Ciphers

The workshop addresses the fundamentals of message encryption and decryption. During the class, participants will learn about different ways and methods of encrypting communication. Participants will take on the role of cipher-breaking teams and, through active exercises, learn about various ciphers used over the centuries, up to the cipher broken by Jan Kowalewski during the Polish-Bolshevik War. Through a series of tasks and challenges, participants will have the opportunity to go through the process of breaking the Bolshevik ciphers themselves and to experience for themselves the process that Jan Kowalewski went through.

Duration: 90 minutes

Age group: 14 to 18 years.

Objectives:

1) **General goals:**
   a) to learn about The Cipher Game and its wider historical context **-** the methods of message encryption used during the Polish-Bolshevik War,
   b) to develop analytical thinking and creative problem solving
2) **Specific goals:**
   a) to learn about a range of ciphers used over the centuries,
   b) to learn the basic commands used in programming languages;
   c) to develop teamwork skills
   d) to develop creativity,
   e) to learn about the history of the Cipher Bureau and some of its activities during the Polish-Bolshevik War

Materials needed:

Checked paper, transcribed (or printed) encrypted messages, scissors.

Trainer preparation:

Before the class, learn about ciphers and cipher-breaking methods yourself, as well as the missions in The Cipher Game.

The workshop can be delivered as a single class or in a series of three workshops around The Cipher Game. Depending on the guiding method, you can choose the phrases to be broken by the participants. The phrases proposed in the following scenario introduce participants to the Polish-Bolshevik War and lead to to the final task (they were actual phrases used by Jan Kowalewski during his work on the cipher). You can also create your own phrases related to the topic of your lessons or representing the most important topics that you want to integrate, e.g. before a test.

STAGES

Duration	Exercise description	Materials needed / comments
10 min.	**Introduction:** Welcome the participants, introduce yourself and tell them what today's workshop is about (VR game, history and encryption). Ask about the group's experience with VR - has anyone played or watched anything in virtual reality before? Ask about experience with programming. Ask about experience with computer and mobile games. Establish with participants the rules of the today's workshop: - we focus on creation, creativity and not criticising others - we don't worry about technical issues and errors - sometimes they just happen 😊 - the “3+10” rule: – *When I ask for 3 minutes for me, I want your full attention and focus. If you don't listen then (when I'm explaining VR support, coding, or a given task), then for the next 10 minutes of your work you just won't know what to do.* - the “pause” rule:	Note: Depending on the group's experience with programming and VR, choose the subsequent exercises and the working method.

15 min.	**Game experience/cipher experience** Explain that in a moment some people will be able to experience the game in virtual reality, each person in the group will perform one task from The Cipher Game. Explain the basic controls in the game, select the first person, and launch the first mission. Get as far as the opening of the second door (which contains a second character listening for enemy transmissions). Pause the game as soon as the participants see the comb and the number card - before they have completed this task. Tasks in the first mission: - Find and activate the torch. Test the option to switch the torch on and off (visual cues are then activated highlighting the items to be used) - Find the board and start the engine ("Dragon") - Control the voltage on the board (test the optimum position and show it to the group, then override and make the jams fall out) - Go to the other room and find the key to the door - Replace the plug in one antenna and switch it on - Replace the plug in the second antenna and switch it on - Switch on the power supply to the apparatus in the correct order - Determine the optimum voltage without burning out the equipment Then, retell the context and history together: - Who is the main character in the game? - Where does the action take place? - In what year? Or years? - In the middle of what important historical event are we?	**If the group hasn't used VR or played the game before, start by experiencing the game. If the group has already been introduced to the game in a previous workshop, move on to the topic of encryption.** Match the implementation of this step to the equipment at your disposal: - If you have one set of goggles and a relatively small group, you can demonstrate VR gaming by dividing the mission into small tasks and swapping participants frequently. Try to connect the goggles to the screen (so that the whole group can see what is happening in the game). - If you have a larger number of goggles, get participants into groups and ask them to take turns and swap goggles.

	- What were its causes? Ask what signals the telegraphers in the game receive (Morse code sent by radio). Ask if such a form of communication can be intercepted and read? (yes) Explain that this will be the topic of today's workshop - cryptography (the use of ciphers and codes) and cryptanalysis (the study of ciphers and codes, particularly for the purpose of breaking them). *In today's workshop, you will play the role of cryptologists whose task will be to decipher secret messages received from me. In each task you will be given a code and supporting material to help you decipher a given code. We will start with simple codes and messages to more difficult codes and challenges.* *In January 1919, an organisational and cipher unit was created as part of the 6th Branch of the Information General Staff. On 11 May, the 6th Branch was changed into the 2nd Branch II in charge of communication and its internal structure features the Ciphers Unit.* *This unit was involved in breaking Soviet ciphers. Today you are playing the role of its staff.*	- If you don't have VR goggles, divide participants into groups and ask them to turn on the game on their smartphones or computers.
10 min.	**Task 1 - Frame cipher ("Chocolate")** Get participants into groups ("teams") of 3-6 people (you can combine or leave the groups from the previous exercise). Distribute sample messages written in a graphic cipher/chocolate to participants. Ask if groups have seen the cipher before and if they can read the message hidden in it. Give groups 3 minutes to try to break the cipher on their own and then 7 minutes to work on the cipher with hints. If groups don't know the cipher and haven't solved it themselves, you can help them through a series of prompts: - Is any of the graphic sign repeated? - Do any of the graphics look similar? - Can the individual graphics combine to form some larger graphic element? - *draw a grid, X and circle on the board without letters. Congratulate the group on possibly solving the cipher or on good and interesting ideas for breaking the cipher (try to look for and appreciate ideas related to finding common parts, repetition, rules or graphic signs).	Note: Some of the group may have experience with basic ciphers (when scouting, for example). Ask these groups to quietly report back to you when they have completed the task and not to give away answers or prompts to other groups. Note: Ideally, the encrypted messages from the supplementary material should be transcribed by you on a checked sheet of paper and photocopied. This will help groups to imagine solutions to

	Distribute extra materials showing the framework cipher to participants. Explain that this is a simple substitution type of a cipher - one letter or number corresponds to one other character. In this case, it is a graphic character, not a letter or number (as is the case in many other ciphers). Ask the group if they know of examples of messages or sign/graphic based writing? Ask if they have heard of hieroglyphs and if they know how Egyptian hieroglyphs were successfully read? Explain that some of the earliest writing systems were pictorial systems (or to put it more professionally) pictographic writing. *The Egyptian hieroglyphs were a mystery to researchers for many years - no documents or memory survived about what the various signs meant. The biggest breakthrough on this topic turned out to be the finding of the Rosetta Stone. Its content is a decree issued on 27 March 196 BC by Egyptian priests in Memphis to honour Pharaoh Ptolemy V on the occasion of the first anniversary of his coronation. It was written in two languages and three writing systems - Egyptian, in hieroglyphic and demotic script (demotic script being a later writing system developed in ancient Egypt), and Greek. As the text written in Greek was readable and the rest of the inscriptions were the same text, just in a different language, it became possible to compare the two systems and assign meanings to the individual hieroglyphs. The conclusion is therefore simple, if we have the same text written in plain text and 'hidden' text (unknown or encrypted), it is possible to decrypt it by analysis and comparison. Keep this story in mind for future assignments.* At the same time, explain the meaning of the deciphered word: ***Iona Jakir*** *was a Soviet military officer, one of the commanders during the Polish-Bolshevik war. He was one of our opponents today whose movements and actions we need to know!*	subsequent tasks later.
10 min.	**Task 2 - Caesar's cipher** Congratulate participants on completing the first task. Ask if reading this cipher was easy? Also ask if this is a cipher that we could transmit using Morse code. Emphasise that this cipher, while interesting, would not be easy to transmit by other means of communication (e.g. radio communication). We therefore need a cipher that allows us to encode our	Note: try to match the degree of your support to how the group is performing. If you see that the groups are engaged and doing well with the ciphers, do not distribute or delay the distribution of the support

	message using 'standard' letters and characters. Distribute messages encrypted with Caesar's cipher to participants. Ask if groups have seen the cipher before and if they can read the message hidden in it. Give groups 3 minutes to try to break the cipher on their own and then 7 minutes to work on the cipher with hints. If groups don't know the cipher and haven't solved it themselves, you can help them through a series of prompts: - Is any letter repeated? - Is there an object or material that could help them break the cipher? If the groups do not manage to solve the cipher on their own, give them additional materials as they work, in the form of two strips with the alphabet (to make it easier, you can make rings out of the strips, allowing them to move even more easily). Congratulate the group on solving the cipher or on good and interesting ideas for breaking the cipher (try to look for and appreciate ideas related to finding common parts, repetition, rules or graphic signs). Demonstrate how to read the message and explain that the cipher is called Caesar's Cipher or Shifting Cipher. It is a cipher that Julius Caesar is said to have used when communicating with his friends. At the same time, the mechanism of this cipher is very simple - each letter in the alphabet corresponds to a different letter of the alphabet (a substitution cipher). Each letter of the plaintext (unencrypted) is replaced by another letter a fixed number of alphabetical positions away from it - the offset is therefore one and fixed. At the same time, explain the meaning of the deciphered word: ***Warszawa** is the site of the decisive battle in the Polish-Bolshevik war, known as the Battle of Warsaw or the Miracle on the Vistula. It took place on 13-25 August 1920. It reversed the previous trend of Polish troops retreating. The Battle of Warsaw created a chance for the Poles to win the war and stopped the march of the Bolshevik army and the revolution it carried. It thus saved the independent existence of the Republic of Poland.*	materials. If groups experience issues, hand out materials and try to guide their work through appropriate questions.
*** 10 min.**	**Task 3 - Polybius checkerboard cipher.** Congratulate participants on completing the second task. Ask if reading this cipher was easy? Also ask if this is a cipher that we could transmit in Morse code.	

	Emphasise that this cipher, could already be sent by radio, although it would still be too easy to decipher. Therefore, in this task, we will tackle a more difficult cipher: Distribute messages encrypted with Polybius checkerboard to participants. Ask if groups have seen the cipher before and if they can read the message hidden in it. Give groups 3 minutes to try to break the cipher on their own and then 7 minutes to work on the cipher with hints. If groups don't know the cipher and haven't solved it themselves, you can help them through a series of prompts: - Is any figure repeated? - Is there an object or material that could help them break the cipher? - Was there something in the previous tasks and methods that we can use to break this cipher (a combination of the method involving strips with grid, as with 'chocolate'). If the groups do not manage to solve the cipher on their own, hand them supplementary materials in the form of two number strips as they work. Congratulate the group on solving the cipher or on good and interesting ideas for breaking the cipher (try to look for and appreciate ideas related to finding common parts, repetition, rules or graphic signs). At the same time, explain the meaning of the deciphered word: ***Odessa*** *is a strategically important port city that was important during the Polish-Soviet War and the Russian Civil War.*	
25 min.	**Task 4 - Bolshevik cipher** Congratulate participants on completing the third task Emphasise that we are facing, the last, most important task. All the ciphers so far have been to prepare us for just this challenge. *The next cipher is the actual cipher you see in the game. It is a cipher that was in fact used in the early days of the Polish-Bolshevik war, although we had to create our own materials for the workshop (the original messages were in Russian). The task you have is therefore almost the same task faced by the hero of our game and history, Jan Kowalewski. On the table is an intercepted Bolshevik message. You also*	Note: Before the exercise, prepare the support material (Comb): cut out several strips of paper with a standard grid (0.5cm). The strips should be about 20 grids long and at least three grids wide. You can cut in the bottom row of strips along the grid of the column to create a strip with 'teeth' resembling the teeth of a comb.

have one supporting element (a strip of checked paper) and know that the telegram will be about an important offensive for the opponent. Use everything you have learnt so far to work out the cipher.

Distribute messages encrypted with the Bolshevik cipher to participants. Give the groups as much time as possible to try to crack the cipher themselves. Try to give groups as few prompts as possible, you can help them through a series of questions:
- Is there an object or material that could help them break the cipher?
- Was there something in the previous tasks and methods that we can use to break this cipher?
- Can you guess what the message might be about?

When working in groups, encourage participants to share information between the groups - Are the groups competing or cooperating? Did anyone mention that it was supposed to be a competition? Emphasise that it's the completion of the task that counts, or maybe someone from another group already has a good idea?

Congratulate the group on solving the cipher or on good and interesting ideas for breaking the cipher (try to look for and appreciate ideas related to finding common parts, repetition, rules or graphic signs).

Demonstrate how, by breaking the teeth of a comb (in our material, cutting a grid in a piece of paper), we can find the word Warsaw (containing the three letters a) and how breaking the Bolshevik cipher can (and did!) work.

Answers for the trainer:

Message:
*Delegate. The target of the next attack is **Warszawa**. Attack from the west. Iona Yakir, Odessa.*

Decryption model: The cipher that Jan Kowalewski worked out is a simple cipher based on Polybius checkerboard, in which the layout of the board is unknown to the casual viewer. His working method involved:
1. to discover that it is a simple cipher based on a checkerboard (two digits correspond to one letter from the chessboard).

	2. to find a distinctive word containing, for example, three identical letters (in the original 'Division', which has three 'i' in Russian, and in the workshop version: 'Warszawa’). 3. to create a pattern of the three letters in a word by breaking out the corresponding teeth in a comb (or cutting out the corresponding grids in a piece of checked paper during the workshop). 4. to find the word in the text encrypted with a comb. 5. to decipher the first letters associated with a distinctive word. 6. to use the comb and deciphered letters to try to find the next distinctive word. 7. to repeat the previous steps until the layout of the Bolshevik cipher board is fully reconstructed.	
10 min.	**Summary** Congratulate all the groups and ask if the groups now have a better understanding of the challenge faced by the main character of our story? Emphasise that the cipher we broke in class is not an exact Bolshevik cipher (as is the message contained in it), but is as closely reproduced as possible for the purposes of this workshop. Mark that the reading of the real cipher really was done with a comb and word frequency analysis (which is still a method of breaking ciphers today). Emphasise, too, that the signatures denoting the city and the commander giving the order were equally important (the signature should not have been ciphered and was the result of an error by the radio operators). Breaking this particular cipher also took place at the beginning of the war (when they were not yet so complicated). However, the Ciphers Unit continued to grow during the war and used increasingly sophisticated methods to work out more Soviet ciphers (including the later and more complex ones that were based on mathematical analysis). Breaking the Bolshevik ciphers had a huge impact on the outcome of the Battle of Warsaw and the entire Polish-Bolshevik war. The knowledge and experience of Polish cryptologists also proved useful years later - in 1931, the Cipher Section was transformed into the Cipher Bureau, which began work on breaking the Enigma ciphers. Just before the outbreak of the Second World War, the results of the work of Polish cryptologists were passed on to the Allies from England and France. The results of the work of Polish cryptologists proved crucial to breaking the Enigma.	

	Emphasise that if participants want to know the rest of the story, you invite them to complete The Cipher Game. Summarise the workshop, thank all participants and teachers, and invite them to the next workshop as well as to learn more about other IPN educational materials.	