Animation as an aid to support the teaching of cyber security concepts

Taylor, Mark (Corresponding author)
Department of Computer Science,
Liverpool John Moores University,
Byrom Street, Liverpool, L3 3AF
Tel : +44 (0)151 231 2215
Fax : +44 (0)151 207 4594
Email : m.j.taylor@ljmu.ac.uk

Baskett, Mike
Department of Computer Science,
Liverpool John Moores University
Email: m.baskett@ljmu.ac.uk

Allen, Mark
Department of Computer Science,
Liverpool John Moores University
Email: m.allen@ljmu.ac.uk

Francis, Hulya
Department of Computer Science,
Liverpool John Moores University
Email: h.francis@ljmu.ac.uk

Kifayat, Kashif
Department of Computer Science,
Liverpool John Moores University
Email: k.kifayat@ljmu.ac.uk

Abstract

Animated learning materials have the potential to support the teaching and learning process. In this paper, we examine the comparative usefulness of animated and static learning materials for teaching cyber security concepts to a group of UK undergraduate computer science students. The animated cyber security learning materials appeared to be viewed by the undergraduate computer science participants overall as being slightly more informative than the equivalent static learning materials for learning some cyber security concepts.

Key Words: animation teaching learning higher education

1. Introduction

Cyber security concerns the threats to computer systems and the measures that can be taken to protect against them. Threats include malicious software such as computer viruses, spyware and Trojan horses (Ahmad, 2013), and malicious individuals such as hackers. Measures to protect against such threats include: physical security to prevent, access, theft or damage to computing devices, and information security measures such as firewalls, anti-malware software, encryption and access control approaches to prevent access to and corruption of data and programs.

The research reported in this paper concerned whether animation can support student learning in the context of teaching cyber security concepts. The theoretical framework of the research is an investigation of animation for supporting the teaching of cyber security concepts in a higher education setting including denial of service attacks, distributed denial of service attacks, symmetric and asymmetric key encryption and digital signatures. The animation tool used to develop the animations was Adobe Flash.

The main limitations of the study were the limited number of student participants available for the research, and that the research covered purely an initial investigation of the perceived usefulness of animated learning materials for supporting learning basic cyber security concepts. Further research into the use of animation for supporting the teaching of cyber security concepts, and the conceptual levels of abstraction of cyber security concepts would involve assessment of the effects of animated learning materials upon the student learning process.

2. Literature review

2.1 Cyber security concepts

Cyber security concepts have different 'layers' of abstraction involved (Bratus, 2010). In a 'physical' sense, cyber security concerns use of an input device, through which data entered will invoke access to or alteration of data or programs stored on one or more computing devices. However, for this to happen a variety of software artefacts are used, and understanding how all the different software components work together, is more complicated. The final level of abstraction concerns the underlying mathematical basis of some of the software, for example, encryption software (Wang et al, 2011).

2.2 Animated learning materials

Animated learning materials can visually present the 'flow' of the elements that constitute a theoretical concept. Previous research indicated that visualisations and pictorial representations are generally accepted as useful educational aids (Mason et al, 2013). Appropriately designed multimedia learning materials consisting of images and text can potentially provide a more accessible approach to learning than traditional learning materials consisting of text alone. James-Gordon and Bal (2001) stated that some learners may absorb information more effectively from pictures and films, whereas other learners may learn best from textual explanations. Although a static pictorial representation or visualisation can provide an overview of the elements of a concept or process, animated representations can potentially provide a deeper appreciation of the concept or process due to provision of a flow of visual information.

2.3 Developing animated learning materials

There are different approaches to the formatting of animations for teaching purposes. One approach is to use a dual-coding format that uses both textual and visual elements displayed together to enhance understanding of the concept or process being taught (Hoffler and Schwartz, 2011). The multiple representations (both textual and visual) may assist learning in terms of building connections between the representations. Mayer and Moreno (2002) advocated displaying the animation and any corresponding narration simultaneously to provide temporal contiguity, and physically near to each other on screen to provide spatial contiguity.

2.4 Use of animated learning materials

Pictorial and animated learning materials can present information in a more "spatial" manner whereas text based learning materials can present information a more "verbal" manner, and it is not necessarily straightforward to determine whether animated representations may be more or less effective than verbal / pictorial representations (Wu et al, 2010). Animation may not provide anything additional for a learner, and may actually be distracting from the learning activity (Tversky et al, 2002). Animation should only be used when it focuses students' attention on appropriate features of the topic being taught, or when it provides attributes relevant to the learning activity (Ploetzner and Schlag, 2013).

Overall, there does not appear to be a consensus view as to the benefits or not of animated learning materials for aiding the teaching and learning process amongst researchers in the field of education. The originality of the research reported in this paper is the examination of the potential benefits of animation for aiding the teaching of cyber security concepts compared to "static" learning materials.

3. Research Methodology

The research reported in this paper concerned whether animation can support the learning of cyber security concepts. The theoretical research framework was investigation of the appropriateness of animations for supporting different aspects of cyber security teaching in a higher education environment. The theoretical research framework was developed from previous research by Mason et al (2103) regarding the potential usefulness of visualisations as a learning aid, and the appropriateness of animations as multimedia learning materials (Mayer and Moreno, 2002).

The research questions posed by the research concerned:

Can animation support learning the physical aspects of cyber security?

Can animation support learning the software aspects of cyber security?

Can animation support learning the mathematical aspects of cyber security?

How effective are animated as opposed to static learning materials for learning cyber security concepts?

How effective are animated as opposed to static learning materials for learning specific cyber security topics such as denial of service attacks?

3.1 Controlled conditions

One room was used for the study with constant lighting conditions and minimal background noise. Each animated and static version of the learning materials for a given topic was displayed to the participants for the same time period. The static and animated materials contained exactly the same information in terms of symbols, images and text. The animated learning materials supported no other actions other than that of viewing the animation.

The 32 undergraduate computer science student participants (who were randomly chosen from cyber security, computer forensics, and computer studies UK degree programmes) were randomly split into two groups that watched the media on one large screen. The first group viewed the static version of the learning materials for a given topic, followed by the animated version for that given topic. This was repeated for all the topics for this first group. The second group viewed the animated version of the learning materials for a given topic, followed by the static version for that given topic. This was repeated for all the topics for this second group. This was done in order to reduce any potential bias in the results due to the participants seeing the materials for a given topic twice. The student participants then anonymously completed a paper-based questionnaire.

The purpose of these controls was to assess whether animation itself was perceived as being useful as a learning medium by the participants, rather than any interactivity provided by the animated learning materials (Taylor et al, 2008; Tversky et al, 2002).

3.2 Assessment of the usefulness of animation to support the teaching of conceptual levels of cyber security concepts

The rationale for the choice of topics for the animations was based upon concerns raised by the previous cohort of students undertaking a network security module that included: what is involved in denial of service attacks, what is the difference between how symmetric and asymmetric key encryption actually works, and how do digital signatures actually work.

The aim of the research was that of an initial investigation into the potential usefulness of animated learning materials for teaching cyber security concepts rather than attempting to assess the effect of the animated learning materials in terms of increasing ability or knowledge.

After the participants had viewed both the static and animated versions of the learning materials, they anonymously completed a paper-based questionnaire. An ordinal scale of measurement from 1 = static version of the learning materials being more informative to 10 = animated version of the learning materials being more informative was used for the first ten questions on the questionnaire. These questions concerned how the animated and static versions compared in terms of explaining the different aspects of the cyber security concepts covered.

The eleventh question on the questionnaire related to whether control of the animated learning materials, for example pause, rewind and fast forward controls, would have altered the participant's view of the usefulness of the animated learning materials. The answer to this question was simply a yes or no.

4. Overview of cyber security animated learning materials

The cyber security concepts covered by the animated (and equivalent static) learning materials used in the study included denial of service attacks, distributed denial of service attacks, symmetric and asymmetric key encryption and digital signatures.

The animation design for denial of service attacks used the simplest images to represent: malware containing and target computing devices and requests in denial of service attacks. Simple line images of computers, servers and arrows to represent communication requests were used. A similar approach to animation design for symmetric and asymmetric key encryption

used the simplest representation of the transmission of encrypted data between two individuals showing original, encrypted and decrypted message texts, key symbols to represent encryption and decryption keys, and arrows to represent message flows. The animation for digital signatures used the simplest representation of hash functions and encryption and decryption keys to represent the processes of creating and verifying a digital signature. The reasoning behind using the simplest pictorial and graphical representations for the animations concerned reducing the cognitive load (Amadieu et al, 2011) associated with viewing the animations, and producing animations that required the least visual processing (Kuhl et al, 2011) in order to support ease of assimilation. In the same manner, the accompanying textual information within the animated learning materials was written in an easily accessible writing style to minimise the mental effort required to comprehend the meaning of the textual information presented.

The animations were stepped animations with static elements materialising into view, and motion was depicted by moving arrows between the elements in the animation. The corresponding text explanations materialised on the screen alongside the images.

The first animation illustrated denial of service attacks. During this animation, request 'arrows' from a client device to a "target" device showed that during a denial of service attack the frequency of the requests to the "target" device causes operational problems for the "target" device (Figure 1).

The second animation depicted distributed denial of service attacks. During this animation, request 'arrows' from a number of client devices to a "target" device showed that during a denial of service attack the frequency of the requests from the different clients causes operational problems for the "target" device (Figure 2).

The third, and fourth animations depicted symmetric and asymmetric key encryption by showing message 'arrows', and how via encryption and decryption keys, a plaintext message is converted to an encrypted format and then back to plaintext again (Figures 3 and 4).

The fifth animation depicted how a digital signature is created in terms of data being put through a hash function and then a private encryption key being used to produce a signature from the hash value (Figure 5).

The sixth animation depicted how a digital signature is verified in terms of data being put through a hash function and then a public encryption key being applied to the digital signature to create a hash value which should be equal to the hash value produced (Figure 6).

Animation controls were not included in the animated cyber security learning materials used during the study in order to avoid any clouding of the results due to the effects of interaction rather than animation itself (Tversky et al, 2002).

5. Results

Table 1 show the anonymous questionnaire answers provided by the undergraduate computer science student participants in the study.

Concepts	Physical	Software	Maths	DSA	DDSA	Encrypt	Digital	Relations	Speed	Control
5	5	5	7	7	7	5	5	5	6	1
7	6	5	4	9	9	5	6	7	6	1

9	10	7	10	10	9	8	9	9	10	1
9	9	9	9	9	9	9	9	9	10	1
8	7	6	8	7	8	8	7	5	8	0
8	7	7	7	8	10	7	8	7	7	1
6	6	4	5	10	10	1	2	4	4	1
2	2	2	2	8	8	2	3	3	5	1
8	2	2	1	10	10	4	5	1	8	0
10	10	1	1	10	10	10	10	10	10	0
10	5	5	5	10	10	10	10	10	10	0
10	10	7	1	9	5	5	1	1	10	0
8	8	8	5	10	10	10	10	10	8	0
7	7	5	5	10	10	10	7	6	6	1
7	7	7	8	7	7	7	8	8	6	1
1	1	1	1	1	1	1	1	1	5	1
1	1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1	1	1	1
2	7	2	2	2	2	2	2	2	2	1
1	1	1	1	1	1	1	1	1	1	0
8	8	6	9	2	9	2	2	8	7	1
10	9	1	1	10	10	1	10	1	10	1
7	7	7	5	8	7	8	8	7	5	1
10	10	10	10	9	10	10	9	10	9	0
5	5	5	5	5	5	5	5	5	5	0
10	9	10	10	10	10	10	9	9	10	1
7	5	6	4	8	8	7	6	5	6	0
3	8	9	5	9	9	10	8	5	9	0
8	10	8	3	10	10	8	5	10	10	1
6	4	4	6	5	4	5	3	5	3	1
5	5	5	5	10	10	10	7	8	8	1
7	5	5	5	1	10	6	6	5	6	0
Mean 6.44	Mean 6.16	Mean 5.06	Mean 4.75	Mean 7.09	Mean 7.50	Mean 5.91	Mean 5.75	Mean 5.59	Mean 6.62	Mean 0.59
SD 3.02	SD 2.93	SD 2.83	SD 3.03	SD 3.41	SD 3.20	SD 3.42	SD 3.17	SD 3.25	SD 2.89	SD 0.50

Table 1. Questionnaire answers provided by the participants. The answer scale was from 1 = static version being more informative to 10 = animated version being more informative.

In terms of assessing how effective are animated as opposed to static learning materials for student learning in the context of teaching cyber security concepts, the results appeared to indicate that overall the majority of the animated versions were viewed as being more useful than the equivalent static versions, but only to a limited extent with mean values ranging from 5.06 to 7.50.

In contrast, with regard to the usefulness with respect to animation supporting learning in the context of teaching the mathematical basis aspects of cyber security, the static versions were

viewed as being slightly more useful, with a mean value for this answer of 4.75. This could imply that the mathematical aspects of cyber security may require more detailed and involved animations in order to convey their meaning and use. For example, including animation elements that illustrate the nature of the mathematical calculations involved in the creation and use of encryption keys.

In terms of assessing if animations can support learning the physical aspects of cyber security, the results indicated that animations were viewed as slightly more effective than static materials with a mean value of 6.16. In terms of assessing if animations can support learning the software aspects of cyber security, the results indicated that there appeared to be no overall consensus view, with an average value of 5.06. In terms of pedagogy, this would imply along with the results from the mathematical aspects, that the more conceptually advanced the topic, the more difficult it may be to meaningfully represent such with a simple animation. Typically, mathematical concepts are viewed as more conceptually advanced than software concepts, which are more conceptually advanced than physical device concepts.

It also appeared that the perceived relative usefulness of an animated or static version covering a given cyber security topic depended to some extent on the nature of the animation itself, or the nature of topic covered. For example, the denial of service and distributed denial of service attacks animations were both viewed as being significantly more useful on average than the equivalent static versions with mean answer values of 7.09 and 7.50 respectively. However, the digital signatures and encryption animations were only viewed as being slightly more useful on average than the equivalent static versions with mean answer values of 5.75 and 5.91 respectively.

It also appeared that from the relatively high standard deviations (between 2.82 and 3.42) compared to the mean answer values (between 4.75 and 7.50), there was a diversity of viewpoints from the student participants. For each of the questions, the actual answer values ranged from 1 to 10, with some students consistently viewing the animated versions as being much more useful than the equivalent static versions, and other students consistently viewing the static versions as being much more useful than the equivalent animated versions. In terms of the overall internal consistency of the questionnaire used, the Cronbach's alpha value was 0.944, which indicated a high level of internal consistency for the questionnaire. Internal consistency describes the extent to which all the items in a test (or questionnaire) measure the same concept or construct. Cronbach's alpha provides an overall reliability coefficient for a set of variables (e.g. questions on a questionnaire).

Analysis of the responses to the different questions indicated that overall the more cognitive effort required for a given aspect of the topics, the less the perceived usefulness of the animations. In terms of complexity, the mathematical concepts of cyber security can typically be the most difficult to understand. Software aspects are typically not quite so complex, and the physical aspects typically the easiest to comprehend. The average scores for the animations regarding the physical, software and mathematical aspects of cyber security were 6.16, 5.06 and 4.75 respectively. Overall, this appeared to indicate that the more complex the cyber security concept, the less useful the animations were perceived to be by the student participants. A one-way analysis of variance (ANOVA) analysis comparing the means of the responses regarding the usefulness of the mathematical, software and physical cyber security animations showed that there was not a statistically significant difference between the responses to these questions ($P = 0.137$). The one-way ANOVA test was used as this enabled a comparison of the

variability between the responses to the questions to the variability within the responses to each question.

Similarly, the concepts of denial of service attacks and distributed denial of service attacks are cognitively simpler than encryption and digital signatures. The average scores for the animations for denial of service attacks, distributed denial of service attacks, encryption and digital signatures were 7.09, 7.50, 5.91 and 5.75 respectively. Overall, this appeared to indicate that the more complex the actual cyber security topic, the less useful the animations were perceived to be by the student participants. A one-way analysis of variance (ANOVA) analysis comparing the means of the responses regarding the usefulness of the denial of service attacks, distributed denial of service attacks, encryption and digital signatures animations showed that there was not a statistically significant difference between the responses to these questions ($P = 0.091$). The one-way ANOVA test was used as this enabled a comparison of the variability between the responses to the questions to the variability within the responses to each question.

Analysis of the responses of the individual students indicated that 4 of the students (roughly 12 %) preferred static representations throughout. In comparison, 14 of the students (roughly 44%) had mean average scores of 7 or more, with virtually all answers above 5, indicating a reasonably strong preference for animations. The remaining 14 students (roughly 44%) had mean average scores ranging from 2.5 to 6.9, with a typically wide variation of scores for the different animations. This appeared to indicate that this group of students found the animations useful for some topics (mainly denial of service attacks and distributed denial of service attacks, and physical cyber security aspects) and less useful for other topics (particularly the mathematical aspects). Overall, this appeared to indicate that topic complexity was significant in terms of the perceived usefulness of the animations, overall the more complex topics were worse served by the animations.

With regard to the perceived usefulness of controls for the animations presented, nineteen of the thirty two student participants regarded these as being useful, with thirteen of the student participants regarding these as not being useful for learning purposes.

6. Conclusions

The results of the initial investigation described in this paper indicated that animated learning materials were perceived as generally being more useful in terms of assimilation than traditional static learning materials for the cyber security concepts covered by the student participants involved. However, the level of relative usefulness varied between the animations / topics covered, and there was a clear diversity of viewpoints among the student participants, with some students clearly finding the static versions more useful and other students clearly finding the animated versions more useful for learning purposes.

The insights provided by the research undertaken were that animated learning materials can overall aid in the development of mental models of how things work (in the context of cyber security), but also that animated learning materials may be more useful for some topics than others. In addition, some students may find animated learning materials more useful than other students. For educators considering the use of animated learning materials for a given topic, it would appear that such materials should be supporting learning materials rather than the main learning materials, since some students may not find them particularly useful. Animated learning materials could possibly be targeted to specific topics or concepts where students have

shown lower performance, since such materials could potentially aid learning for some students. Further research could examine the possibility of adapting animated learning resources and their accessibility to better suit individual learner needs, in particular allowing students to control when, how often, and how long they access resources to suit their own needs. In addition, further research could attempt to assess the possible improvement of student perception of more challenging concept and topic content by more detailed / extensive animations that might match the level of complexity involved. For example, animations could include elements that illustrate the nature of the mathematical calculations involved in the creation and use of encryption keys.

References

Ahmad, A. (2013) Social media security risk and its protection against security attacks, *International Journal of Computer Technology and Applications* 136, 134-140.

Amadieu, F., Marine, C., Laimay, C. (2011) The attention-guiding effect and cognitive load in the comprehension of animations, *Computers in Human Behaviour*, 27, 1, 36-40.

Bratus, S., Shubina, A., Locasto, M. (2010) Teaching the principles of the hacker curriculum to undergraduates, *41st ACM Technical Symposium on Computer Science Education*, 10-13 March, 2010, Milwaukee, WI, USA, p122-126.

James-Gordon, Y., Bal, J. (2001) Learning style preferences of engineers in automotive design, *Journal of Workplace Learning*, 13, 6, 239-245.

Hoffler, T., Schwartz, R. (2011) Effects of pacing and cognitive style across dynamic and non-dynamic representations, *Computers and Education*, 57, 2, 1716 – 1726.

Kuhl, T., Scheiter, K., Gerjets, P., Edelmann, J. (2011) The influence of text modality on learning with static and dynamic visualizations, *Computers in Human Behaviour*, 27, 1, 29-35.

Mason, L., Lowe, R., Tornatora, M. (2013) Self-generated drawings for supporting comprehension of a complex animation, *Contemporary Educational Psychology*, 38, 3, 211-224.

Mayer, R., Moreno, R. (2002) Animation as an aid to multimedia learning, *Educational Psychology Review*, 14, 87-99.

Ploetzner, R., Schlag, S. (2013) 'Strategic learning from expository animations: short and mid-term effects', *Computers and Education*, 69, 159-168.

Taylor, M., Pountney, D., Baskett, M. (2008) Using animation to support the teaching of computer game development techniques, *Computers and Education*, 50, 4, 1258-1268.

Tversky, B., Morrison, J., Betrancourt, M. (2002) Animation: can it facilitate? *International Journal of Human-Computer Studies*, 57, 247-262.

Wang, Y., Wong, K., Liao, X., Chen, G. (2011) A new chaos-based fast image encryption algorithm, Applied Soft Computing, 11, 1, 514-522.

Wu, H., Chang, C., Chen, C., Yeh, T., Liu, C. (2010) Comparison of earth science achievement between animation-based and graphic-based testing designs, *Research in Science Education*, 40, 5, 639-673.

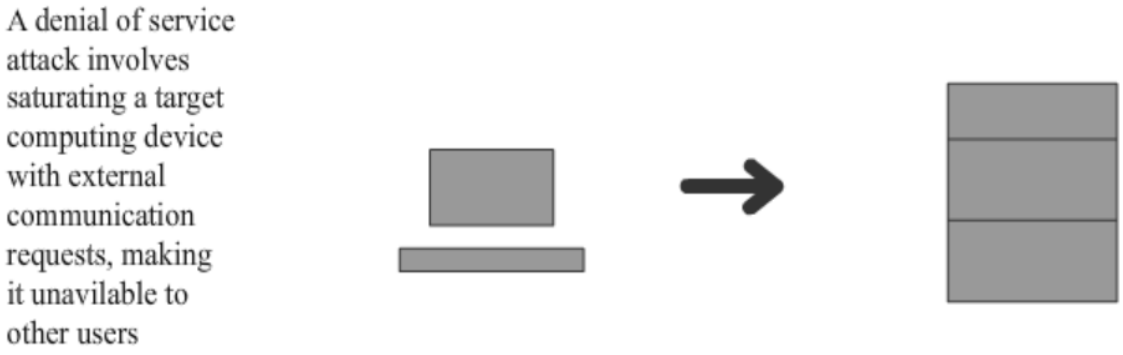

Figure 1. Static version of the learning materials for denial of service attacks.

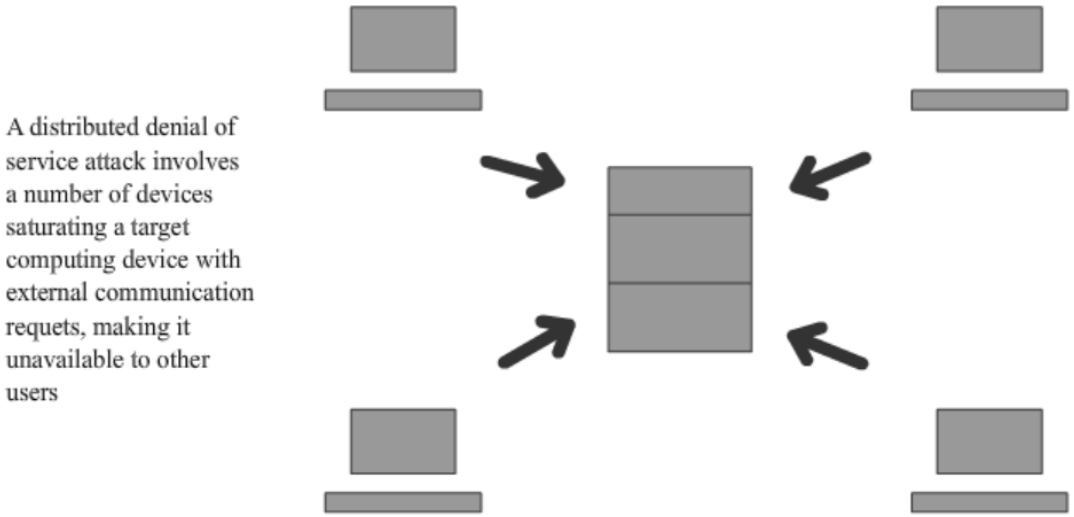

Figure 2. Static version of the learning materials for distributed denial of service attacks.

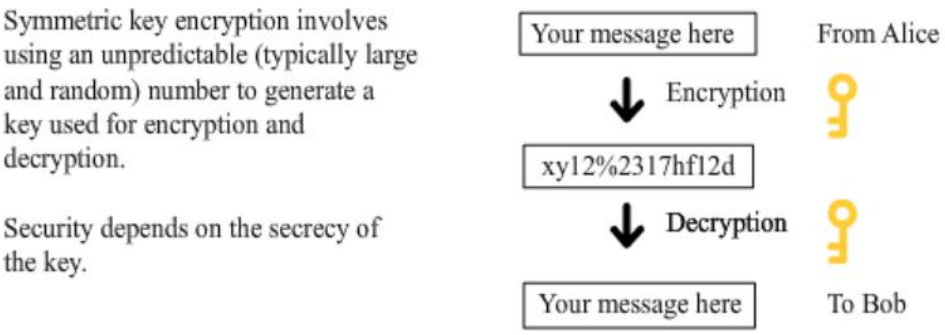

Figure 3. Static version of the learning materials for symmetric key encryption.

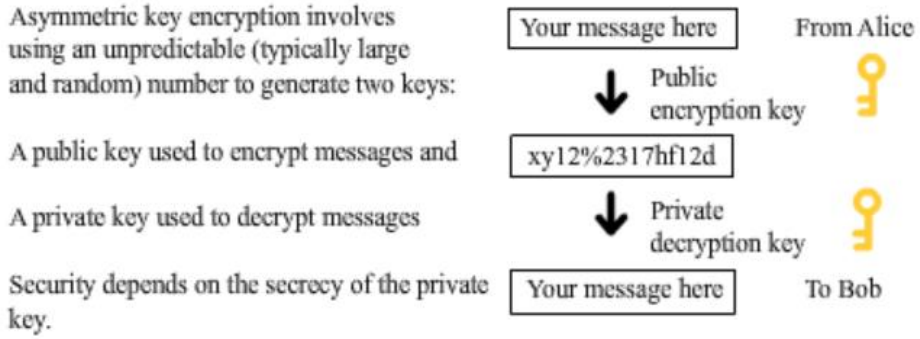

Figure 4. Static version of the learning materials for asymmetric key encryption.

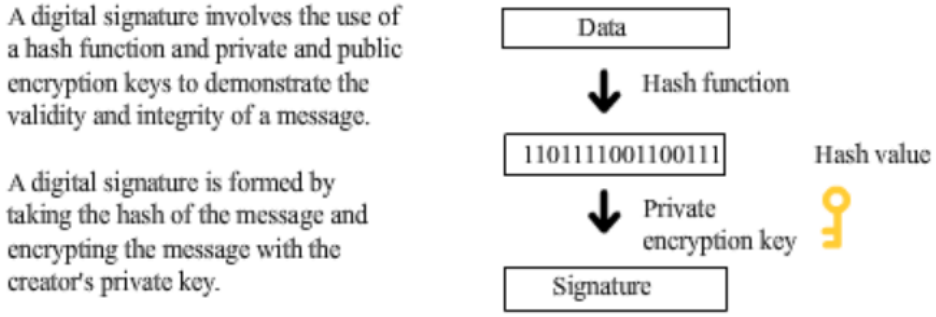

Figure 5. Static version of the learning materials for creating a digital signature.

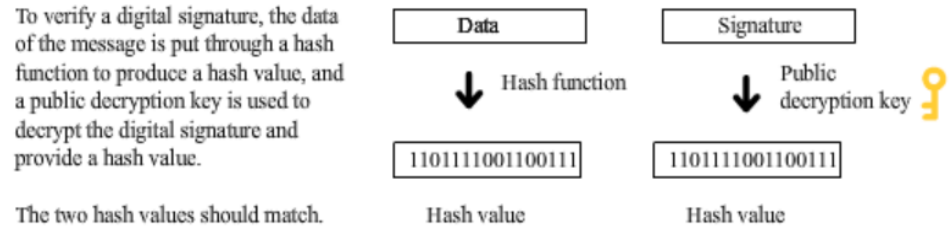

Figure 6. Static version of the learning materials for verifying a digital signature.