*Information & Security: An International Journal*

George Sharkov & Christina Todorova, https://doi.org/10.11610/isij.3707
vol.37, 2017, 95-102

# CAPTURE THE FLAG FOR CYBER-RESILIENCE EXERCISING THROUGH CRYPTOGRAPHIC PUZZLES AND COLLABORATIVE PROBLEM-SOLVING

George SHARKOV and Christina TODOROVA

**Abstract**: The importance of cybersecurity in the digital society and our daily lives is becoming increasingly apparent. With the rise of digital reliance, securing information, whether this information is at rest, in transit, or in use, is vital to ensuring the interoperability of systems, including critical infrastructure, on which society's physical well-being depends. Cryptography is well-known for its role in cybersecurity as a crucial tool for protecting information exchanged via digital devices.

Cryptography is the science of concealing information so that only the intended parties can read it. As a result, we may generalise that cryptography enables people to communicate via the Internet while securely sending critical and secret information. However, cryptography is a relatively complex combination of mathematics and computer science, where typical learning methodologies may fall short when it comes to achieving hands-on expertise. This paper provides an overview of the possibilities of Capture the Flag (CTF) exercises to test cybersecurity capabilities using collaborative methodologies and cryptographic challenges.

**Keywords**: capture the flag, CTF, cyber resilience, cryptography, problem-solving, collaboration

## Introduction

The interdependence and complexity of the digital society never stop growing. The modern world is one where complex systems-of-systems interact with one another in a supply chain, heavily dependent on other sectors. Defending the complexity of such systems requires strong cybersecurity capabilities. Thus defenders can retain their robustness through regular exercising.

Cybersecurity exercises have long been recognised as a method to train and maintain talent within the domain.[1] Exercises are a crucial component of the emergency planning process, and educating the staff members responsible for preparing and responding to emergencies is essential to an organisation's capacity to manage any situation.[2] Likewise, businesses must regularly and adequately exercise their continuity

plans to maintain their viability, making exercise a crucial component of organisational resilience and flexibility.

Capture the flag (CTF) is a cybersecurity puzzle that challenges participants to solve various tasks for finding and exploiting various security flaws. They are generally well-recognised as an effective pedagogical mechanism, leveraging game-based learning to improve team interoperability and provide opportunities for in-depth, hands-on knowledge in information security and secure coding principles.

The most common orchestration of a CTF competition follows a division of participants into two teams: red and blue. Teams are given the same challenges and must collaborate to solve them using their shared knowledge of information security. The term "Flag" relates to the primary type of challenge in a CTF exercise - locating one or more pieces of text hidden as part of the game.[3] Two basic formats of the exercise exist, as defined by Arvind Raj et al.,[4] namely Jeopardy-style and Attack-Defence style, described below in Fig. 1:

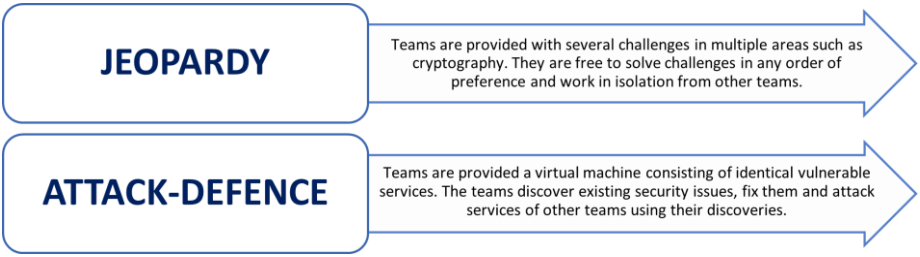


**Figure 1: CTF Formats (adapted from Arvind Raj et al.).**

Both provide educational merit due to their practicality and game-based design, empowering collaboration. However, most commonly, Jeopardy-style CTFs seem to be organised due to the resource-intensive process around creating, curating and managing attack-defence CTF exercises.

For cryptography training, a healthy mixture of both approaches could be implemented. This paper aims to share an overview of the benefits of such a mixed approach and introduce the importance of CTFs for cryptography to facilitate the establishment of collaborative-based cybersecurity capabilities.

## From Cryptography to Cyber Resilience

The role of cryptography in our daily lives grows the more critical our digital dependence becomes, making cryptography, the mathematical means of securing information, one of the core cybersecurity layers and a core mechanism for safeguarding data. Cryptographic methods may be employed alone or in combination to construct robust security systems that are difficult to attack.

Cryptography holds a central space at the heart of cybersecurity due to its ability to achieve multiple security goals (Fig. 2), including data confidentiality and integrity, as well as sender/receiver authentication and non-repudiation.

.

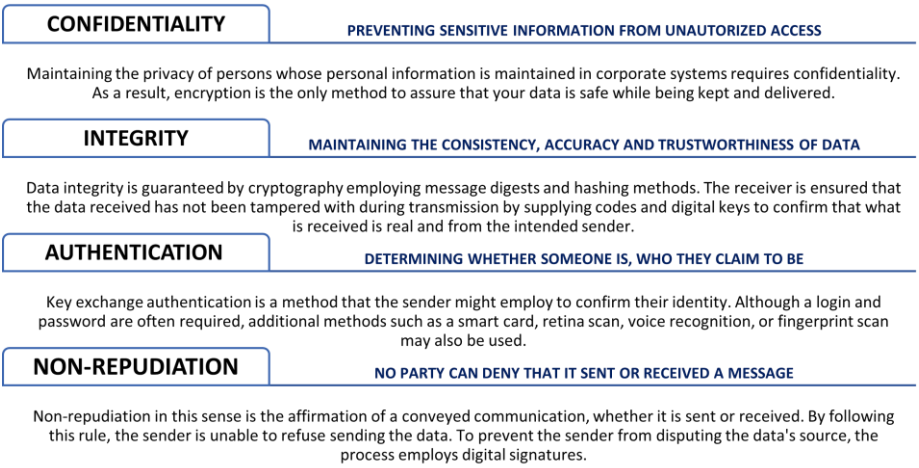


**Figure 2: Security Goals Achieved Through Cryptography.**

However, although cryptography is an essential tool in cybersecurity, it is not foolproof, especially when misused. This makes Capture the Flag a perfect collaborative exercise to test team collaboration for security and defence.

A mixed-method approach could be applied in cases where cryptographic challenges might not be viable for development in a virtual-based challenge setting. Such methods could include Pen and Paper CTFs, combined with a technology enhanced attack and defense CTF, where a flag of a task in the Pen and Paper CTF, could be used to unlock a part of the flag of an attack and defense CTF challenge. An example is included in Fig. 3.

The task presented in Figure 3 tests the participants' knowledge of classical cryptography and the history of cryptography. Although a small task, its answer is used to unlock part of the flag for a more complex web vulnerability task in a standard, virtual attack-and-defence CTF exercise.

The solution of the current problem is to decrypt with an offset of 10 to receive the result:

HEYWHATAREYOUDOINGTHISMESSAGEISINVISIBLEANYWAYTHEPASS WORDISANANAGRAMOFNAILS

An anagram of NAILS is SNAIL, which is the correct answer. This answer has also been implemented as part of another task in the Pen-and-Paper CTF, as shown in Fig. 4.

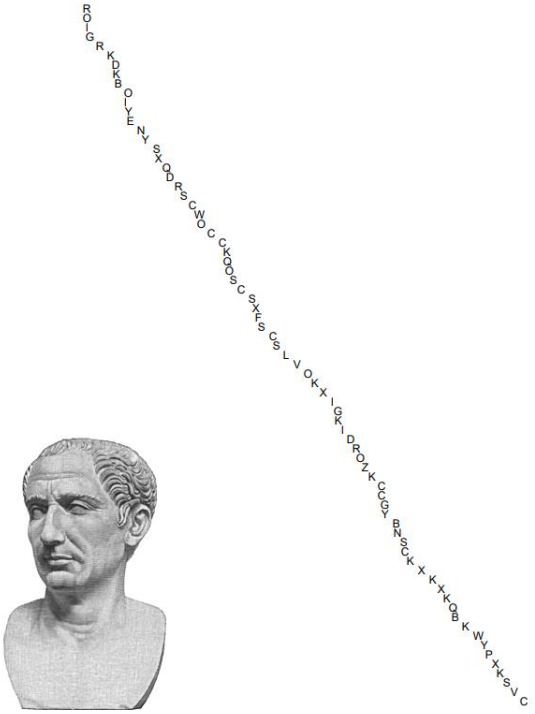


Figure 3 A Caesar Cipher Task for a Pen-and-Paper CTF in CryptoBG*2017. Developed by Miroslav Dimitrov.

In essence, the problem is

"(MSG1 + AGOODLUCK) XOR
RPJHRKDKCOJYFNYTYQDSTCXPCCLROTDSYGSCTLWOKYIHLJDSOALC
DHYCNTCLYKXKRCLWAPXLTWCAGOPEMUCK = ?"

where MSG1 is a reference to the task in Figure 3. The "plus" sign means concatenation. The 'xor' operation is not plain xor - if the letters are equal, given a fixed index, the result is 'A' (or some other symbol), or else the result is 'B' (or some other symbol). At the end, we receive a string:

*"ABBBAAAABABABAABBAABBABBAABBABBABBAABABAABABBBABAABABBA*
*BABABBAAABBBABAABBBAAAABBBAAA"*

Or translated to binary (A=1, B=0)

MSG1+ AGOODLUCK

XOR

RPJHRKDKCOJYFNYTYQDSTCXPCCLROTDSYGSCTLWOKY
IHLJDSOALCDHYCNTCLYKXKRCLWAPXLTWCAGOPEMUCK

=

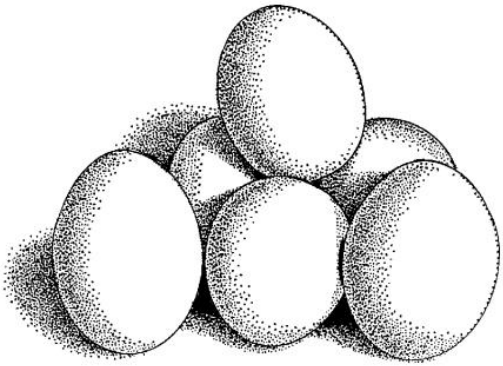

**Figure 4: A Task for a Pen-and-Paper CTF in CryptoBG*2017 combining a puzzle, xor and binary. Developed by Miroslav Dimitrov**

"10001111010101100110010011001001001101011010001011010010101001110001011000111000111"

The length of the string is 84, not divisible by 8, so participants should try 7 bits representation of a symbol. The answer refers to the dualities involved when choosing a strategy: A=0 or A=1?, splitting by 8 or by 7? or reading the little-endian or big-endian after the split. The answer (GULLIVERSEGG) is used as part of the flags for the virtual CTF.

The visual references are from Jonathan Swift's 1726 satire Gulliver's Travels, in which a civil war breaks out over whether the small or big end of a cooked egg is the right end to use to split open the egg.

Not all participants have the same challenge (referring again to the challenge of Fig. 4) in their Pen-and-Paper CTF, and only one participant out of each attack and defence team has a booklet with this extra challenge. The solution to the virtual challenge relies on the participants' discussion and collaboration more than the difficulty of the challenges themselves.

## Collaborative Problem-Solving

Collaborative problem-solving seems to be a simple notion. Still, each of its complex components needs further explanations via the lens of cybersecurity specifically and within the framework of Capture the Flag exercises.

Firstly, it is essential to note that collaboration and problem-solving are among the skills and abilities that some educational experts define as critical components of the so-called "21st-century skills" – a list of skills required by young professionals, students, and experts alike to prepare them for the demands of the rapidly changing landscape of digital society.

*Collaboration* is commonly defined as a person's capacity to work effectively with others to achieve a common goal.[5] Among the core values of collaboration are shared responsibility and constructive contribution. Within the context of a CTF, the collaborative approach also provides a safe space for the participants to learn from their peers and enter the role of experts, depending on their specific strengths and skill-set.[6]

Collaboration within the context of cyber exercises, including Capture the Flag exercises, is leveraged through *communication*, including the ability to use technology to facilitate communication, information sharing and dialogue. Within the context of cyber exercising, information sharing might be conducted not only through standard communication means, such as chats, email, etc. but also through situational awareness and shared monitoring dashboards, security monitoring instruments, simulated early warning systems and more. Effective communication generally requires the ability to write and listen effectively, as well as the ability to work in a cross-cultural environment.[7] Whether or not CTF exercises could enhance communication skills in participants, we could only speculate at this point, however, exercising communication in a simulation-based environment, facilitated through problem-solving, could be considered a means to build the habit of teamwork and communication across participants.

The ability to effectively use technology to communicate with others, as well as to communicate an incident, facilitate collaboration in the case of a remote setting, and visualise concepts might also be introduced under the umbrella of *digital fluency* [8] (otherwise called digital literacy [9]), along with other subject-specific hard skills. It is essential to mention that introducing hybrid teams in problem-solving technical challenges, based on the authors' observations, could provide a relevant toolset in exercising and working towards solving problems such as inconsistent engagement among team members, as well as the ability to convey complex matters into simple and understandable ways.

Last but not least comes the concept of problem-solving. Among the most studied abilities on the list of 21st-century skills, *problem-solving* is an innate ability of humans and a very successful learning mechanism.[10] Even in the dawn of cognitive sciences, researchers have observed the problem-solving tools in model problems and their relationship to real-world problem-solving. Throughout decomposition or other approaches, exercising a problem-solving process, as long as it involves similar cognitive processes, is an excellent method of exploring, setting in stone, and analysing the characteristics of cognitive processes underlying more complex challenges.[11]

*Collaborative problem-solving*, on the other hand, is a "cyclical process in which team members go back and forth between various cognitive and affective phases as they interact with the problem state and each other."[12] As a result, researching shared experiences, processes, and artifacts in collaborative contexts may give valuable insights into team cooperation quality.

## Conclusion

Against the contemporary cybersecurity backdrop, cryptography and collaboration are competences of core importance. According to recent studies, education, training and collaborative problem-solving are among the core strategies to increase cybersecurity capabilities and attempt at closing the ever-growing cybersecurity skills gap.[13]

Capture the Flag exercises offer a solution towards training security teams, but also teams of hybrid skillsets. On the contrary, an important outtake of the current overview is not to necessarily to emphasise the technical aspects of cyber exercising, whereas putting additional weight on collaboration and communication of team members.

We hope that by researching cybersecurity exercises and Capture the Flag exercises, in particular, we will encourage institutions to seek out additional possibilities and promote the implementation of routine CTF exercises as part of their teaching and organisational resilience processes.

## References


1 ENISA, "Good Practice Guide on National Exercises. Enhancing the Resilience of Public Communications Networks," Resilient e-Communications Networks, 2009, https://www.enisa.europa.eu/activities/res-old/policies/good-practices-1/exercises/exercises-on-resilience.

2 UK Cabinet Office, "Exercise Planners Guide," Home Office Publication, 1998, https://www.gov.uk/government/publications/the-exercise-planners-guide.

3 Arvind Raj, Bithin Alangot, Seshagiri Prabhu, and Krishnashree Achuthan, "Scalable and lightweight CTF infrastructures using application containers," *2016 USENIX Workshop on Advances in Security Education (ASE '16), Austin TX*, 2016.

4 Raj, Alangot, Prabhu, and Achuthan, "Scalable and lightweight CTF infrastructures using application containers".

5 Ignacio J. Marinez-Moyano, "Exploring the Dynamics of Collaboration in Interorganizational Settings," Ch. 4, p. 83, in Schuman (Ed.), *Creating a culture of collaboration: the International Association of Facilitators handbook* (San Francisco, CA: Jossey-bass, 2006).

6 Patrick Griffin, Barry McGaw, and Esther Care "Assessment and teaching of 21st century skills," in *Assessment and teaching of 21st century skills*, (2012), https://doi.org/10.1007/978-94-007-2324-5.

7 National Commission on Excellence in Education, "A Nation at Risk: The Imperative for Educational Reform," 1983.

[8] Stedman Graham, "Preparing for the 21st Century: Soft Skills Matter," H*uffington Post*, Apr 26, 2015.

[9] Bernie Trilling and Charles Fadel, *21st Century Skills: Learning for Life in Our Times* (Jossey-Bass, 2009).

[10] Herbert A. Simon and Allen Newell, *Human problem solving. Englewood Cliffs* (NJ: Prentice-Hall, 1972).

[11] Richard E. Mayer, *Thinking, problem solving, cognition*, Second ed. (New York: W. H. Freeman and Company, 1992).

[12] Muhterem Dindar, Sanna Järvelä, Andy Nguyen, Eetu Haataja, and Ahsen Çini, "Detecting shared physiological arousal events in collaborative problem solving," *Contemporary Educational Psychology* 69 (2022): 102050, https://doi.org/10.1016/j.cedpsych.2022.102050.

[13] $(ISC)^2$, "Strategies for Building and Growing Strong CybersecurityTeams," Technical Report, Cybersecurity Workforce Study, 2017, https://www.iamcybersafe.org/s/.

## About the authors

**George SHARKOV** obtained his Ph.D. in Artificial Intelligence, specialising in applied informatics, biophysics, thermography and genetics, and intelligent enterprise systems. Since 1994 he has been leading international software projects and companies for banking and financial systems, e-business, online markets and innovative e-trading solutions. Since 2003 he has been Executive Director of the European Software Institute - Center Eastern Europe, with CyResLab on Cyber Resiliency. Since 2016 he is also Head of the Cybersecurity Lab at Sofia Tech Park. Since 2014 George has been appointed as a National Cybersecurity Coordinator for the Bulgarian Government and is currently a cybersecurity adviser to the Prime Minister (formerly to the Minister of Defense). He is in charge of developing and implementing the Bulgarian Cybersecurity Strategy.

**Christina TODOROVA** is an aspiring information security research fellow working at the European Software Insititute – Center Eastern Europe. Her field of research currently revolves around means and methods of collaborative enhancement of cybersecurity capabilities through cyber/hybrid exercising.