suchen wissen

ich was suchen
ich nicht wissen was suchen
ich nicht wissen wie wissen was suchen
ich suchen wie wissen was suchen

ich wissen was suchen
ich suchen wie wissen was suchen
ich wissen ich suchen wie wissen was suchen
ich was wissen

Ernst Jandl, die bearbeitung der mütze (http://www.worte-projekt.de/jandl.html)
First results

- 18/19 students handed in their text.
- Grading "without consequences":
  - Best: 3
  - OK: 10
  - Almost OK: 3
  - Not OK: 2
- About deadlines: “No excuses”. Hand in early enough. When planning: Don’t even think to come close to the deadline.
- Meet the teacher in order to discuss your text with him. Pick a time slot…

Th, 8th Nov:
9:00
9:20
9:40
10:00
10:20
10:40
11:00
11:20
11:40
14:00
14:20
14:40
15:00
15:20
15:40
16:00
16:20

Fr, 9th Nov:
9:00
9:20
9:40
10:00
10:20
10:40
11:00
11:20
11:40
14:00
14:20
14:40
15:00
15:20
15:40
16:00
16:20

Find a slot
Initial difficulties

- What does the teacher want me to do?
- What are the habits?
- What are the no-nos?

- How to learn?
- How to deal with stress?
- How to deal with time?
- How to use time in lectures?

- How to work in a team?
- How to present results
- How to read?
- How to do exams?
- How to plan ahead?

What you should learn now:

- What I think of your work
- What you have done right
- Which mistakes you should eradicate

- That I would like to „activate“ you
- That I would like you to react to my comments
Analyzing an introduction

• Example text taken from:

1. INTRODUCTION

The rise of user-centric identity management amplifies the need for a combination of strong security and privacy protection. Anonymous credential systems are one of the most promising answers to this need. They allow users to selectively prove statements about their identity attributes.

Industry aims to employ anonymous credential systems on PCs and small devices with very limited computational power, such as cell phones and corporate or government-issued electronic identity cards. Previously proposed anonymous credential systems are not practical for such restricted devices because the complexity of proving possession of an attribute is linear in the total number of attributes in the credential.

European electronic identity cards, for instance, often contain several attributes that are either binary or discrete values from predefined finite sets. In fact, these attributes constitute the lion’s share of typical EID systems. They are partially highly privacy-sensitive and require a selective disclosure of one or more attributes, while hiding others completely (e.g., nationality, sex, civil status, hair and eye color, and applicable minority status, such as blind, partially sighted, wearing corrective lenses, or hearing-impaired). To render anonymous credential systems practical on small devices, notably electronic identity cards, we focus on efficient encoding of binary and finite-set attributes.

There exist two approaches for encoding binary or finite-set attributes in anonymous credential systems. The first method encodes each binary attribute in one attribute base (i.e., as one exponent in a discrete logarithm representation). We call this method traditional encoding. It is directly impacted by the complexity restriction mentioned: proofs of possession are linear in the total number of attribute bases. Therefore, each binary attribute burdens all credential transactions. This traditional approach precludes applications with small devices and a significant number of binary/finite-set attributes.

The second method encodes binary attributes as a bit vector in one attribute base. Clearly, this approach limits the number of attribute bases required. It therefore circumvents the linear computational complexity in the total attribute number. However, as soon as a user reveals some of the attributes in the bit vector, the complexity is linear again. It is either impacted by the total number of (binary) attributes concerned or by the length of the bit vector, depending on the particular implementation. Hence, this approach is also unacceptable for small devices.
We extend the Camenisch-Lysyanskaya (CL) credential system [Camenisch and Lysyanskaya 2001, 2003] with a finite-set encoding. It enables the efficient selective disclosure of binary and discrete-values attributes. This method overcomes the severe limitations of existing schemes. We require a solution with two key properties. (1) It uses, at most, one attribute base for all binary and finite-set attributes. (2) It impacts the proof complexity by only the number of attributes used, instead of the total number. Our extension provides a highly efficient toolkit of attribute proofs, as well as AND, OR, and NOT proofs over binary or finite-set attributes. Our approach requires a constant number of exponentiations in the number of encodable attributes and is only restricted by space considerations for the attribute exponent length in the credential and the size of the issuer’s public key.

The core idea of our article is the following. We encode binary attributes, as well as discrete values of finite sets, as products of prime numbers in a single attribute base. We use the divisibility and coprime properties to efficiently prove the attributes’ presence and absence. We also employ this technique to facilitate conjunction and disjunction proofs. Whereas earlier schemes prove equality of exponents, we prove divisibility. The efficiency of our scheme surpasses that of any existing encoding of binary and finite-set attributes.

Other cryptographic primitives with privacy protection can also benefit from our approach, particularly group signatures, blind signatures, and electronic voting schemes.

We structure the remainder of this article as follows. Section 2 covers related literature for anonymous credential systems, as well as existing methods for encoding binary attributes. Section 3 contains preliminary definitions, including the Camenisch-Lysyanskaya credential system, as well as traditional encoding variants. We define our prime encoding extensions for binary and finite-set attributes in Section 4. Section 4.1 contains the attribute representation in CL signatures, followed by the setup and encoding paradigm. We treat proofs with AND, OR, and NOT statements in Section 4.4 and propose a technique for tight interval proofs over small ranges in Section 4.5. We analyze the complexity of our scheme compared with existing approaches in Section 5, including a report on the implementation in Section 5.4. Section 6 covers the cumulated bit length of prime products as a possible limiting factor. Section 7 governs possible application scenarios, such as electronic identity cards and role-based access control. We conclude the paper in Section 8. We provide a formal protocol specification for setup and issuing in Appendix A. Appendix B considers professional taxonomies as additional application example.
1. INTRODUCTION

**The problem:** The rise of user-centric identity management amplifies the need for a combination of strong security and privacy protection.

**The solution:** Anonymous credential systems are one of the most promising answers to this need.

**The reason:** They allow users to selectively prove statements about their identity attributes.
The fact: Industry aims to employ anonymous credential systems on PCs and small devices with very limited computational power, such as cell phones and corporate or government-issued electronic identity cards.

The problem: Previously proposed anonymous credential systems are not practical for such restricted devices because the complexity of proving possession of an attribute is linear in the total number of attributes in the credential.

The example: European electronic identity cards, for instance, often contain several attributes that are either binary or discrete values from predefined finite sets. In fact, these attributes constitute the lion’s share of typical EID systems. They are partially highly privacy-sensitive and require a selective disclosure of one or more attributes, while hiding others completely (e.g., nationality, sex, civil status, hair and eye color, and applicable minority status, such as blind, partially sighted, wearing corrective lenses, or hearing-impaired).

The focus: To render anonymous credential systems practical on small devices, notably electronic identity cards, we focus on efficient encoding of binary and finite-set attributes.

The fact: There exist two approaches for encoding binary or finite-set attributes in anonymous credential systems.

The first method encodes each binary attribute in one attribute base (i.e., as one exponent in a discrete logarithm representation). We call this method traditional encoding. It is directly impacted by the complexity restriction mentioned: proofs of possession are linear in the total number of attribute bases. Therefore, each binary attribute burdens all credential transactions. This traditional approach precludes applications with small devices and a significant number of binary/finite-set attributes.

The second method encodes binary attributes as a bit vector in one attribute base. Clearly, this approach limits the number of attribute bases required. It therefore circumvents the linear computational complexity in the total attribute number. However, as soon as a user reveals some of the attributes in the bit vector, the complexity is linear again. It is either impacted by the total number of (binary) attributes concerned or by the length of the bit vector, depending on the particular implementation. Hence, this approach is also unacceptable for small devices.
The extension: We extend the Camenisch-Lysyanskaya (CL) credential system [Camenisch and Lysyanskaya 2001, 2003] with a finite-set encoding.

How does this extension improve the situation: It enables the efficient selective disclosure of binary and discrete-values attributes. This method overcomes the severe limitations of existing schemes.

What do we need? We require a solution with two key properties. 
(1) It uses, at most, one attribute base for all binary and finite-set attributes. 
(2) It impacts the proof complexity by only the number of attributes used, instead of the total number.

Why is our solution better? Our extension provides a highly efficient toolkit of attribute proofs, as well as AND, OR, and NOT proofs over binary or finite-set attributes. Our approach requires a constant number of exponentiations in the number of encodable attributes and is only restricted by space considerations for the attribute exponent length in the credential and the size of the issuer’s public key.

The core idea: The core idea of our article is the following. We encode binary attributes, as well as discrete values of finite sets, as products of prime numbers in a single attribute base. We use the divisibility and coprime properties to efficiently prove the attributes’ presence and absence. We also employ this technique to facilitate conjunction and disjunction proofs. Whereas earlier schemes prove equality of exponents, we prove divisibility. The efficiency of our scheme surpasses that of any existing encoding of binary and finite-set attributes.

Another benefit: Other cryptographic primitives with privacy protection can also benefit from our approach, particularly group signatures, blind signatures, and electronic voting schemes.
The mapping: We structure the remainder of this article as follows. Section 2 covers related literature for anonymous credential systems, as well as existing methods for encoding binary attributes. Section 3 contains preliminary definitions, including the Camenisch-Lysyanskaya credential system, as well as traditional encoding variants. We define our prime encoding extensions for binary and finite-set attributes in Section 4. Section 4.1 contains the attribute representation in CL signatures, followed by the setup and encoding paradigm. We treat proofs with AND, OR, and NOT statements in Section 4.4 and propose a technique for tight interval proofs over small ranges in Section 4.5. We analyze the complexity of our scheme compared with existing approaches in Section 5, including a report on the implementation in Section 5.4. Section 6 covers the cumulated bit length of prime products as a possible limiting factor. Section 7 governs possible application scenarios, such as electronic identity cards and role-based access control. We conclude the paper in Section 8. We provide a formal protocol specification for setup and issuing in Appendix A. Appendix B considers professional taxonomies as additional application example.

An analogy

1. INTRODUCTION

The problem: The rise of fast-food restaurants in Austria amplifies the need for a combination of adequate education in school and re-establishing the joy of eating proper and healthy food.

The solution: Cooking clubs are one of the most promising answers to this need.

The reason: They address the problem of poor eating habits in way where young people can express themselves using their own life styles.
The fact: Food industry has aimed to maximize their profit by offering unhealthy food accompanied with heavy use of commercial advertisements. This combination led to a huge success of fast-food restaurants in recent years.

The problem: However, this extraordinary success also led to an increase of specific eating-related diseases in Austria.

The example: The fast-food company McUneatable, for instance, often uses ingredients that are either binary or discrete values from predefined finite sets. In fact, these attributes constitute the lion’s share of typical EID systems. They are partially highly privacy-sensitive and require a selective disclosure of one or more attributes, while hiding others completely (e.g., nationality, sex, civil status, hair and eye color, and applicable minority status, such as blind, partially sighted, wearing corrective lenses, or hearing-impaired).

The focus: To counter the rise of eating-related diseases in Austria, we focus on effectively establishing cooking clubs in small towns and villages.

The fact: There exist two approaches for establishing cooking clubs.

The first method encodes each binary attribute in one attribute base (i.e., as one exponent in a discrete logarithm representation). We call this method traditional encoding. It is directly impacted by the complexity restriction mentioned: proofs of possession are linear in the total number of attribute bases. Therefore, each binary attribute burdens all credential transactions. This traditional approach precludes applications with small devices and a significant number of binary/finite-set attributes.

The second method encodes binary attributes as a bit vector in one attribute base. Clearly, this approach limits the number of attribute bases required. It therefore circumvents the linear computational complexity in the total attribute number. However, as soon as a user reveals some of the attributes in the bit vector, the complexity is linear again. It is either impacted by the total number of (binary) attributes concerned or by the length of the bit vector, depending on the particular implementation. Hence, this approach is also unacceptable for small devices.
**The extension:** We extend the Camenisch-Lysyanskaya (CL) credential system [Camenisch and Lysyanskaya 2001, 2003] with a finite-set encoding.

**How does this extension improve the situation:** It enables the efficient selective disclosure of binary and discrete-values attributes. This method overcomes the severe limitations of existing schemes.

**What do we need?** We require a solution with two key properties:
1. It uses, at most, one attribute base for all binary and finite-set attributes.
2. It impacts the proof complexity by only the number of attributes used, instead of the total number.

**Why is our solution better?** Our extension provides a highly efficient toolkit of attribute proofs, as well as AND, OR, and NOT proofs over binary or finite-set attributes. Our approach requires a constant number of exponentiations in the number of encodable attributes and is only restricted by space considerations for the attribute exponent length in the credential and the size of the issuer’s public key.

**The core idea:**

The core idea of our article is the following.

We encode binary attributes, as well as discrete values of finite sets, as products of prime numbers in a single attribute base.

We use the divisibility and coprime properties to efficiently prove the attributes’ presence and absence.

We also employ this technique to facilitate conjunction and disjunction proofs.

Whereas earlier schemes prove equality of exponents, we prove divisibility.

The efficiency of our scheme surpasses that of any existing encoding of binary and finite-set attributes.

**Another benefit:** Other cryptographic primitives with privacy protection can also benefit from our approach, particularly group signatures, blind signatures, and electronic voting schemes.
The mapping: We structure the remainder of this article as follows. Section 2 covers related literature for anonymous credential systems, as well as existing methods for encoding binary attributes. Section 3 contains preliminary definitions, including the Camenisch-Lysyanskaya credential system, as well as traditional encoding variants. We define our prime encoding extensions for binary and finite-set attributes in Section 4. Section 4.1 contains the attribute representation in CL signatures, followed by the setup and encoding paradigm. We treat proofs with AND, OR, and NOT statements in Section 4.4 and propose a technique for tight interval proofs over small ranges in Section 4.5. We analyze the complexity of our scheme compared with existing approaches in Section 5, including a report on the implementation in Section 5.4. Section 6 covers the cumulated bit length of prime products as a possible limiting factor. Section 7 governs possible application scenarios, such as electronic identity cards and role-based access control. We conclude the paper in Section 8. We provide a formal protocol specification for setup and issuing in Appendix A. Appendix B considers professional taxonomies as additional application example.

1. INTRODUCTION

The rise of user-centric identity management amplifies the need for a combination of strong security and privacy protection. Anonymous credential systems are one of the most promising answers to this need. They allow users to selectively prove statements about their identity attributes.

Industry aims to employ anonymous credential systems on PCs and small devices with very limited computational power, such as cell phones and corporate or government-issued electronic identity cards. Previously proposed anonymous credential systems are not practical for such restricted devices because the complexity of proving possession of an attribute is linear in the total number of attributes in the credential.
European electronic identity cards, for instance, often contain several attributes that are either binary or discrete values from predefined finite sets. In fact, these attributes constitute the lion’s share of typical EID systems. They are partially highly privacy-sensitive and require a selective disclosure of one or more attributes, while hiding others completely (e.g., nationality, sex, civil status, hair and eye color, and applicable minority status, such as blind, partially sighted, wearing corrective lenses, or hearing-impaired). To render anonymous credential systems practical on small devices, notably electronic identity cards, we focus on efficient encoding of binary and finite-set attributes.

There exist two approaches for encoding binary or finite-set attributes in anonymous credential systems. The first method encodes each binary attribute in one attribute base (i.e., as one exponent in a discrete logarithm representation). We call this method traditional encoding. It is directly impacted by the complexity restriction mentioned: proofs of possession are linear in the total number of attribute bases. Therefore, each binary attribute burdens all credential transactions. This traditional approach precludes applications with small devices and a significant number of binary/finite-set attributes.

The second method encodes binary attributes as a bit vector in one attribute base. Clearly, this approach limits the number of attribute bases required. It therefore circumvents the linear computational complexity in the total attribute number. However, as soon as a user reveals some of the attributes in the bit vector, the complexity is linear again. It is either impacted by the total number of (binary) attributes concerned or by the length of the bit vector, depending on the particular implementation. Hence, this approach is also unacceptable for small devices.

We extend the Camenisch-Lysyanskaya (CL) credential system [Camenisch and Lysyanskaya 2001, 2003] with a finite-set encoding. It enables the efficient selective disclosure of binary and discrete-values attributes. This method overcomes the severe limitations of existing schemes. We require a solution with two key properties. (1) It uses, at most, one attribute base for all binary and finite-set attributes. (2) It impacts the proof complexity by only the number of attributes used, instead of the total number. Our extension provides a highly efficient toolkit of attribute proofs, as well as AND, OR, and NOT proofs over binary or finite-set attributes. Our approach requires a constant number of exponentiations in the number of encodable attributes and is only restricted by space considerations for the attribute exponent length in the credential and the size of the issuer’s public key.
The core idea of our article is the following. We encode binary attributes, as well as discrete values of finite sets, as products of prime numbers in a single attribute base. We use the divisibility and coprime properties to efficiently prove the attributes' presence and absence. We also employ this technique to facilitate conjunction and disjunction proofs. Whereas earlier schemes prove equality of exponents, we prove divisibility. The efficiency of our scheme surpasses that of any existing encoding of binary and finite-set attributes.

Other cryptographic primitives with privacy protection can also benefit from our approach, particularly group signatures, blind signatures, and electronic voting schemes.

We structure the remainder of this article as follows. Section 2 covers related literature for anonymous credential systems, as well as existing methods for encoding binary attributes. Section 3 contains preliminary definitions, including the Camenisch-Lysyanskaya credential system, as well as traditional encoding variants. We define our prime encoding extensions for binary and finite-set attributes in Section 4. Section 4.1 contains the attribute representation in CL signatures, followed by the setup and encoding paradigm. We treat proofs with AND, OR, and NOT statements in Section 4.4 and propose a technique for tight interval proofs over small ranges in Section 4.5. …

Before we go on: Tasks for this week

- Define a work mode with your partner. I want to know about it.
- Search and research.
- Sort material.
- Select material.
- Make a mindmap.
- Try to understand your topic.
- Prepare your oral presentation together with your group partner. 2x2 minutes. Stay simple. Hand in slides by 10:00 to the teacher.
Your next text

• Beginning – middle – end.
• Write an “introduction”.
• In the mapping you explain what you intend to research next and what you plan to have in your final paper.

• Preferably use Latex.
• List references at the end of your test. Refer to them in the text.
Erster Vortragstermin

• 2 x je 2 min

• Der Vortrag muss mit audiovisuellen Medien unterstützt werden. Muss nicht unbedingt.

• Die Präsentationen (Powerpoint-Files oder PDF) sollten Sie auf USB-Stick/CD-ROM zu Ihrem Vortragstermin mitbringen. Es ist auch erlaubt ein eigenes Notebook zu verwenden. Tun Sie das nicht.

Schedule

1. Internet of Things
2. Secure cloud computing
3. Virtual machines
4. Symmetric cryptography
5. Side-channel analysis
6. Mobile security
7. Advanced electronic signatures
8. Fault analysis
9. Identity theft
10. Secure code writing
Two times two minutes

- Introduction: “My name is N.N. Together with my colleague N.N. we work on…” State your topic. What is it about?
- Why is your problem important?
- Give some facts.
- End: “My colleague Walter will now continue by explaining… discussing…and concluding…”

- Intro: “Thank you for introducing me. OK. So our topic is such and such. I will now briefly show what we have found so far, and discuss some open questions. Finally, I will conclude this talk by sketching our plans.”
- Explain what you have found (= researched) so far.
- Discuss some existing open questions (from your point of view.
- Conclusion: What comes next? What are your plans?
- Outro: “This is the end of our presentation. I want to thank you for your attention.”

And a tip…

Dear Mr Posch,

we would like to ask for an extension of the deadline for handing in the first version of our Seminararbeit.

We know that the current deadline is the 11th of November, 23:59. Please, take into account that we already have handed in a first text. We really hope that you grant an extension; we propose to hand in the Seminararbeit at the latest by Friday, Nov 16th, 2 pm.

Thank you in advance.
And now for something completely different.

The source

Martha Boeglin:
Wissenschaftlich arbeiten – Schritt für Schritt.
Gelassen und effektiv studieren;
W. Fink UTB 2007. [€13,30]

- Organise yourself
  - Space
  - Time
  - Emotions
  - Learning
- Get informed
- Write, write, write, write.
Time: Meetings. Deadlines. Deliverables.

- **We, Nov 7**
  - seminar: working in science

- **Su, Nov 11, 23:59**
  - first summary of research

- **We, Nov 14**
  - short presentations; hand in slides by 10 am.

- **We, Nov 21**
  - seminar: writing

- **Tue, Nov 27, 14:00**
  - deadline for draft version

- **We, Nov 28**
  - review short presentations

- **We, Dec 5**
  - seminar: presenting

- **Su, Dec 9, 23:59**
  - deadline for final version

- **Mo, Dec 10, 8:15**
  - presentations & discussion

- **We, Dec 12, 16:30**
  - presentations & discussion

- **Upon appointment:**
  - individual review with trainer

And when do YOU work on the deliverables?
Calender

Time: Meetings. Deadlines. Deliverables.

- **We, Nov 7**  
  seminar: working in science

- **Su, Nov 11, 23:59**  
  first summary of research

- **We, Nov 14**  
  short presentations; hand in slides by 10 am.

- **We, Nov 14**  
  seminar: writing

- **Tu, Nov 27, 23:59**  
  deadline for draft

- **We, Nov 28**  
  short presentations

- **We, Dec 3**  
  seminar: presenting

- **Su, Dec 9, 23:59**  
  deadline for final version

- **Mo, Dec 10, 8:15**  
  presentations & discussion

- **We, Dec 12, 16:30**  
  presentations & discussion

- **Upon appointment:**  
  individual review with trainer

And when do YOU work on the deliverables?

Emotions
Get informed

- **Plan:**
  - Understand the teacher’s requirements.
  - Plan: You need a calendar!

- **Research:**
  - Search, evaluate, sort, make abstracts, write a journal, write regularly (summarising, commenting, defining)

- **Write a draft:**
  - Update the teacher’s task, define questions for your work, collect ideas, sort, structure, draft.

- **Revise:**
  - Style, language, grammar.

- **Spit and polish:** Punctuation, capitalisations.

Sich informieren: Recherchieren

- Sichten von Einführungstexten
- Mit Schlagwörtern suchen
- Quellen sofort notieren
- Sortieren: Unbedingt lesen, vielleicht lesen, nicht lesen


Sich informieren: Lesestrategien

- Effektives Lesen
- Aktives Lesen:
  - Frage an Text zum gezielten Lesen
  - Textzusammenfassung machen
  - Exzerpieren eines Textes
  - Abstand zum Text
  - Visualisierung, Mindmaps
  - Grundstruktur eines Textes erfassen
  - Argumentationsstruktur visualisieren

- Mangel an Konzentration?
Schreiben: Ordnung ins Gedankenchaos

• Fragestellung erarbeiten
• Problem identifizieren, danach analysieren
• Ideenfindungsmethoden: Brainstorming, Cluster
• Gliedern
• Phasen
  – Gedanken sammeln
  – Gedanken sortieren
  – Gliederung erstellen
  – Erstentwurf schreiben
  – Überarbeitung des Entwurfs
  – Sprachlich-stilistische Überarbeitung
  – Korrektur: Grammatik, Rechtschreibung und Zeichensetzung


Aspekte

• Definieren
• Beschreiben
• Verbinden
• Vergleichen (Analogien)
• Analysieren (Ursache, Wirkung)
• Lösungsansätze
• Anwenden
• Argumentieren

Schreiben: Erstentwurf für „Rabbits“

- Fragestellung notieren
- Gliederung im Kopf haben
- Gedanken festhalten
- Wenn ein Wort nicht einfällt, einfach ein Dummy-Wort verwenden
- Chaotisch, schlecht formuliert, unvollständig
- Rechtschreibung nicht wichtig
- „Ich-kann-eh-alles-wieder-verändern“-Modus
- Formulierungswut bekämpfen
- Ohne Notizen schreiben
- Immer ein Schritt nach dem anderen


Schreiben: Überarbeitung

- Genauigkeit
- Kritischer Blick
- Klarheit
- Kohärenz
- Begriffsdefinition
- Argumentation
- Richtig zitieren

Schreiben: Leserfreundlichkeit

- Der Leser: hat wenig Zeit, ist eigentlich nicht interessiert, ist anderer Meinung, will es klar und einfach haben, er will Sie verstehen, er schätzt Ehrlichkeit

- Best Practices zum Vorbild nehmen
- Wie mache ich eine Einleitung?
- Wie mache ich den Schluss?
- Betonung des roten Fadens
- Wie strukturiere ich einen Absatz?
- Beziehungswörter

Hierarchie der Betrachtung eines Textes

- Aufsatz  Thema
  - Frontmatter – Einleitung – Kernteil – Schluss – Backmatter
- Kapitel
  - Überschrift + Body
- (eventuell) Unterkapitel bzw. (Unter-Unterkapitel…)
  - Überschrift + Body
- Absatz  Gedanke
  - Darstellung – Ausführung – Schlussfolgerung
- Satz  Grammatik
- Wort  Rechtschreibung
- Buchstabe  Font
Qualitative elements for grading

1. The indication of your willingness to improve towards becoming a professional
2. The **process** of collecting, prioritising, sorting, and presenting your topic
3. The **structure** of your paper/presentation
4. Your **active participation** in the seminar
5. The use of the English **language**
6. The **correctness** of your content
7. The **depth** of your content

---

**Grammar, Punctuation, and Capitalization**

*NASA SP-7084*

A Handbook for Technical Writers and Editors

Mary K. McCaskill
Langley Research Center
Hampton, Virginia

http://www.sti.nasa.gov/publish/sp7084.pdf
der tagesplan
gestern machte ich mir einen tagesplan für heute
heute stehe ich auf und schaue lange nicht darauf
es steht darauf was noch nicht getan ist
und noch heute soll das alles getan werden
und wer soll es sein der das tut
diese frage ist nicht gut
und die antwort darauf auch nicht

Ernst Jandl, der gelbe hund (http://www.worte-projekt.de/jandl.html)