14

Introducing elements of active learning in a small course

Laura Mančinska

Department of Mathematical Sciences
University of Copenhagen

Setting the scene

Despite the modern consensus that traditional-style lectures do not promote deep and longlasting learning outcomes, many mathematics courses are delivered precisely in this manner.[1] How does one incorporate elements of active learning in a pre-established course with traditional-style lectures? Are these additional activities introduced at the expense of covering less material and do more advanced students suffer from this style of teaching? If so, do the advantages outweigh the negative effects in the context of a master's level mathematics course?

Context of the study

This study will be conducted in the context of the 7.5 ECTS Master's level course "Introduction to Modern Cryptography" at the Department of Mathematical Sciences (see Table 14.1 for a quick overview of the course). The teaching format adopted in the previous years was traditional-style lectures plus exercise classes which are normally used for going over assignment solutions or additional course material. This was the first time the course was offered as a graded rather than a pass/fail course. Therefore, to allow for

[1] A typical mathematics course consists of lectures and exercise classes. It is the lecture component that is often delivered in the traditional "instructor-at-the-blackboard" manner. Most of this article concerns the format of the lecture rather than exercise-class component.

more accurate individual assessment, I introduced a final exam. This was done in view of the fact that the students are encouraged to work on assignment problems collectively. Another change in comparison to the previous years was that the deliverable component of the project was changed from written to oral presentation. Oral presentations allow students to gain experience and improve their presentation skills, as well as allowing them to learn from each other.

Table 14.1. The course "Introduction to Modern Cryptography" at a glance.

Audience	**Study program**	Mathematics (majority), Computer Science, Statistics
	Level	Master's (majority), Bachelor's
	Size	9 students
Course	**Weekly contact hours**	4 hours of lectures + 3 hours of exercise classes
	Assessment	• 4 assignments • Individual project presentation (15 min) • Written final exam (3 hours)
	Credit	7.5 ECTS

To evaluate and reflect on the planned intervention we must consider them in the context of intended learning outcomes (ILOs). To comply with the Danish Qualifications Framework for Higher Education (Danish Ministry of Higher Education and Scince, 2008), ILOs are specified in terms of knowledge, skills, and competencies (see Table 14.2).

Table 14.2. Intended learning outcomes of the course "Introduction to Modern Cryptography".

Knowledge	The students will have an understanding of the theoretical and mathematical basis of modern cryptographic systems.
Skills	The students will be able to give rigorous security proofs of basic cryptographic systems and connect various cryptographic primitives with rigorous reductions.
Competencies	Understanding theorems about theoretical cryptography; proving security reductions; reasoning about the limits of computationally-bounded adversaries.

The planned intervention and its theoretical backing

In this section we describe the planned intervention which can be summarized as incorporating elements of active learning in traditional-style lectures of a pre-existing course. We include a description of the elements to be incorporated, give specific examples, explain the desired outcomes of each of the elements. We also provide theoretical backing of the intervention as a whole as well as its constituent elements.

Theoretical backing and motivation behind the intervention

Roediger et al. define learning as "Acquiring knowledge and skills and having them readily available from memory so you can make sense of future problems and opportunities." (Roediger et al., 2014). According to the seminal work (Piaget, 1978), the learner is viewed as a goal-oriented agent who actively seeks information. In contrast, the traditional didactic lectures are one-way exchanges, where the knowledge is supposed to flow from the instructor to the students. In addition, the modern consensus is that the acquiring of usable knowledge and skills occurs when the learner examines different facets of the topic in question and connects it to already existing knowledge and skills (see e.g. Bransford et al., 2000)). During a traditional-style lecture it is easy for a student to take the role of a passive listener and leave the auditorium without having connected the discussed topic with their previous knowledge and experiences. Active and student-centered learning is an approach that seeks to correct this by putting the focus on the student and placing them into situations where they are "forced" to take a more active role and form the desired links. Of course, not all the students require such forcing as they independently examine different aspects of the discussed topic and contrast it with their pre-existing knowledge via an un-coerced inner reflection. However, it is not this group of students[2] that an instructor should focus on as they are bound to learn almost irrespective of the circumstances. Instead one should encourage the more passively-inclined students and design activities that would encourage them to take up a more active role therefore promoting the acquisition of deep, usable and long-lasting knowledge.

[2] For the purpose of this article, let us briefly refer to this group as "advanced students" or "advanced learners".

Description of the intervention

We now proceed to describe the elements of active learning introduced in the lecture-component of the course "Introduction to Modern Cryptography". We also describe what aspects of active learning each of these elements is meant to address.

a) ***Short self- or peer-graded quizzes at the beginning of the lecture.***
Description: Start a lecture by asking the students to recall the previously introduced concepts necessary for the upcoming lecture. The students would be given a few minutes to write down their answer and then provided with a model solution along with a sample grading scheme. Sometimes the students would grade their own solutions and sometimes they would be asked to switch with a peer. The students' performance in these quizzes had no effect on their final grade. However, similar style questions were asked in the first part of the final exam and I would remind the students of this in order to encourage maximum effort.
Intended outcome: Activate the students at the beginning of the lecture and refresh the concepts needed to place the forth-coming material in the context of the previously covered topics. The purpose of the grading scheme is to help the students identify the essential ingredients of a correct answer. The intention behind peer-grading is to help the students recognize a correct and complete answer as we are often quicker to notice shortcomings of others' work in comparison to our own.

Table 14.3. An example quiz question.

Question	Define a private-key encryption scheme
Answer	A (simple) PK-encryption scheme Π over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ consists of three probabilistic algorithms • **Key generation** algorithm Gen producing key $k \in \mathcal{K}$ • **Encryption** algorithm Enc: $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$ $c \leftarrow \mathrm{Enc}_k(m)$ • **Decryption** algorithm Dec: $\mathcal{K} \times \mathcal{C} \to \mathcal{M}$. Scheme must satisfy **correctness requirement** $\mathrm{Dec}_k\big(\mathrm{Enc}_k(m)\big) = m$ for any $m \in \mathcal{M}$ and any key output by Gen.
Grading scheme	[1pt] mention the three sets $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ [1pt] for a correct description of each of the 3 algorithms [1pt] Correctness requirement [1pt bonus] For "probabilistic" and quantifiers on *m, k*.

b) ***Guided interactive investigation of a topic.***
Description: Rather than presenting the students with a ready-made theory and concepts, sometimes I would attempt to develop the material together with them via a series of leading questions. Precisely what is meant here is best understood via an example (see Table 14.4).
Intended outcome: Engage the students and allow them to actively discover the material themselves, promote deeper understanding, develop research skills.
Further considerations: When employing this tactic, one should bear in mind that it is rather time-consuming. It is a very engaging way to present new material and it undoubtedly activates students and leads to a deeper understanding of the topic. However, due to the associated time cost and the fact that not every topic lends itself easily to this approach, I did not use it in every single lecture.

Table 14.4. An example of guided investigation.

Concept to be discovered	Message authentication codes (MACs) for long messages.
Question and answer sequence	*Initial question (instructor)*: Now that we have seen fixed-length MACs, how could we use them to authenticate longer messages?
	Answer (student): Split message into blocks and obtain the tag by concatenating tags for each of the blocks.
	Instructor (writes on the board): Alright, so we consider a block-message $m_1 m_2 \ldots m_k$ and then obtain its tag as $t_1 t_2 \ldots t_k$, where $t_i = \mathrm{Mac}_k(m_i)$ Does anybody see a possible attack? (Give some time if no one raises their hand.)
	Student: We can request tags for two different messages and then produce a new valid message-tag pair.
	Instructor: Formalizes the suggested answer on the board. Does anyone see how we could modify the previous idea to render this attack ineffective? (Give some time.)
	Students: ...
	Instructor: Recall that we know from the last week that deterministic encryption schemes are insecure…
	Student: Offers an idea that is later formalized by the instructor as a complete construction for MACs that can be used to authenticate long messages.

c) ***Short activation questions.***
Description: While explaining the material pose quick questions to the audience. For example, the question could be drawing students' attention to crucial or subtle aspects of the notion currently being introduced or asking them to compare it to a related previously introduced concept. Other questions of this type would be to encourage the students to suggest a relatively easy-to-anticipate next step in a proof or perform a simple calculation. In order to avoid interrupting the flow of the exposition these questions are designed to be rather straightforward.
Intended outcome: Activate the students that have slipped into passive listening, encourage the students to link the new material with the previously introduced one, give them a chance to gain further familiarity with the concept in question.

Evaluation and outcomes of the intervention

The intervention was evaluated via the following four methods:

E1. A standard course evaluation form (Anonymous, Response rate: 5/9).
E2. Additional free-form question specifically regarding the small exercises and quizzes during the lectures (Anonymous, Response rate: 5/9).
E3. An individual, informal follow-up interview with select students.
E4. Feedback from the peer-supervision group who observed two lectures.

The course evaluation E1 was generally very positive. For instance, all of the students agreed that *"they have acquired the competencies described in the course objectives"*. The students evaluated this year's course a bit higher than the previous year's one in practically all the categories. Also, based on evaluation E1, the Teaching Committee at MATH categorized this course as belonging to (the highest) category A. This category is described as *"Courses where the teaching has worked particularly well and can inspire others."*

Of course, without a further follow-up E1 does not allow us to conclude that the positive evaluation was due to the added elements of active learning. In E2 the students explicitly mention that they found the small exercises helpful and that they allowed them to discern the most important aspects of definitions. However, most of the students did not like that some of the quizzes were peer-graded. Some mentioned feeling uncomfortable while others felt they could do just as well by grading their own work.

According to the feedback from the peer-supervision group who observed two of the lectures (E4), the students were generally engaged during the lectures and the interactive student-activation elements were perceived as aiding active learning. However, according to E4, student engagement lowered while a longer proof was being presented on the board.

Finally, according to evaluation E3, students generally enjoyed the added interactive elements. However, some of the more advanced students mentioned that the they found the pace of the course a bit slow. This was also echoed in one of the anonymous comments from E1.

Discussion of the outcomes and further improvements

In general, the introduced elements of active learning seem to have increased the student engagement and also their satisfaction with the course. However, the small number of involved students does not allow to conclude with certainty that the observed improvement is due to the intervention. In fact, to me the most convincing piece of evidence is my own empirical observation of the student engagement during the lectures that suggests that the intervention worked well. However, the small exercises did take up time which slowed the pace of the lectures and reduced the amount of material I was able to cover.

I believe that the effects of the intervention varied between different groups of students. For instance, if the definition from the last week is fresh in your memory, you are not gaining much by being asked to repeat it. Also, the time used for the small exercises is generally tailored to the average pace of the students. Therefore, I believe that the intervention might have caused some negative effects for the learning outcomes of the more advanced students. In general, I find that it is challenging to design activities that are equally beneficial to all groups of students.

The evaluation shows that peer-grading was generally not perceived well. However, evaluations E1 and E3 show that this can be attributed to miscommunication. The students seemed to believe that peer-grading was used to promote fair assessment. However, this was not the intention behind it (see (a) Intended outcomes in Section 2.1). I believe the perception of peer-grading can be altered by better communicating the reasons behind it.

In the future I would like to experiment with incorporating elements of active learning into the presentation of mathematical proofs. Proofs are

important elements of virtually any mathematics course, as they form the foundation of mathematical thinking. They are most often presented in the most elegant available form that highlights the crucial steps. This is usually not the form the proof is first conceived. So often times the instructor presents the proof without much interaction with the students. This can lower the student engagement. In fact, this was my experience during the "Introduction to Modern Cryptography" course and it was also pointed out by my peer-supervision group (evaluation E4).

References

Danish Ministry of Higher Education and Scince. (2008). "Danish Qualifications Framework for Higher Education." Uddannelses og Forskningsministeriet. ufm.dk.

Bransford, J. D., Brown, A. L., & Cocking, R. R. (2000). *How people learn* (Vol. 11). Washington, DC: National academy press.

Roediger, H. L., McDaniel, M. A., & Brown, P. C. (2014). *Make it stick: The science of successful learning*. Harvard University Press.

Piaget, Jean. (1978). Success and Understanding. Harvard University Press.