(De-)Coding adventures for young researchers

Pavel Boytchev

1 Coding, encryption, ciphers

We often associate *coding* with writing secret messages; however, this is usually called *encrypting*. Coding is a more general notion meaning to represent a message using specially designed symbols (AKA *codes*). Codes are not only the symbols used to code a message (sorry for this recursive statement), but are also the rules that control the processes of using these codes. The sole goal of a code is to be decoded. When we talk about *secret codes*, the goal becomes to make decoding easy for specific recipient and impossible to everybody else. This represents the encryption meaning of coding. In Greek *kryptos* means *hidden*. The other word that is often used for coding secret messages, is *ciphering*. The origin of this word leads us to the Arabic word *sifr*, meaning *zero*, *empty*, *nothing*. It has been introduced in Europe by the arrival of the Arabic numerals and soon its meaning has become not just zero, but also any numeral. Later on, it has started to be used for *coded messages*. Nowadays the cipher is usually a code based on digits.

Let us see two of the most famous ancient codes and try to develop techniques to decode them.

The Skytale is one of the oldest encryption techniques. It relies on changing the places of letters in order to hide the meaning. Coding and decoding uses simple tools – a stick with predefined width and a long leather or paper strip. The sender of the message would wrap the strip around the stick and then write the text across the strip (Fig. 1). The courier carries only the strip – when unfolded it contains a "random" meaningless sequences of letters. The receiver of the message wraps back the strip on a stick with an identical width in order to align the letters in the correct way and read the text.

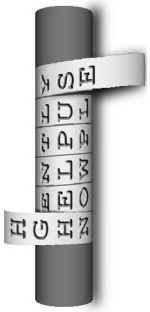

***Fig. 1** Model of a skytale*

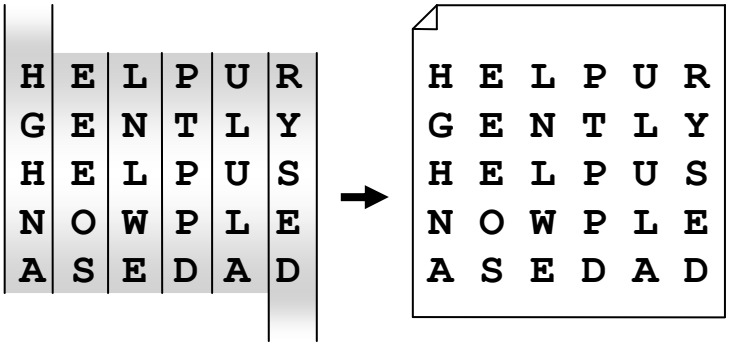

Fig. 2 The strip ordered in columns

If an enemy captures the courier, he would need the exact stick in order to decode the message. If the original message is HELP URGENTLY, HELP US NOW, PLEASE, DAD then the enemy would see HGHNAEEEOSLNLWEPTPPDULULARYSED. If we imagine a sheet of paper wrapped around the stick, then the text on it would look like in Fig. 2. Note that text is read line-by-line, but appears on the strip column-by-column. This information is sufficient to decode any message - just order the text in columns of 2 letters, 3 letters, etc. until you get a meaningful text horizontally.

Task 1. Describe an algorithm to decode any text even if the width of the stick is unknown.

Task 2. Describe how to eliminate stick width's that results in unaligned text (i.e. the letters are not aligned in rows when the band is wrapped around the stick).

Task 3. The enemy knows that you know how to decode any message without the correct stick, and yet it sends a secret message to challenge your decoding skills. Try to decode the message if it reads: HEGEHENOASLPNTLPWPEDURLYUSLEAD[1].

[1] Hint: What if letters are always written in pairs?

The Rome commander Julius Caesar is believed to have used another encryption method, which is nowadays called after his name – *Caesar's Code*. Each letter of the message is replaced by a letter three positions further on the alphabet (Fig. 3).

Our message HELP URGENTLY, HELP US NOW, PLEASE, DAD! would be coded as KHOS XUJHQWOB, KHOS XV QRZ, SOHDWH, GDG. Because of the shift, few letters will fall outside of the shifted alphabet. In our case such letter is Y, which is coded as B. Of course, it is possible to use other variations of this code – for example to use another shift number, or another shift direction.

Computers can break the Caesar's code by brute force, because there are only 26 letters in the English alphabet and it is easy to try all possible shifts. Even if there is no computer, a human can quickly understand which one of the shifts works – this is the one that produces meaningful text.

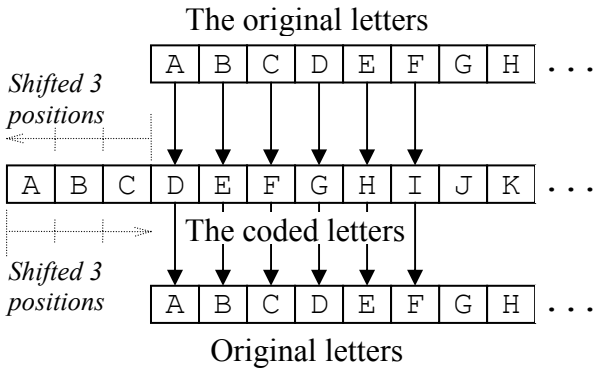

Fig. 3 Coding and (de)coding Caesar's Code

An interesting property of the Caesar's code is that the processes of coding and decoding are practically the same. If we code a message using shifting to the left by 3 positions, then we code it again by using shifting to the right by 3, then we will get the same message (Fig. 3). Thus, the second coding is in fact decoding.

The Caesar's code is still used today. The so-called ROT13 code, which uses shift of 13 positions, is often used to make accidental reading impossible – for example, the answer of a quiz could be coded by ROT13, so that it is both impossible to understand it immediately, but also it is easy to decode it.

The application of shift codes is related to "circular" arithmetic where only a given subset of numbers is used. All numbers outside this set are as if wrapped back to the set. If we imagine that this ring of numbers has 8 slots (i.e. it can accommodate the numbers from 0 to 7 inclusive), then 2+4 = 6 and 6+4=2 (actually 6+4 is 10, but 10 maps onto 2 after wrapping).We write in this case $6+4 \equiv 2 \pmod 8$.

The Caesar's coding is equivalent to using a ring of 26. If we apply shift-by-one code to a message 26 successive times, we will get the same message, because 1+1+1+…+1 (26 times) = 26 which overlaps with 0, or $26 \equiv 0 \pmod{26}$.

Task 4. Find a shift code for which coding and decoding is absolutely the same using the same shift, i.e. to decode a message you just code it again with the same shift position[2].

Task 5. Invent and manufacture a tool, which could help you to use Caesar's code easily[3].

Task 6. Study the ring arithmetic with various lengths of the ring. How is addition and subtraction done? Can the sum of two positive numbers be smaller than any of them? What will happen if a number is multiplied by a number equal to the size of the ring?

[2] Hint: ROT13 is such coding, purely symmetrical.
[3] Hint: One possible tool is to have two paper disks with different radii and letters typed along their perimeters. When disks are put one over the other, they can be rotated in order to represent various shift positions.

2 Projects

Coding and decoding could be quite interesting and engaging, but usually things are not that straightforward. Most often people need a lot more additional work to decode a message. The next section will present an interesting project that could involve several people working together, but before it, we will describe what a *project* is.

The etymology of the word *project* dates back to the Latin language. *Projectus* means *to throw forward*, and the root *ject* is nowadays a root of many words besides *project*, e. g. *projection*, *injection*, *inkjet*, *jet* (-liner), etc.

By *project* we mean a very complex task, which requires significant amount of time and other resources, and which is solved by a team of several people. There are two approaches to manage large projects and quite often they are used together.

- **Approach 1**: Split the task into simpler tasks. If the tasks are still too hard to do, then decompose them further into subtasks. Repeat this until all final tasks are relatively small and easy to accomplish. This approach is an implementation of the ancient Latin saying *Divide et Impera* (*Divide and Conquer*).
- **Approach 2**: Build one or more teams of specialists in different fields. Every team-member should know his/her task and how it depends on the rest.

The successful outcome of a project relies not only on the actual job related to the topic of the project, but also on other important issues, such as:

- Project management and collaborative work
- Gathering information from various resources
- Producing results that document every step of the project (these results are often called *deliverables*, and they could be a document, a software program, a study, etc.)
- Dissemination of the achieved results.

The next section deals with a project, which combines various activities. The intention is to have several teams engaged in the same project, solving different tasks in parallel. To solve the tasks in the project the teams would have: to gather information about the Ancient Greek pottery; to solve a decrypting problem; to find information about a mysterious illustration; to use software tools to build virtual models, and to solve problems involving calculations of volumes.

3. The big project

Everyone has visited museums … these buildings with large silent halls, full of ancient artefacts – statues, vases, tools and weapons. Museums tell us interesting stories about past times. We have the chance to see the same objects that were seen and used by people many centuries ago. Many of the exhibits present moments of the past. By studying the ancient artefacts, we could learn a lot about the culture, the habits and the dreams of our predecessors. Unfortunately, many of the artefacts are not in perfect condition – vases are broken, drawings are destroyed, pieces are missing, texts and ornaments are not easy to restore. And this is the beginning of the (de)coding adventure of the young researchers.

A real researcher is not someone who knows the answers of many problems, but rather someone who knows how to solve problems without obvious solutions. You, as young researchers, are asked to help the museum to solve a mysterious problem. There are four artefacts related to the problem and now you can examine them for the first time:

Artefact №1 – An ancient Greek vase with elegant drawings of people and animals. Unfortunately, the archaeologists found the vase broken into many pieces. They have made their best to reconstruct the vase as a 3D puzzle, but realized that some of the pieces are still missing (Fig. 4a).

Artefact №2 – A terracotta pot believed to be manufactured by Oltos 26 centuries ago (Fig. 4b). The most mysterious fact is that there is an upside-down drawing of dolphins.

a **b** **c** **d**

Fig. 4 The artefacts of the big project

Artefact №3 – A relatively large pot with unknown purpose (Fig. 4c). The archaeologists conjecture that it is used together with artefact №2, but how and why is still a mystery.

Artefact №4 – A clay plate with a sharp script based on Egypt hieroglyphs (Fig. 4d). Every word is coded with a single glyph. The conjecture is that it describes how artefacts №2 and №3 are used.

The goal of the project is to study all artefacts and help archaeologists to solve several problems:

- to build a virtual 3D model of artefact №1 so as to help its restoration;
- to determine how artefacts №2 and №3 were used;
- to find out why the dolphins in artefact №2 are upside-down.
- to *decode* the text of artefact №4;
- to calculate the volume of specific pots.

This project is a miniature version of an original research project – it can be split in tasks and subtasks, the work can be distributed among several teams, deliverables are to be produced for every task, and so on. The end of the project is a report to be presented to the whole group; it should reflect all the work done to help the archaeologists, as well as everything that has been found and learned.

The participation in a project requires a successful implementation of many skills including collaborative work, finding and using various resources, ensuring that tasks are complying their deadlines, transferring ideas and results from one domain to another, and finally, dispatching resourcing including personal efforts and time.

Before starting the actual scientific research, you should form teams. A team is supposed to have 3-7 members. This is not a strict rule, however. The number of the team-members may vary depending on their experience, but to get a realistic feeling about a project work, it is better to have at least three members in a team.

Building the teams is the first and the last job of the project that all young researchers will do together. All other activities are specific to individual teams. An important note to all teams is that every team will work on the whole project. The tasks in the project will be distributed within the team. Teams may compete with each other without sharing information and results while the project is running.

Every team-member should be responsible for at least one research activity required for the project: decoding ancient scripts; computer modelling; surfing for information and online scientific resources; electronic data processing, and project presentation. When the teams are ready, they should notify the supervising teacher about their decisions.

The next very important task for each team is to study the project and to try to group all related efforts into several tasks. The main problem here is that one and the same project can be split in different ways, so there is no single correct sequence of tasks.

After tasks are clearly defined, each team should distribute them among its members. There is no requirement to have one-to-one correspondence between tasks and members, i.e. a task can be given to several members, as well as a team- member could take part in several tasks.

The last activity in this task is to define how tasks are related to each other. This involves answering questions of the following kind: *Which tasks must be done before (or after) which tasks? Which tasks could be done in parallel, How much time will every task need, Is it possible that the result of one task be a hint to the solution of another task?*

Artefact №1 is reconstructed by several pieces, but still there is a part of the pot, for which no pieces are found. An important activity for you now is to find the missing pieces and put them in the correct places in order to get a whole and complete picture of the research object. The goal of this task is **to study the shape of the artefact and make a virtual 3D model**. For this purpose you could use a specially designed software application called *Potter's Wheel* [1]. It can build a 3D virtual model of a pot by defining its profile. The application assumes that the resulting shape is a rotational solid (Fig. 5). Potters use similar technique for making pots.

Fig. 5 The *Potter's Wheel* application

A good feature of the application is that it could be used in exploratory style – i.e. you can experiment with the functionalities, play with the buttons and learn-by-doing how to build a virtual 3D model.

Another task could be **to collect information and study the Ancient Greek pottery** – the kinds of pots, their typical shapes, decorations, purpose, etc. The outcome would have a great impact on the project success. A special attention must be paid to the first three artefacts – the broken pot, the upside-down dolphins and the large pot. If the researchers in charge of this task finish first, they could provide helpful information to the fellow-team-members working on other tasks.

Quite often a problem could be solved in several different ways. **Decoding the Egyptian hieroglyphs**[4] on the forth artefact could provide an alternative route to the problem with the dolphins. Here is a translation table supposedly sent by a famous Egyptologist (Fig. 6).

	In, inside		Sea
	Wine		Walk around
	Water		Psykter
	Dolphin		Jump
	Krater		Put, place

Fig. 6 Hieroglyphs dictionary

Fig. 7 The solution

[4] Most of them are true hieroglyphs, a few are „invented" just for the project.

The translation table provides literal translation of all symbols in artefact №4. However, you are expected to construct the meaning of the text based on a skeleton of translated words. It is also important to find the traversal path of reading.

If the plate is read top-to-bottom and then left-to-right, the translation would be: *Put wine in psykter* | *Put water in krater* | *Put psykter in krater* | *Sea walks around psykter dolphins jump in water*.

The solution of this puzzle is shown in Fig. 7 – the large pot is filled with cold water, the pot with the dolphins is filled with wine and its narrower side is placed in the krater. This construction is an ancient Greek wine cooler. While wine is being used, the remaining will always stay "underwater", exposed to the full potential of the cooling water. Thus the psykter is placed upside-down and the dolphins appear with normal orientation (jumping above the sea of cold water).

The goal of this task is not mere decoding of hieroglyphs. It teaches an important lesson, that sometimes scientists should consult different sources of information and experiment different ideas until they find a proper solution. This interdisciplinary approach is a fundamental tool for solving difficult problems. Having a Rosetta Stone is a lucky situation and scientists should not rely on it.

The next research task in the project could involve some mathematical explorations of the results from the previous tasks such as **measuring and calculating the volumes of various pots.** By applying their mathematical knowledge young researchers could get experience in several areas of mathematics: volumes of rotational solids; decomposing complex volumes into simpler ones; calculations with approximation; symbolic calculation; using interactive mathematical software; using spreadsheets for structuring and calculating of data; integrating knowledge from various domains.

The end of the project is a task involving all team-members – this is a **presentation of the team's activities and achievements**. This presentation could be a hard copy of a report, a multimedia presentation or both. This task is really important, because the young researchers develop and practice the skills to present scientific results to other people. Collaboration and social activities are a main factor for the success of modern projects, and the dissemination is the last milestone.

4 Introduction

Although this section is the last, it is captioned as *Introduction*, because the end of every scientific and research project lays the foundation of the next project. Researchers are never happy and content for a long time. Their curiosity pushes them into new scientific adventures.

Engaging young researchers in a large-scale project develops important skills and experience. These skills will help the young people in whatever direction they head later on. The experience of being a member of a team and being both *depender* and *dependee* develops a sense of collaborative work.

The presented project implements just one of the many possible ideas of how to blend research, exploration and discovery into one. Whatever the young people decide to do further on, they will always stumble upon projects with tasks, partners, deadlines, deliverables and presentations.

References

[1] http://www.elica.net/site/museum/Dalest/dalest.html, 1.10.2009
[2] http://www.math.uni-augsburg.de/prof/dida/innomath, 1.10.2009

Suggested further reading

Butler, W.S., Keeny, L. D. *Secret messages*, Simon&Schuster, NY, 2001

Christou, C., Sendova, E., Matos, J.F., Jones, K., Boytchev, P. et al (2007). *Stereometry Activities with Dalest* . University of Cyprus : Nicosia,2007, ISBN 978-9963-671-26-7

Boytchev, P., Chehlarova, T., Sendova, E., *Enhancing Spatial Imagination of Young Students by Activities in 3D ELICA Applications*, in Proceedings of the 36th Spring Conference of the Union of Bulgarian Mathematicians, Varna, Bulgaria, 2007, pp 109-119