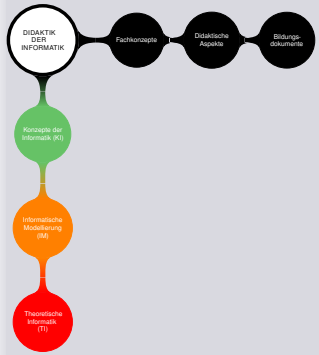
- untersuchen und bewerten anhand von Fallbeispielen Auswirkungen des Einsatzes von Informatiksystemen sowie Aspekte der Sicherheit von Informatiksystemen, des Datenschutzes und des Urheberrechts (A).
- untersuchen und bewerten Problemlagen, die sich aus dem Einsatz von Informatiksystemen ergeben, hinsichtlich rechtlicher Vorgaben, ethischer Aspekte und gesellschaftlicher Werte (A).



Inhaltsfeld 4: *Informatiksysteme*
Die Schülerinnen und Schüler

- erläutern Eigenschaften und Aufbau von Datenbanksystemen unter dem Aspekt der sicheren Nutzung (A).
- analysieren und erläutern Eigenschaften, Funktionsweisen und Einsatzbereiche symmetrischer und asymmetrischer Verschlüsselungsverfahren (A).

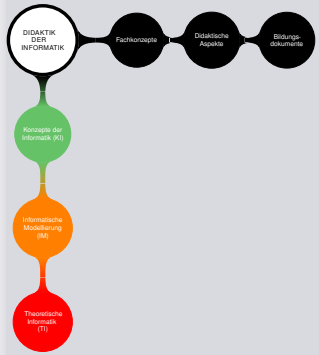
(**SILP-IF-2015**)



Informatik: Schulinterner Lehrplan zum Kernlehrplan

Unterrichtsvorhaben Einführungsphase:

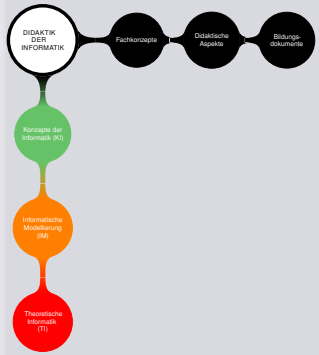
- **Thema:** Datenschutz aus informatischer Perspektive (Fragen nach Datensicherheit – Kryptologie)
- **Kompetenzen:** Die Schülerinnen und Schüler bewerten anhand von Fallbeispielen die Auswirkungen des Einsatzes von Informatiksystemen.



Unterrichtsvorhaben Qualifikationsphase 2:

- **Thema:** Sicherheit in der Informatik: Verschlüsselung und ihre Folgen
- **Verfahren:** Cäsar-Chiffre, Vigénere-Chiffre, RSA-Verschlüsselung, PGP/GPG, Hashverfahren, Diffie-Hellman uvm.
- **Implementierung:** Cäsar- und Vigénere-Verfahren implementieren, RSA im GK nur wenn die math. und implementationstech. Fähigkeiten es hergeben.

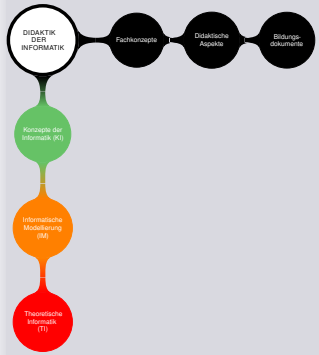
(**KMNW_KLP_IF_2013**)



RSA in der Primarstufe

Die mathematischen Grundlagen des RSA-Verfahrens, wie die Eulersche *Phi*-Funktion, die Bestimmung der privaten Schlüssel oder auch die modulare Rechnung sind selbstverständlich zu komplex für die Primarschule.
Zum Näherbringen des RSA-Verfahren werden die folgenden zwei Themenbereiche aufgegriffen:

- Rechnen mit Restklassen
- Eine Idee zur Einführung in die Kryptologie



In den Grundschulen in NRW wird die schriftliche Division in der zweiten Hälfte der 4. Klasse eingeführt (optional).

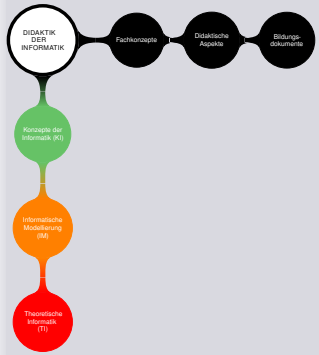
Idee:

Führe die *modulo*-Schreibweise schon in der Grundschule, wie folgt, ein:

$$\begin{array}{rl} & 17 \;:\; 5 \;=\; 3 \quad \text{Rest:} \quad 2 \\ - & 15 \\ \hline & 2 \end{array}$$

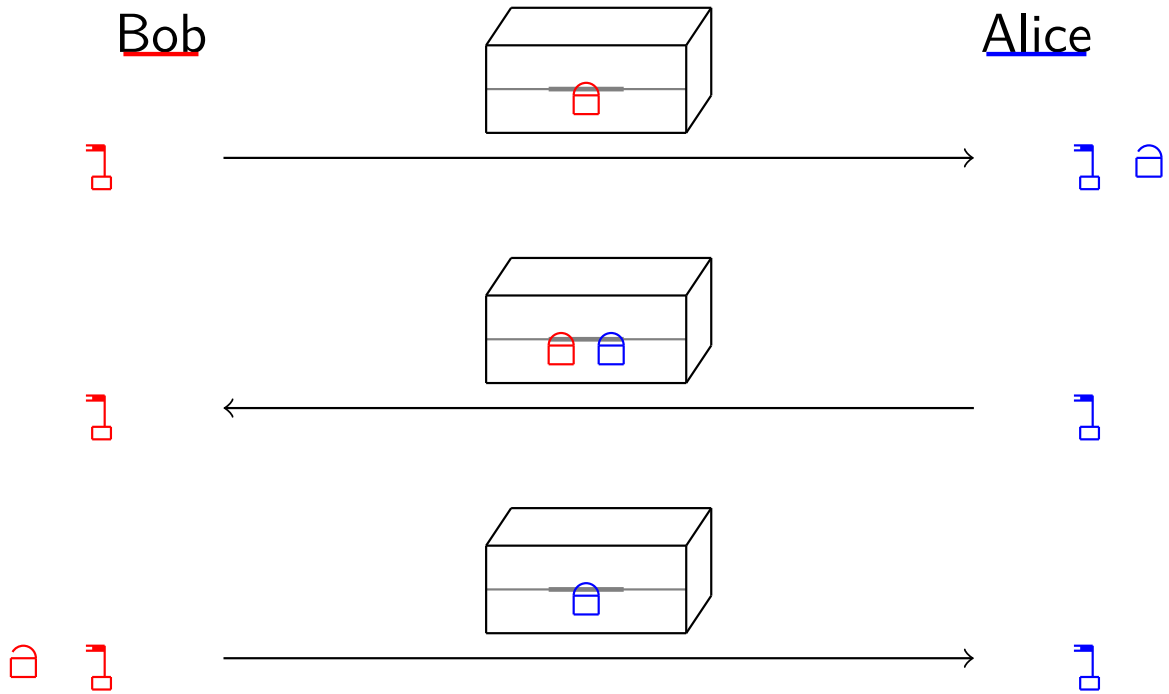
$$\text{Rest:} \quad 17 \mod 5 = 2$$

Die Einführung dieser Schreibweise ist gegebenenfalls nicht notwendig.

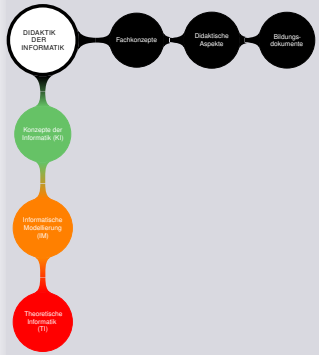


Idee:

Führe die folgenden Schritte in der Realität den Schülerinnen und Schülern vor.



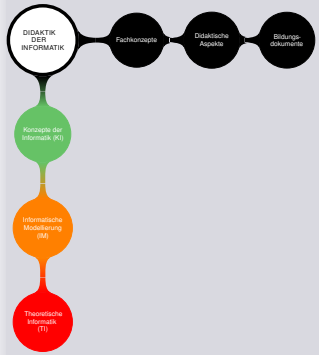
Dadurch erhalten die Schülerinnen und Schüler eine gewisse Vorstellung von der Kryptologie (**Rothe2008**).



RSA in der Primarstufe

Diskussion

Diskutieren Sie inwieweit diese Ideen in der Primarstufe umsetzbar sind und schlagen Sie gegebenenfalls Verbesserungen bzw. Ergänzungen vor.



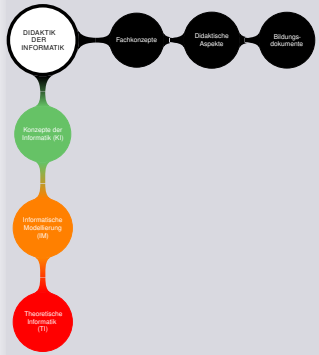
Weitere Vertiefungsmöglichkeiten des RSA-Verfahrens:

Verfahrensumsetzung:

- Chinesischer Restsatz
- Beschleunigung der modularen EXP durch binäre EXP
- Programmieren von RSA
- Verschlüsselungsverfahren (wie z. B. PGP), die RSA verwenden
- hybride Verfahren: RSA in Kombination mit symmetrischen Verfahren

Angriffsszenarien gegen RSA

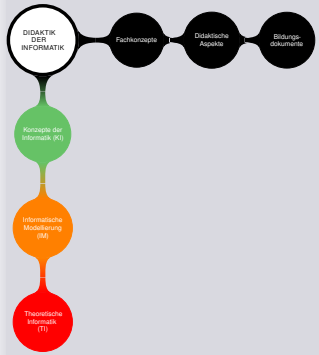
Angriffe gegen unmodifizierte RSA-Verfahren und die Gegenmaßnahmen (z. B. Padding)



RSA in der Sekundarstufe I

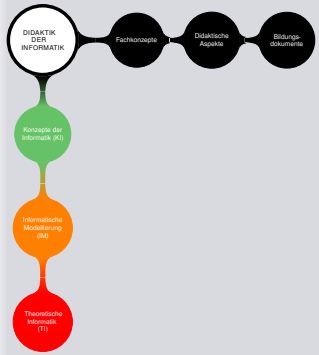
Damit die Schülerinnen und Schüler den Ablauf des RSA-Verfahrens nachvollziehen können, müssen sie vorher zwei Themengebiete kennengelernt haben:

- Bestimmung des inverses Schlüssel d
- Potenzieren in Restklassen



Beispiel: Schlüsselerzeugung

Anhand eines Beispiels kann man diese Problemzonen besser erkennen:
Seien $p = 5$ und $q = 7$ zwei vorgegebene Primzahlen und $n = 5 \cdot 7 = 35$.
$\Rightarrow \varphi(35) = 4 \cdot 6 = 24$
Wähle einen öffentlichen Schlüssel $e < 24$, derart dass $\mathrm{ggT}(e, 24) = 1$ erfüllt ist: z. B. $e = 11$.
Bestimme einen privaten Schlüssel d mit der Eigenschaft $d \cdot 11 \equiv 1 \bmod 24$.



Beispiel: Der private Schlüssel d

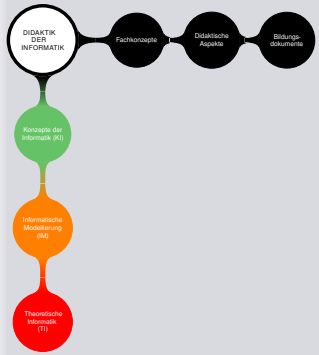
1. Möglichkeit: Multiplikationstafel

Mittels einer Multiplikationstafel kann man den Schülerinnen und Schülern den inversen Schlüssel ablesen, (**Puhlmann1998**).

2. Möglichkeit: Geeignete Beispiele

Geeignete Beispiele finden, bei denen die Division $\varphi(n) : e$ einen Rest von 1 ergeben:

$$\begin{aligned} d \cdot 3 &\equiv 1 \bmod 220 \\ \Leftrightarrow 220 : 73 &= 3, \text{ Rest } : 1 \end{aligned}$$

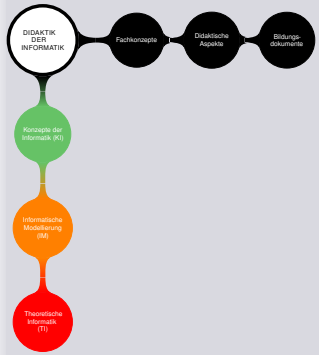


Beispiel: Der private Schlüssel d

3.Möglichkeit: (Erweiterter) euklidischer Algorithmus

$$
\begin{aligned}
24 &= 2 \cdot 11 + 2 \\
11 &= 5 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 11 - 5 \cdot 2 \\
\Rightarrow 1 &= 11 - 5 \cdot (24 - 2 \cdot 11) \\
\Rightarrow 1 &= \underline{\mathbf{+11}} \cdot 11 - 5 \cdot 24
\end{aligned}
$$



Beispiel: Verschlüsselung

Alice kennt $(n = 35, e = 11)$ und möchte den Klartext $k = 4$ verschlüsseln und anschließend an Bob verschicken. Dafür bestimmt sie:

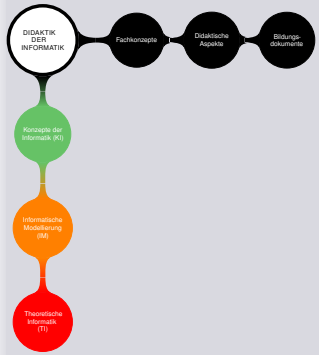
$$\begin{aligned} c : &= 4^{11} \bmod 35 \\ &= 4194304 \bmod 35 \end{aligned}$$

1. Möglichkeit: Kleine Potenzen, Taschenrechner

Bei kleineren Potenzen kann man die gewünschte Zahl mit dem Taschenrechner bestimmen.

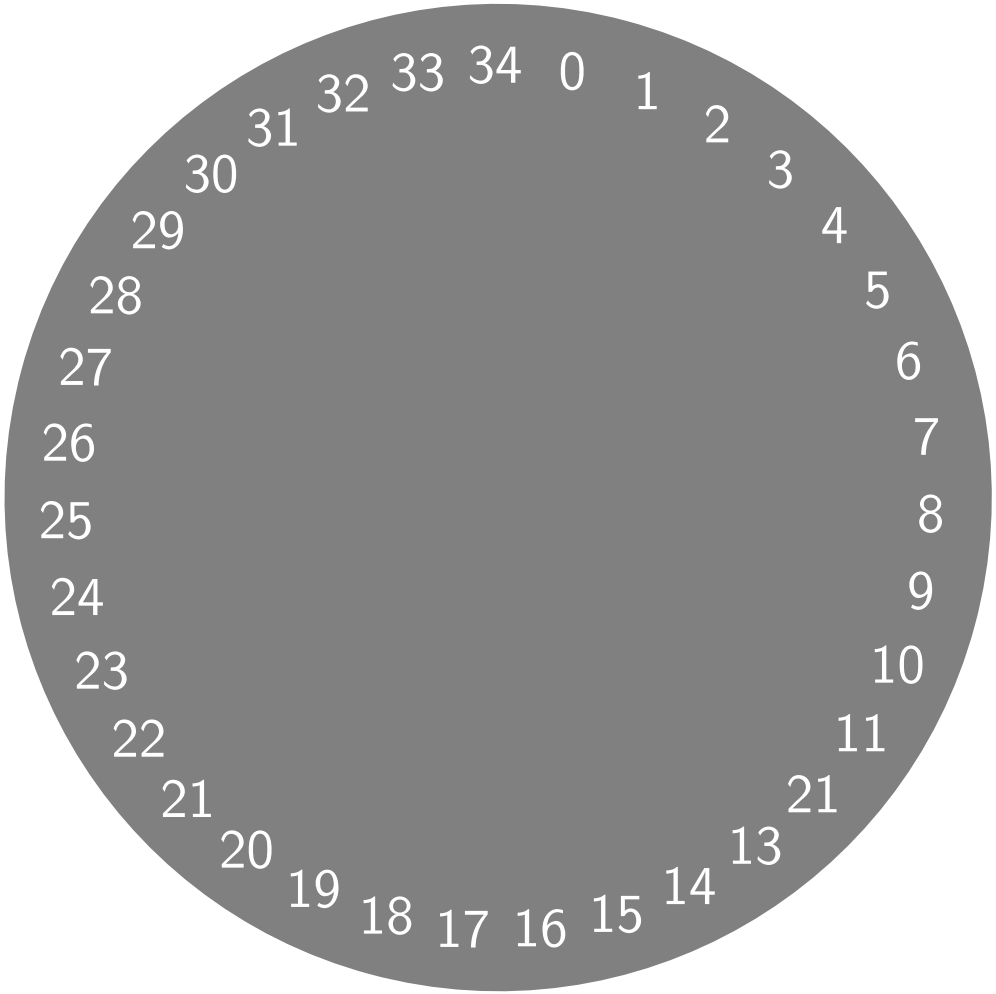
$$4194304 : 35 = 119837,2571 \quad ; \quad 119837 \cdot 35 = 4194295$$

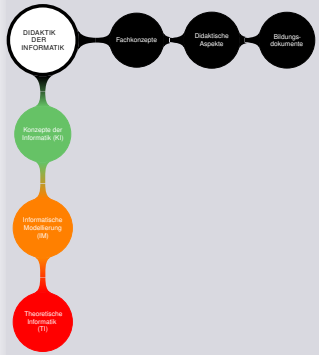
$$c = 4^{11} \bmod 35 = 4194304 - 4194295 = 9$$



2.Möglichkeit: Ringe

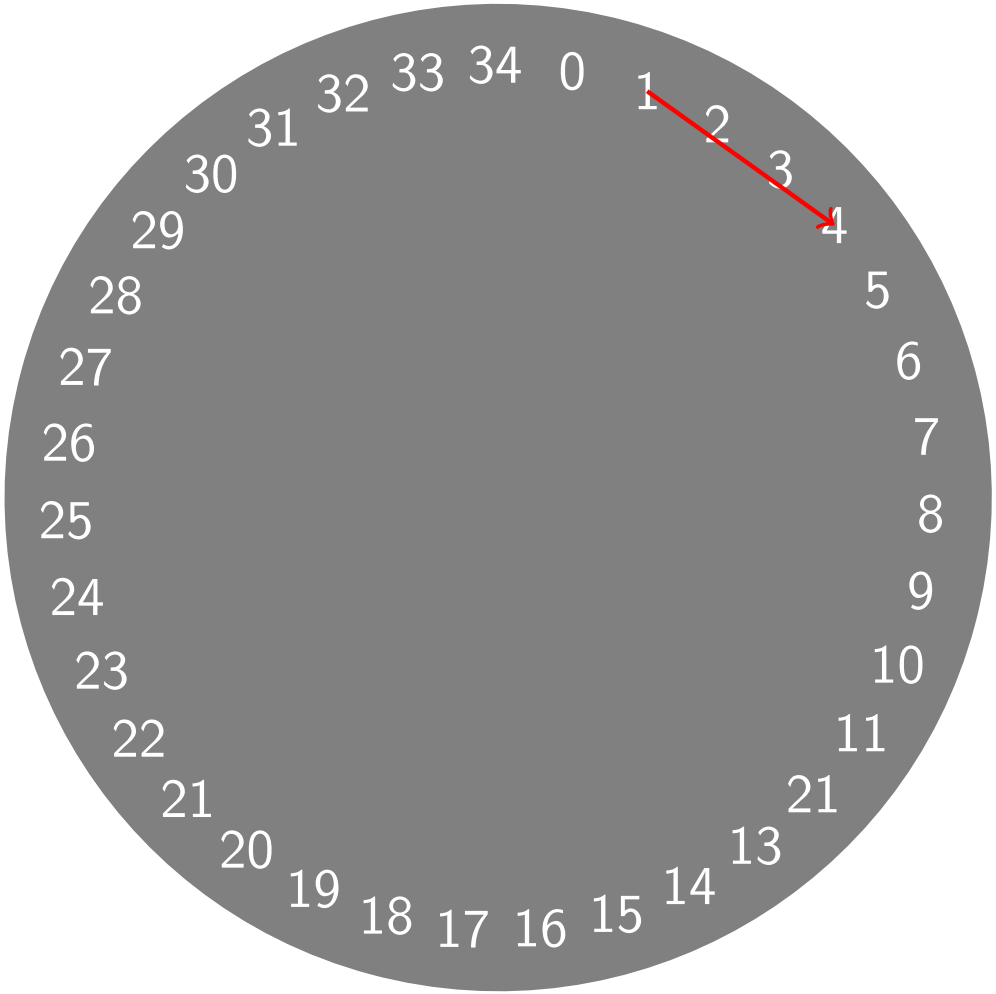
Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):

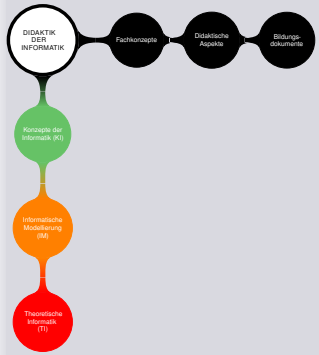




2.Möglichkeit: Ringe

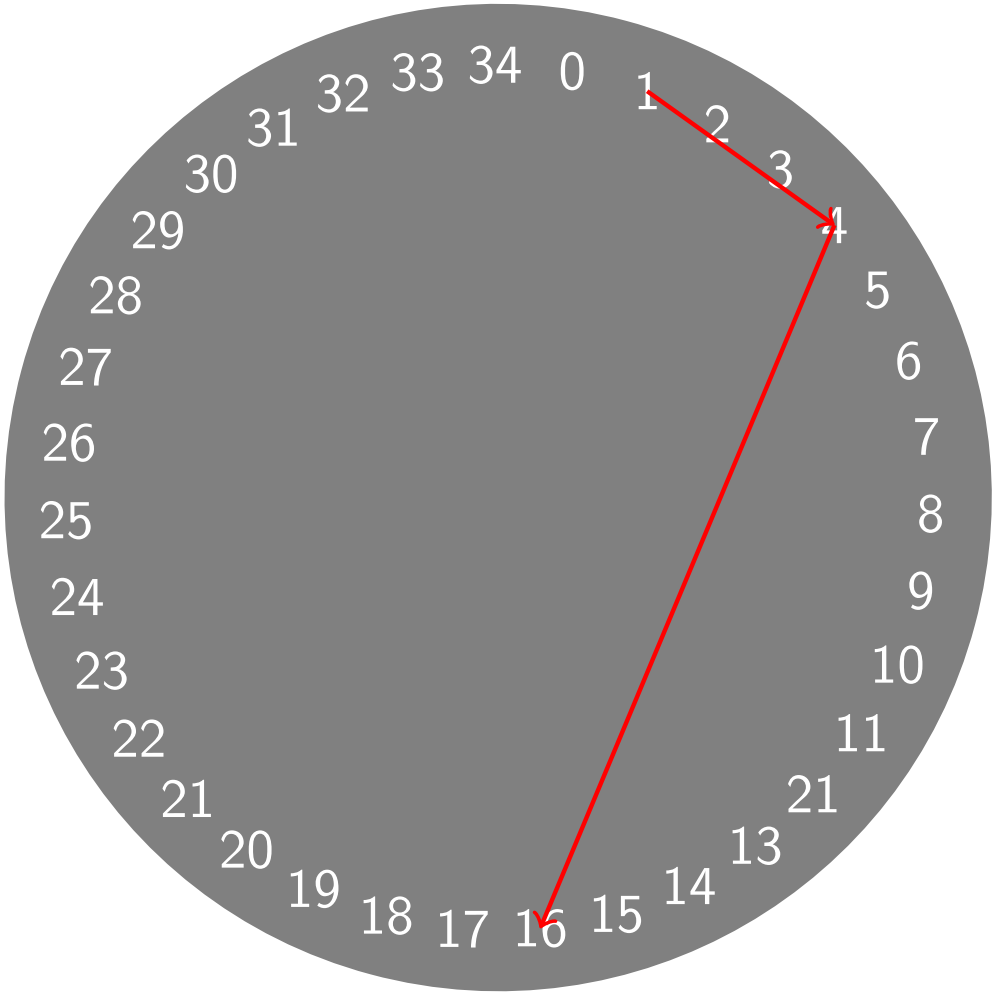
Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):

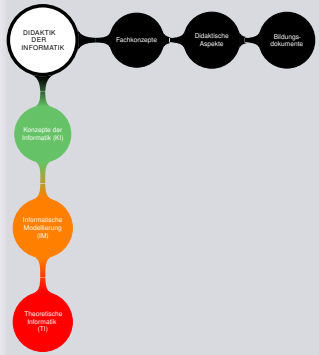




2.Möglichkeit: Ringe

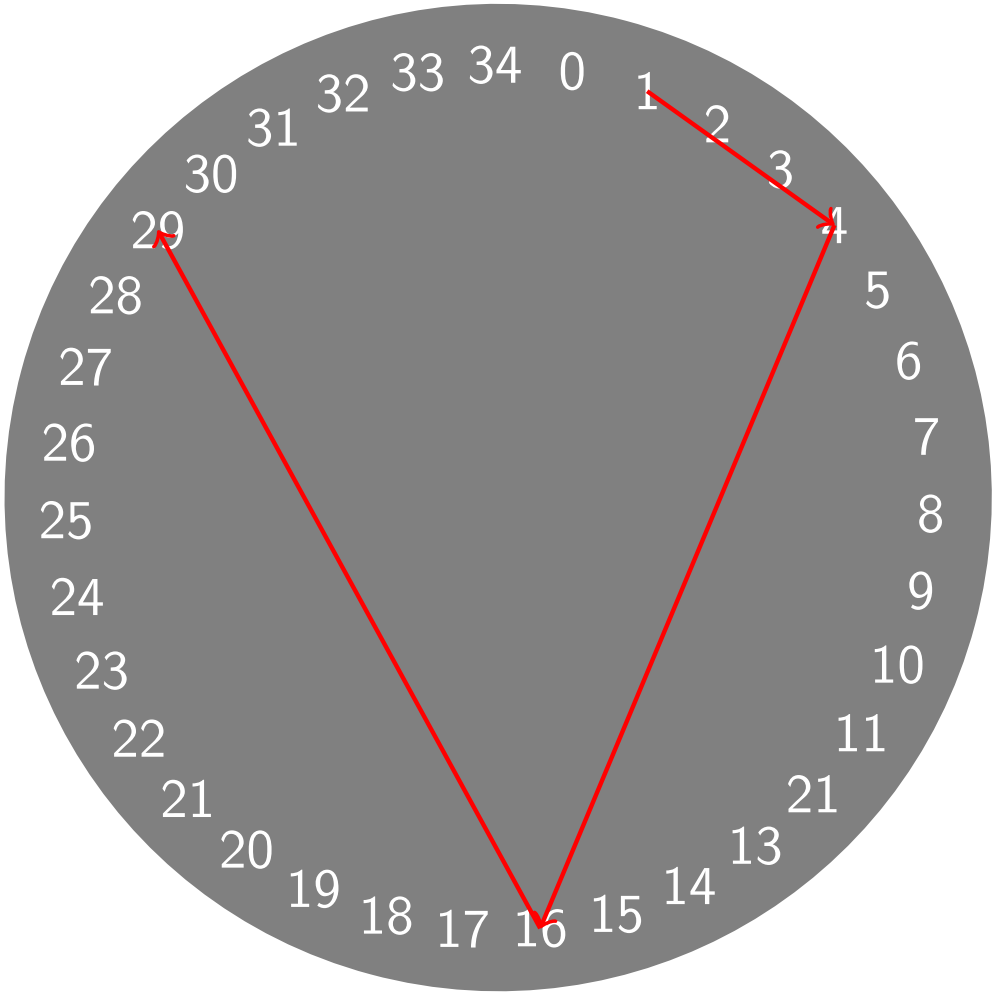
Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):

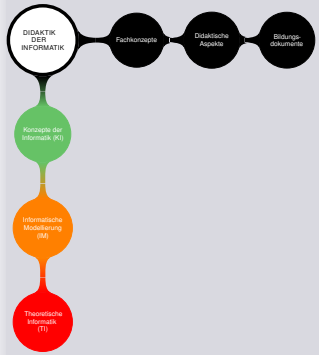




2.Möglichkeit: Ringe

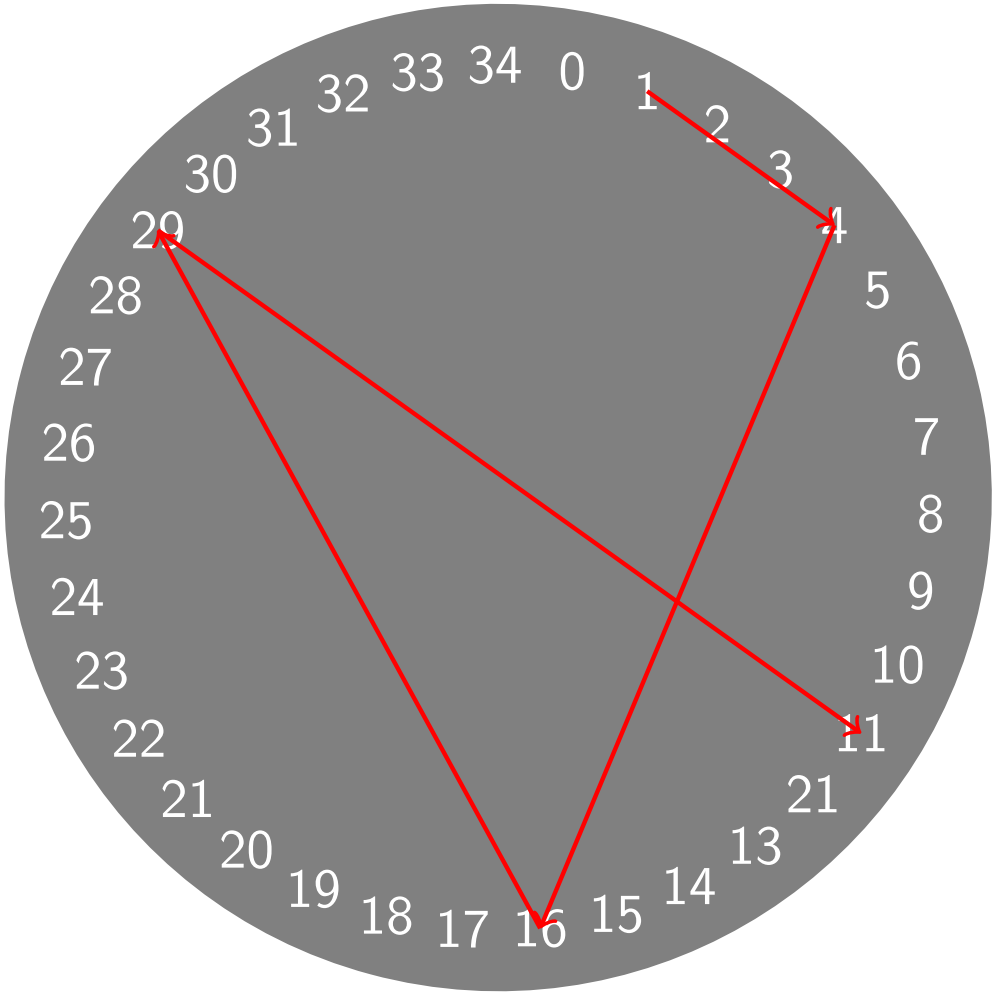
Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):

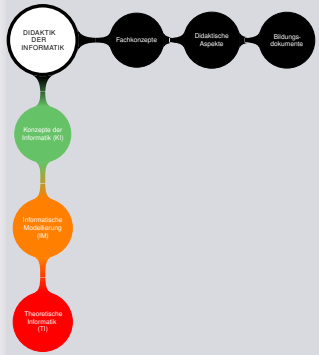




2.Möglichkeit: Ringe

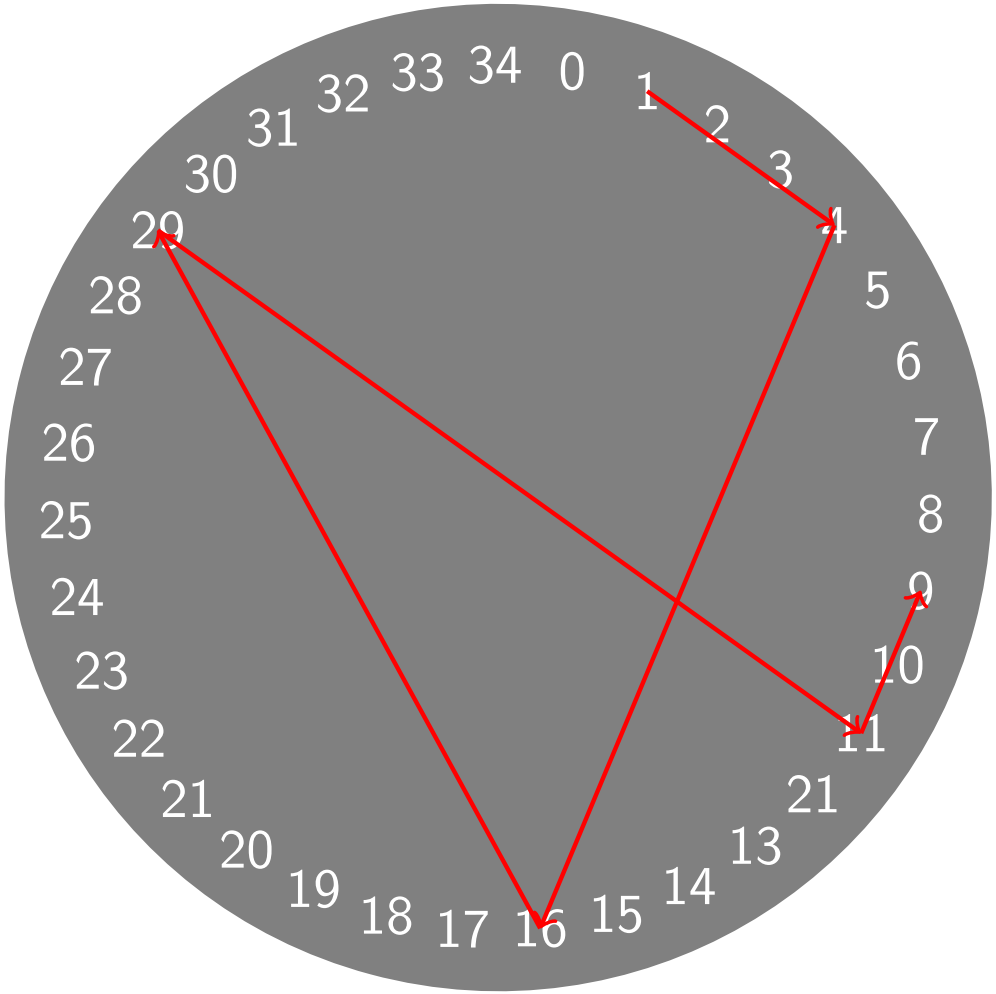
Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):

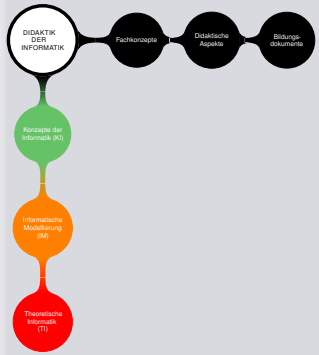




2.Möglichkeit: Ringe

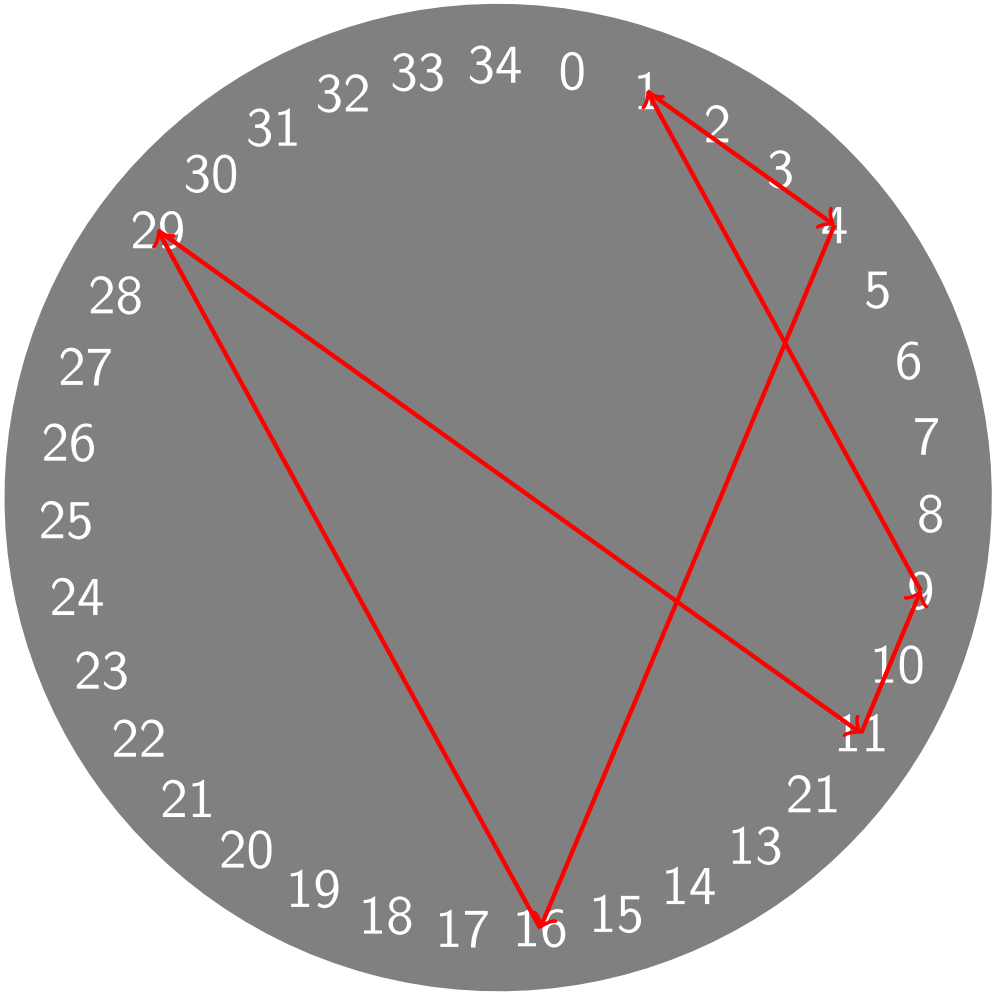
Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):

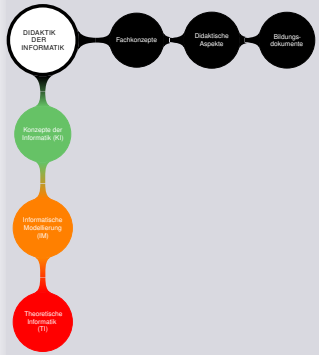




2.Möglichkeit: Ringe

Um einen experimentellen Einstieg in die Potenzrechnung in Restklassen zu verschaffen kann man z. B. die Ringe, wie folgt, illustrieren (**Puhlmann1998**):



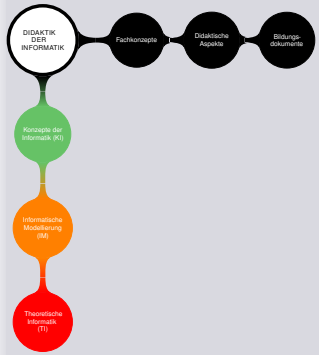


Beispiel: Entschlüsselung

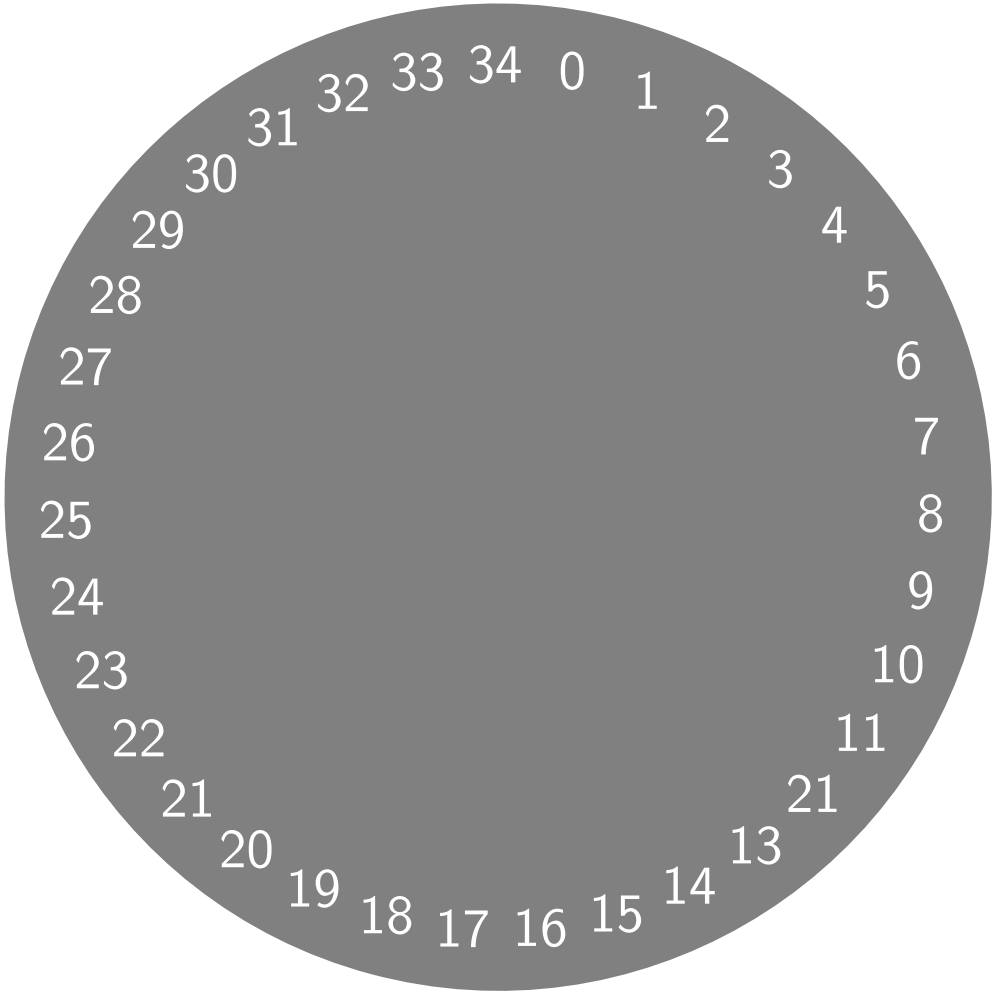
Bob entschlüsselt den Kryptotext $c = 9$ mit

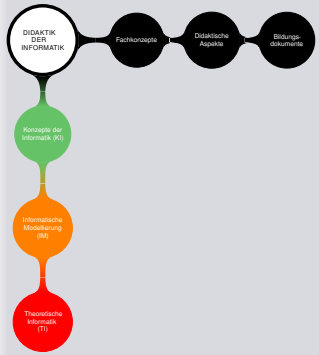
$$k = 9^{11} \bmod 35.$$

Für diese Potenz könnte man wieder den Ring verwenden.

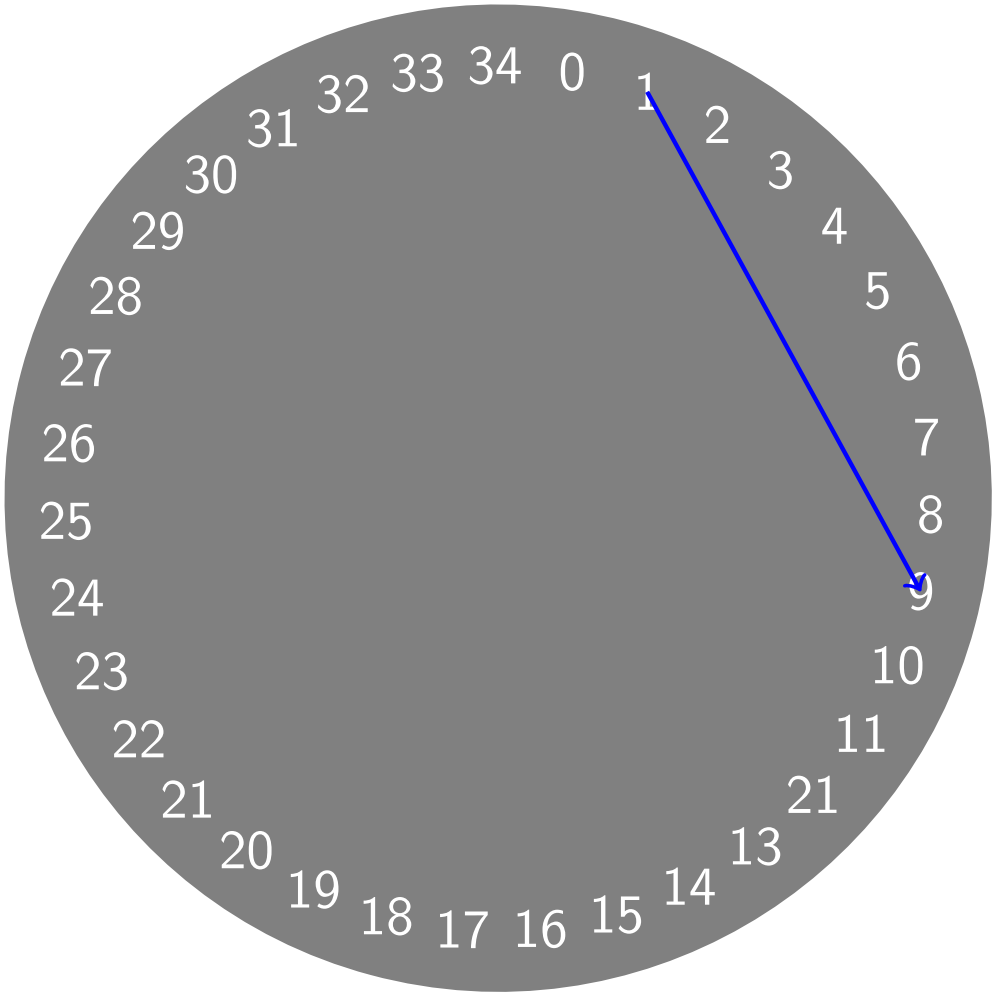


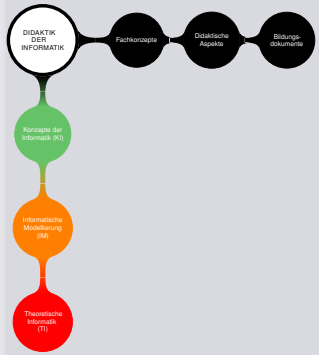
Beispiel: Entschlüsselung



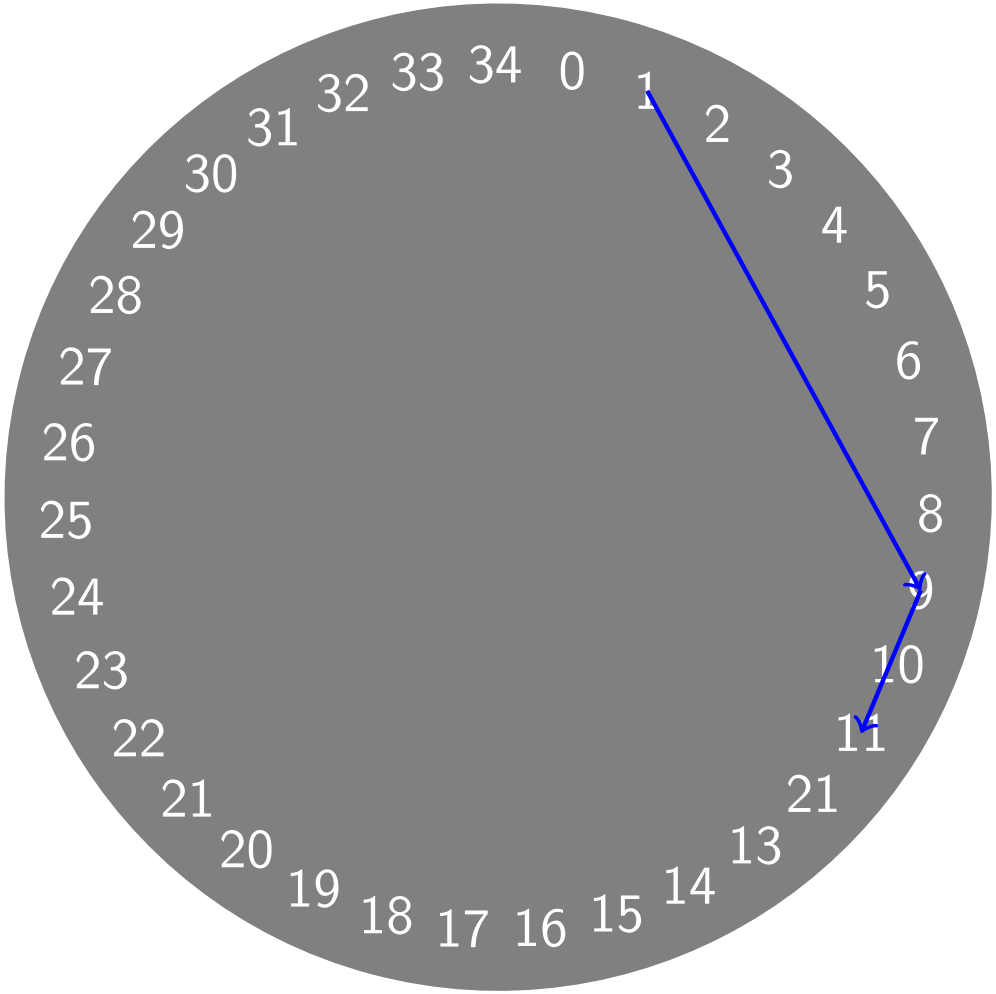


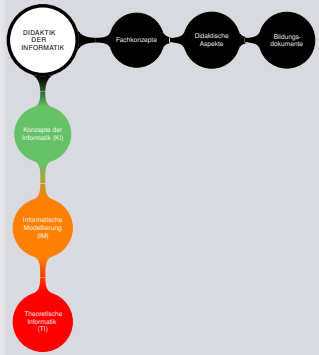
Beispiel: Entschlüsselung



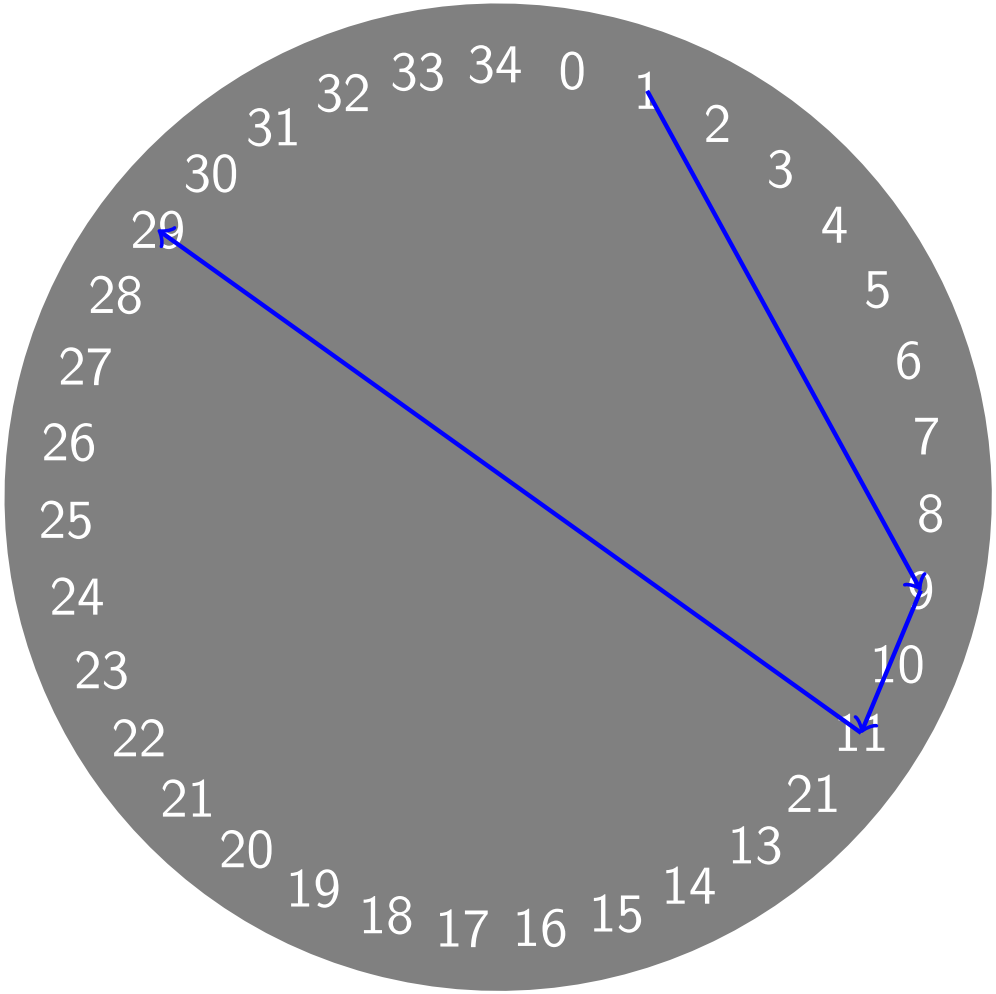


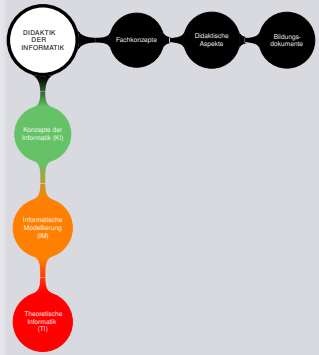
Beispiel: Entschlüsselung



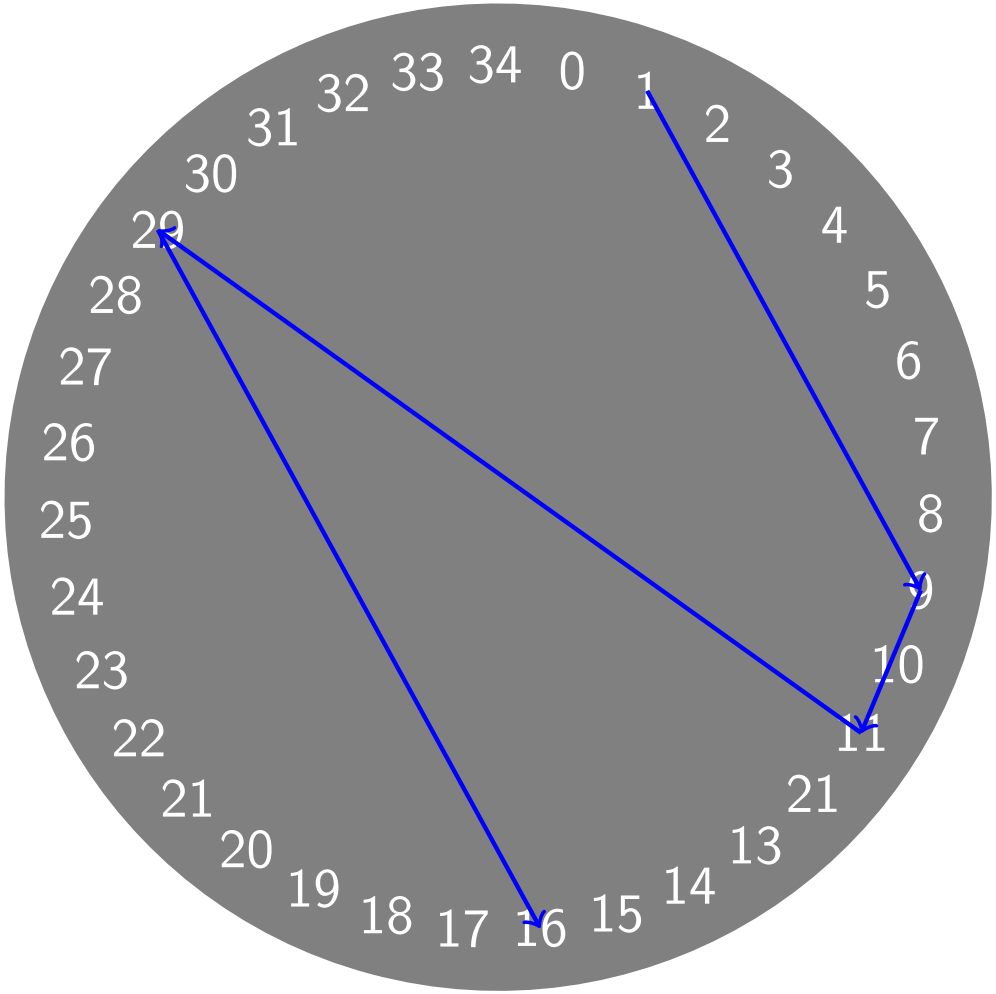


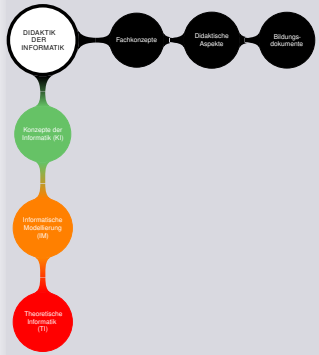
Beispiel: Entschlüsselung



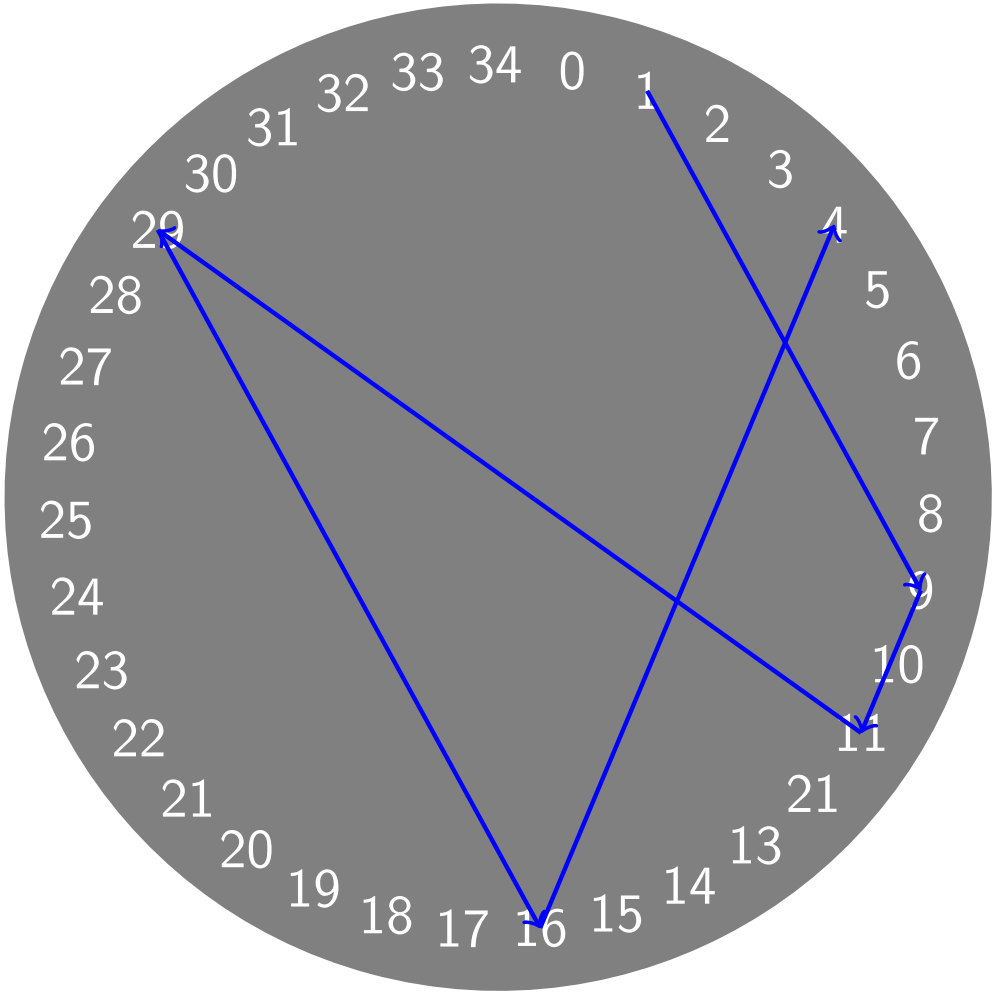


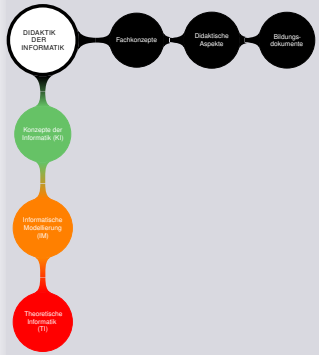
Beispiel: Entschlüsselung



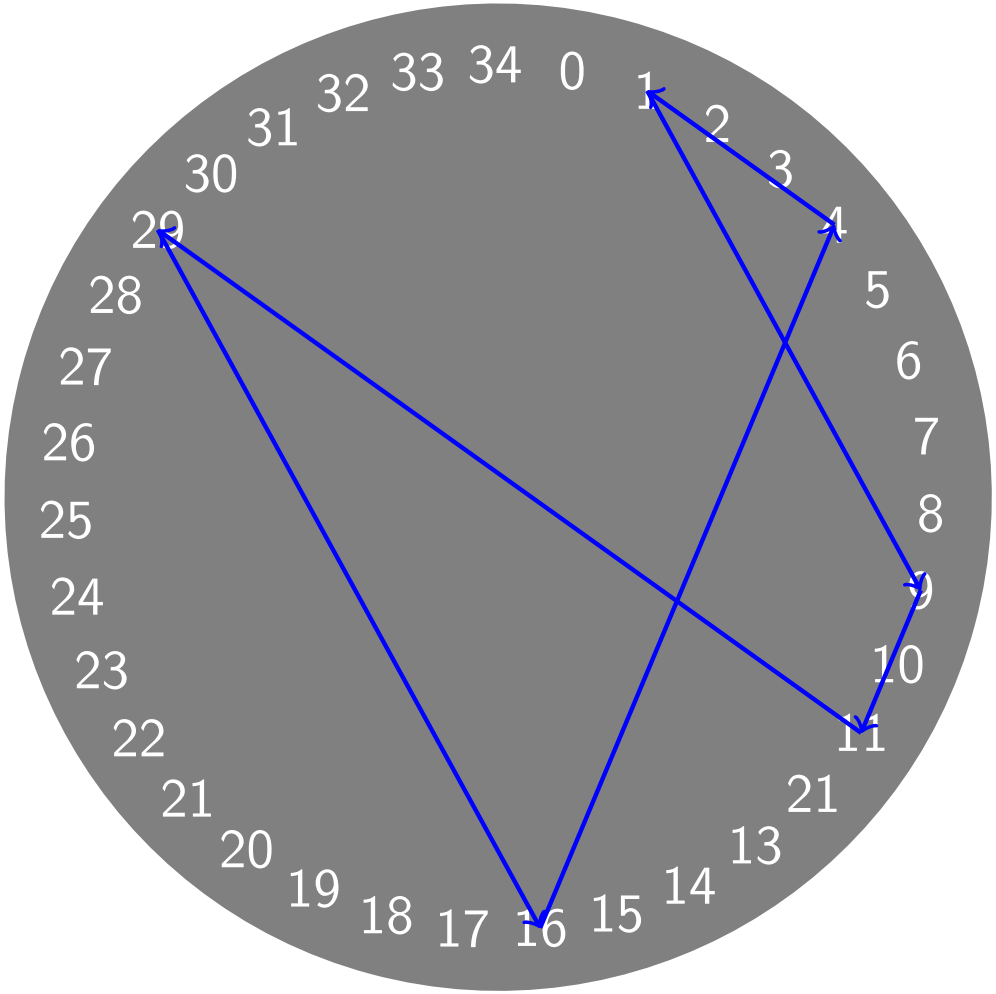


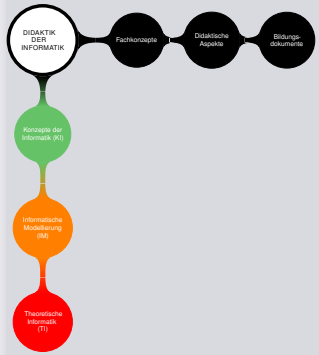
Beispiel: Entschlüsselung

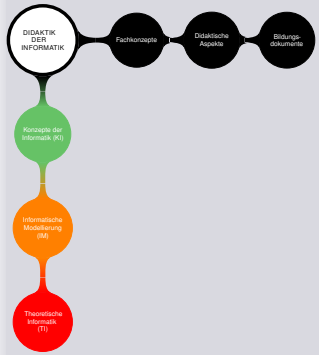




Beispiel: Entschlüsselung





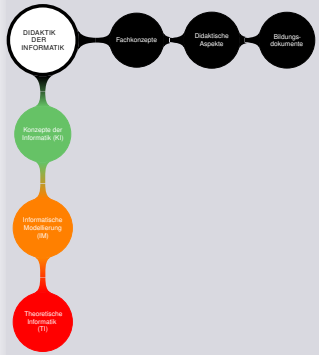


Diskussion

Beurteilen sie beide Möglichkeiten in beiden Themengebieten anhand von selbst erstellten Kriterien.

Fazit

Viele Ideen müssen auf dem jeweiligen Niveau umgesetzt, verfeinert und explizit ausgearbeitet werden.



Literatur für das Seminar I