Main challenges in teaching/learning of mathematics for cyber-security

Miguel V. Carriegos

MAIN CHALLENGES IN TEACHING/LEARNING OF MATHEMATICS FOR CYBER-SECURITY

[1]M.V. Carriegos, [2]Noemí DeCastro-García and [3]J.F. García-Sierra

[1]Universidad de León, Algebra, School of Engineering, Spain, miguel.carriegos@unileon.es ; [2]Universidad de León, Didactic of Mathematics, School of Engineering, Spain; [3]Universidad de León, RIASC (Research Institute Cyber-Security), Spain.

In this poster the didactics of a specific matter, Cryptography in Master degree studies of Cyber-Security, is studied. Some concrete weakness are found by performing an assessment survey and observation. This weakness is related with some kind of applicationism. Some improvements are proposed by taking into account the design of real-world experiences perhaps by using old-fashioned data.

Keywords: Master Degree, Cryptography, Applicationism

RESEARCH TOPIC

This poster deals with teaching and learning challenges, weakness and possible solutions of matter of Mathematics for Cyber-security at Master degree studies. Some problems are detected and pointed-out. Moreover, some conclusions are given based on results of a concrete questionnaire of assessment. Finally some improvements are proposed.

THEORETICAL FRAMEWORK

Following Barquero, Bosch and Gascón (2014), the "Applicationism" or "Aplicacionismo" is a epistemology based, roughly speaking, on stressing theoretical matters of mathematical concepts devaluating concrete applications and scientific scenarios or real-world situations. Applicationism is detected in the framework of cryptography matter. To be concise, the topic is described from its theoretical roots and thus applications are proposed to the students. However our results show that it is necessary a more active approach to the matter maybe by process of teaching and learning based on projects; or giving an historical approach to the subject.

DESCRIPTION OF THE RESEARCH

The study was carried out by at Master Degree on Cybersecurity of Universidad de León by the Research Institute of Cyber-Security of the University. The participants were all the 20 students of the Master; 18 of them (90%) were Graduate Computer Engineers, 1 of them (5%) was Mathematician and 1 of them (5%) was Graduate Engineer in Electronics.

Our research is based in both observation and an assessment survey involving questions about learning, satisfaction, teachers, facilities and didactical material given in the subject of Cryptography. The objective of the quiz was to assess the quality of Master studies. This quiz was composed following SEEQ standard (Perry & Smart, 1997) and performed for all the 20 students of the Master.

RESEARCH RESULTS

A first overview of the results shows that our students were motivated and skilled and consequently overall scores were high: In fact means of about 4,5/5 in every matter except Cryptography. In this specific matter the score was 4/5; more than 10% less. This deviation was analyzed in a concrete session together with the students and several answers focused on “too much theory”, “too much mathematics”, “too few applications”, “we want to put our hands on concrete problems in real scenarios”, and so on.

IMPLICATIONS AND CONCLUSIONS

Cyber-security is a novel matter in university studies curricula; it is not cleat yet its concrete competences, skills or contents. Moreover it is still not defined as a scientific field because its dynamic aspect, hence the contents are unstable. Therefore conclusions of any study must be restricted to the concrete environment of the study, and hence we won't try to generalize our conclusions to the whole list of mathematics matters at university level or even to mathematics for cyber-security. Maybe this subject could be researched by means of a wide data collection across the whole university system when available. We do not have such data at this moment.

However we think we're able to state some conclusions related to the field: detecting weakness and stating acting guidelines to avoid difficulties and improve the studies. In particular it is necessary to create active situations of teaching and learning of Cryptography where students can model real problems. But real data is hard to obtain, an alternative deals with use of old-fashioned data of concrete cyber-security problems like the Enron email Corpus (Kessler, 2010), which is a public database obtained by the authorities after Enron bankrupt; thus this real old-fashioned data show criminal corporative behaviors or structures, data-flows, &c.

AKNOWLEDGEMENTS

This research was partially supported by Instituto de Ciberseguridad (Spanish Ministry of Industry, Tourism and Communications) under the contract X43 with Universidad de León.

REFERENCES.

Barquero B., Bosch M. and Gascón J., (2014), Incidencia del “aplicacionismo” en la integración de la modelización matemática en la enseñanza universitaria de las ciencias experimentales [Influence of applicationism in the integration of mathematical modelization in the experimental sciences teaching at university level] *Enseñanza de las Ciencias,* Vol. 32, Issue 1, pp. 83-100.

Kessler G., (2010), Virtual business: An Enron email corpus study, *Journal of Pragmatics,* Vol. 42, Issue 1, pp. 262-270.

Perry R.P. and Smart J.C., (1997), *Effective teaching in higher education: research and practice* Academic Press, New York.