

DECODING THE WORLD: CRYPTOGRAPHY AND MATHEMATICS

Duration	Age	Difficulty
1 hr	15-16	Low
#EXPERIMENTATION #MATHEMATICS		

DESCRIPTION

This activity introduces students to the fascinating world of cryptography and message encoding using basic mathematics and logic. Through a narrative guided by Iranian mathematician Maryam Mirzakhani (first woman awarded the Fields Medal), students will solve challenges related to Caesar cipher and binary coding.

They will experience how mathematics is applied to protect information, encouraging teamwork, critical thinking, and creativity.

ACTIVITY OBJECTIVES

- **Learn about Maryam Mirzakhani** as a female role model in mathematics.
- **Understand basic concepts of cryptography and codes.**
- **Apply mathematical concepts** (modular arithmetic, numerical systems) in a real-world context.
- **Develop problem-solving, collaborative work, and critical thinking skills.**

KEY COMPETENCES (EU)

- Mathematical competence and basic competences in science and technology.
- Digital competence.
- Learning to learn.
- Sense of initiative and entrepreneurship.
- Cultural awareness and expression.



MATERIALS



Notebook



Pencils and pens



Calculator



Provided by students



Provided by the teacher/institution



Downloadable Elements



Computer with internet connection



Projector or Screen



[Code templates](#)



[Excel for competition \(optional\)](#)

PREVIOUS PREPARATION

- Form groups of 4-5 students. The groups must be mixed.
- Prepare support material and computers.
- Project an image and a short video about Maryam Mirzakhani.





Watch video 🎥 - "Maryam Mirzakhani"

[Maryam Mirzakhani](#)



Note for the teacher 📝 **Maryam Mirzakhani and Cryptography: A Story of Creative Mathematics**

Here we have an infographic about Maryam Mirzakhani.

MARYAM MIRZAKHANI

Born
May 12, 1977
Tehran, Iran

Fields of Study
Mathematics
Geometry, Dynamical systems

Achievements
In 2014, she became the first woman to be awarded the Fields Medal, known as the "Nobel Prize of Mathematics"

Legacy

Mathematical diagrams include: a cylinder with $\frac{1}{2}x$, a dashed line with $\frac{1}{2}x$, a square with $4x$, a spiral with dx , and a geodesic line.

Maryam Mirzakhani was a groundbreaking Iranian mathematician and the first woman to receive the prestigious **Fields Medal**. Her work, focused on the deep structures of geometry and dynamic systems, showed the world how powerful creativity and persistence can be in solving complex mathematical challenges.

Although her research was not directly about cryptography, the mathematical fields she contributed to, such as hyperbolic geometry and Riemann surfaces, form the backbone of several modern cryptographic systems. For instance, concepts derived from her areas of study are applied in advanced encryption techniques that keep our digital communications secure.

Introducing Maryam’s legacy in the context of cryptography allows students to see how abstract mathematics can be transformed into real-world applications like secure messaging, online banking, and data protection. It also offers a strong female role model in a domain where women have historically been underrepresented.

Her story reminds us that mathematics is not just about numbers and formulas, it’s a creative language that can be used to build solutions to some of the world’s most pressing problems, including the protection of information in the digital age.



CONTEXTUALIZATION AND ADAPTATION

During the activity, we will provide context about the use of cryptography in data security, such as WhatsApp messages or banking transactions.

The world of cybersecurity is fascinating yet complex to understand, so thanks to this activity, we will be able to better understand how people work to keep our messages and our money in the bank safe.

Classroom activity

Let's do a quick class survey:

- Why is it important to protect information?
- Which fields are essential to handle this information properly?
- Do you think mathematics has a relation to this?

Cryptography is essential for protecting information in the **digital age**. For example, WhatsApp uses a system called **end-to-end encryption** to ensure that only the sender and receiver can read the messages; not even the company itself has access to them. Additionally, technologies like blockchain use advanced cryptographic techniques to secure the integrity and traceability of transactions, as in cryptocurrencies. These systems prevent data tampering and allow the creation of immutable digital records, increasing trust in digital environments.

Cryptography and mathematics are deeply connected. Modern cryptography uses mathematical concepts such as modular arithmetic, number theory, algebra, and probability to create secure codes. For example, algorithms like RSA or ECC rely on the difficulty of factoring large numbers or solving complex problems on elliptic curves, which protects our digital communications. Without mathematics, it would be impossible to design secure systems like encrypted messaging or blockchain.

Classroom activity Suggested classroom discussion questions:

- Why do you think mathematics is essential to protect digital information?
- What kind of mathematical operations do you think are used to create secret codes?
- How do you think mathematics helps secure blockchain transactions?
- Do you think cryptography in the future will rely on fields other than mathematics?
- How many encryption systems do you all know?

Discuss: how encryption affects digital rights and ethical communication





Note for the teacher 

Why is mathematics important to protect digital information? Mathematics creates secure encryption systems that make it extremely difficult for unauthorized people to access information. Without it, any message or digital transaction could be easily intercepted or altered.

What mathematical operations do you think are used to create secret codes? Operations include modular arithmetic (e.g., Caesar cipher), number theory (essential for RSA), algebra, and random key generation algorithms.

How does mathematics help secure blockchain transactions? Blockchain uses hash functions and digital signatures, based on mathematically hard problems that cannot be solved without the correct key, preventing forgery or modification of transactions.

Do you think cryptography will rely on fields other than mathematics in the future? It's possible. Quantum cryptography combines quantum physics and mathematics for even more secure systems. Artificial intelligence might also complement cryptography techniques.

Ultimately, if we look at it simply, the main idea is to make our information as secret as possible – and that's exactly what this activity will focus on: finding creative ways to keep our messages hidden and secure. To do this, there are various methods, next, we are presenting one of them.

The **Caesar Cipher** is a simple encryption technique named after Julius Caesar, who reportedly used it to protect his messages. It works by shifting each letter of the plaintext by a fixed number of positions in the alphabet. For example, with a shift of 3, A becomes D, B becomes E, and so on. It is an excellent introduction to modular arithmetic and the basic principles of cryptography.

Apart from the Caesar Cipher, we have the **binary code** as an encryption method. Binary code is a system of representing text, instructions, or data using only two symbols: 0 and 1. It is the fundamental language of computers and digital devices. Every letter, number, or symbol can be translated into a unique combination of zeros and ones. Understanding binary helps students grasp the basic principles of how computers store and process information.

Watch video  - "Binary Explained in 01100100 Seconds"

[Binary Explained in 01100100 Seconds](#)



ACTIVITY

Now each team must encode a message, indicating the key for decryption. Once they have created their message, another group (which will have also encoded their own message for another team to decode) will take the encrypted message and the key, and try to uncover the original message.

We recommend printing two copies of the "Resources" document per group. On the first page, you'll find the reference alphabet along with an example to guide students for the Caesar Cipher method. On the third page, there is a larger version of the alphabet designed to be printed and cut out, so students can use the letters as movable pieces, making it easier for them to experiment and rearrange the characters like a puzzle.



Now, the detailed steps to do the encryption by the Caesar Cipher method is explained:

PART 0 - PRACTICING CAESAR CIPHER

Step 0. Introduction. First, all teams will start with an example using a preset secret message, this is the first exercise on the printed template. As you'll notice, the decryption key is 3, which means each letter in the original message is found by moving three steps forward from the one written down.

Academia de inventores
POWERED BY EDELVIVES

Curricular

EXAMPLE (REFERENCE)

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

KEY FOR DECRYPTION

3

ENCRYPTED CODE

EBIL COBKAP

ENCRYPTION RESULT



The message that we have to decipher is:

EBIIL COFBKAP

So, in order to decode this, we must "step on" each letter on the alphabet and then move 3 steps to the right, for example:

E + 3 → H

B + 3 → E

I + 3 → L

...

After doing this deciphering work, students must write down their answer in the space prepared for that:

ENCRYPTED CODE

_____ EBIIL COFBKAP _____

ENCRYPTION RESULT

The result of this encryption is "**Hello friends**". Have you got it right?

Now, we'll walk through the detailed steps for creating an encryption using the Caesar Cipher method from scratch. Each group will then create their own encrypted message and pass it to another group to decode.

PART 1 - CAESAR CIPHER

Step 1. Choose a Key. Choose a number between 1 and 25. This number will be your *encryption* key.

CAESAR CIPHER

A	B	C	D	E	F
G	I	J	K	L	
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

KEY FOR DECRYPTION

-



Step 2. Create a Message. Each team writes a short, simple message (e.g., a greeting, a fun fact, a motivational phrase). Use the Caesar Cipher to shift each letter of your message forward by the number you chose.

CAESAR CIPHER

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

KEY FOR DECRYPTION

3

ENCRYPTED CODE

EBIIL COFBKAP

Step 3. Exchange Messages. Swap your encrypted message with another team. Make sure they also give you their encrypted message and key.





Step 4. Decrypt the Message. Using the key provided, shift the letters back to reveal the original message.

CAESAR CIPHER

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

KEY FOR DECRYPTION

3

ENCRYPTED CODE

EBIIL COFBKAP

ENCRYPTION RESULT

HELLO FRIENDS

Each team must improve their code after peer testing, using feedback to refine encryption and decryption strategies. And then they may re-do de activity with a new code.

PART 2 - BINARY CODE

Step 0. Practice. Each team will decrypt a simple message encoded with binary code. What word is hidden in the message?

01001000 01001001

A	01000001	H	01001000	O	01001111	V	01010110
B	01000010	I	01001001	P	01010000	W	01010111
C	01000011	J	01001010	Q	01010001	X	01011000
D	01000100	K	01001011	R	01010010	Y	01011001
E	01000101	L	01001100	S	01010011	Z	01011010
F	01000110	M	01001101	T	01010100		
G	01000111	N	01001110	U	01010101		



Note for the teacher

The result of the encryption is HI.

Step 1. Create a message. Now each team must encode a message, using binary code. Once they have created their message, another group (which will have also encoded their own message for another team to decode) will take the encrypted message and try to uncover the original message.

A	01000001	H	01001000	O	01001111	V	01010110
B	01000010	I	01001001	P	01010000	W	01010111
C	01000011	J	01001010	Q	01010001	X	01011000
D	01000100	K	01001011	R	01010010	Y	01011001
E	01000101	L	01001100	S	01010011	Z	01011010
F	01000110	M	01001101	T	01010100		
G	01000111	N	01001110	U	01010101		

Step 2. Decrypt the Message. Using the board, shift the letters back to reveal the original message. You must first exchange messages with other groups.

Classroom activity - Optional inclusive design challenge (Extension Activity)

Now those same groups will engage in an interdisciplinary design challenge: create an accessible cryptographic system tailored for people who are blind or have low vision. This task integrates mathematics (encryption logic), engineering (physical structure), art (visual/tactile design), and technology (optionally digital prototypes).

The process will follow an iterative design cycle:

- **Design Phase:** Each group decides if their code system will be visual (high contrast, large symbols) or tactile (using textures like foam, string, braille dots).
- **Prototype Phase:** Teams build a physical code board or message key that can be touched, seen, or both, using recycled materials and explaining why this is important.
- **Testing Phase:** They exchange their system with another group, who will decode it.
- **Feedback & Iteration:** Each team will receive peer feedback and refine their design.
- **Reflection Phase:** Groups analyze what disciplines they used (math, design, art, etc.), and how each contributed to making the system accessible and effective.





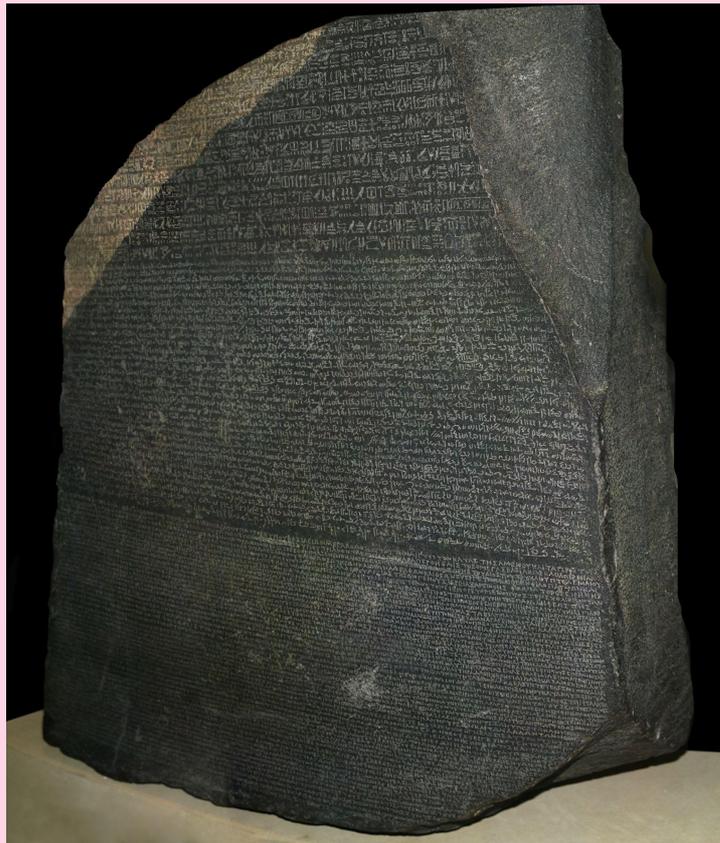
Classroom activity

If you have time, each group can think about what your perfect encryption method would be. You can create it yourselves and then present it to the rest of your classmates. You can watch an illustrative video about how the hieroglyphs used in Ancient Egypt were deciphered thanks to the discovery of the Rosetta Stone.

Watch video - “How The Rosetta Stone Unlocked Hieroglyphics” [How The Rosetta Stone Unlocked Hieroglyphics](#)

Note for the teacher

They can be asked to create their own encryption system, explaining that it could be a code using drawings, something related to mathematics, or whatever they prefer. It's important that they think about both the encryption and decryption processes. For example, the Egyptians had their hieroglyphs, but no one knew how to decipher them until the Rosetta Stone was discovered.





PART 3 - ENCRYPTING WITH HIEROGLYPHICS

Step 1. Create a Code. Each group must create a code using visual elements, such as colors, shapes, or symbols, to design a pictographic language. This code should go beyond function: it must also be a form of artistic communication. Students should explain the logic behind their choices (e.g., why a triangle means "A" or why blue represents "E", or complete words) and how their design makes the message clearer, more engaging, or more expressive. Creativity and visual coherence are key. The final result must work both as a cipher and a visual piece, similar to how ancient codes combined information and art.

	THE		TREE
	GREEN		SUN
	SHINE		AND
	ALIVE		OF
	DAY		SKIES
	BLUE		BIRD
	FRIENDSHIP		DEEP
	NIGHT		IS
	STRONG		HOW
	DARK		
	ONE / A		

Step 2. Write a message and share it with your classmates so they can decrypt it.





Note for the teacher 

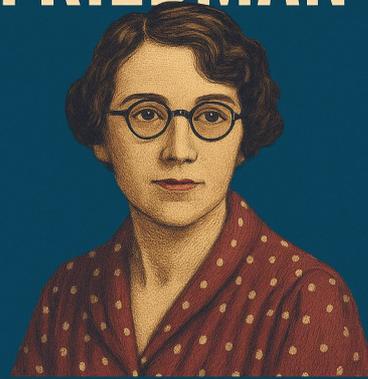
As you've just explored the powerful connection between mathematics and cryptography, take a moment to discover other remarkable women who contributed to this field, often against great odds. Alongside Maryam Mirzakhani, pioneers like Ada Lovelace, considered the first computer programmer; Joan Clarke, who played a key role in breaking the Enigma code during World War II; and Dorothy Vaughan, a mathematician and human computer at NASA, remind us that women have long shaped the history of mathematical innovation and code-breaking. Their stories show us that curiosity, logic, and creativity have no gender, and that the future of science and technology is built by diverse minds working together.

ADA LOVELACE



**PIONEERING MATHEMATICIAN AND WRITER
WORKED WITH CHARLES BABBAGE ON
THE PROPOSED 'ANALYTICAL ENGINE'
WROTE THE FIRST ALGORITHM INTENDED
FOR A MACHINE
SEEN AS THE FIRST COMPUTER PROGRAMMER**

ELIZABETH FRIEDMAN



**PIONEERING CRYPTANALYST
BROKE CODED MESSAGES
DURING WORLD WAR II
UNCOVERED SMUGGLING AND SPY RINGS
FOUNDER OF MODERN CRYPTOGRAPHY**

Classroom activity  - Recommendation (not included in the timing of the activity)

As an optional enrichment, students can explore traditional encryption systems, such as Navajo Code Talkers, and compare them to modern digital encryption techniques.

They may choose to represent their findings visually (e.g., through posters, diagrams, or illustrated timelines) to analyze how different cultures developed unique ways of encoding and protecting information.

This comparison encourages students to see STEAM as a culturally connected field, where traditional knowledge and modern innovation can intersect meaningfully.



PART 4 - MEASURING DECRYPTION TIME

Now, that we have trained several encrypting methods, from different times and procedures. We will see how the performance of each team as decrypting are.

The teacher will have several pre-encrypted codes, in binary and in caesar cypher. Each team will have to solve each message in the less time possible, to do this. 1 member of each team is going to exchange places with other team member of another group, this "external" participant is going to be in charge of measuring the time that each team takes to decipher each message.

The recording of the results of each team should be something like this:

Code/Hidden message	Time - Group X
1 (Caesar Cipher)	1 min
2 (Binary code)	50 s
3 (Caesar Cipher)	1 min 15 s
...	...

Next, we invite each group to gather their recorded times and enter them into the first sheet of the data recording template provided, titled "Results per group." We recommend making a copy of this file and saving it to the teacher's personal account before editing.

As shown in the image below, this first sheet provides an overview of the data template. The only section that needs to be edited is the "Time" column for each group.



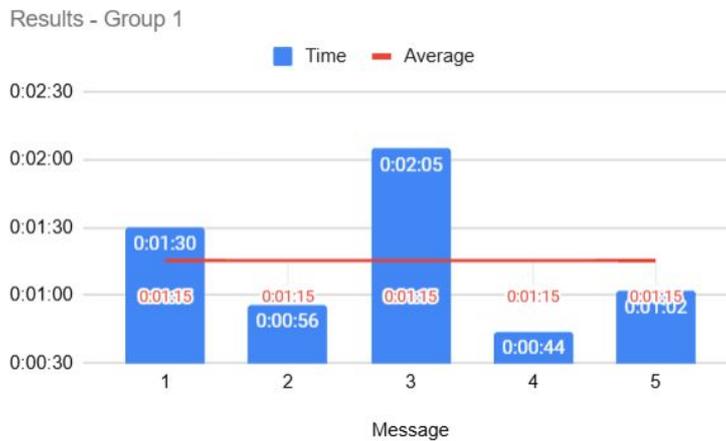


What will you find in this template?

Each team will collect data on their decryption performance by measuring the time taken to solve each encrypted message using different cipher methods (e.g., Caesar, Binary). This data will then be entered into a shared spreadsheet template. Students will use this dataset to create visual representations, including a bar chart showing the number of correct decryptions per method and a line graph of their average decryption times.

As part of their analysis, teams will compare their performance across methods and interpret the results to identify patterns. They will answer key questions such as: Which encryption method was decoded most efficiently? Why might that be?

This exercise will help students practice data collection, visual storytelling through graphs, and critical evaluation of technological efficiency, all within the context of mathematical cryptography.



Finally, once all the results have been entered, simply switch to the second sheet titled "Winner 🏆." There, you'll automatically see a podium displaying the top three teams with the fastest times in solving the codes. There's no need to modify anything on this page, the podium updates automatically.

Results	
Group	Avarage
4	0:01:11
3	0:01:13
5	0:01:13
1	0:01:15
2	0:01:18



+ ☰ Results per group ▾ Winner 🏆 ▾



CONCLUSION AND SHARING

Groups will present how they solved the codes.

Guided reflection:

- What was the most challenging part?
- How could this knowledge be applied to improve internet security?
- What did you learn about Maryam Mirzakhani?
- Do you think there is a difference between the way women and men work when it comes to encoding or decoding codes?



You can share the project social media if any teachers want to share with us their results using the following sentence and template with the links:

Don't forget to take a photo of your experience and share it with us!



[LinkedIn](#)



[Instagram](#)



[X](#)

BIBLIOGRAPHY AND REFERENCES

About Maryam Mirzakhani

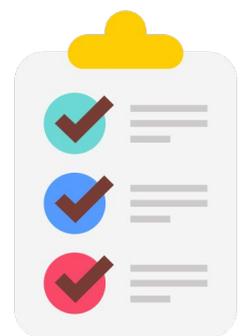
https://en.wikipedia.org/wiki/Maryam_Mirzakhani

About Cryptography

<https://en.wikipedia.org/wiki/Cryptography>

Steambrace

<https://steambrace.eu>





PROJECT EVALUATION

Activity Objectives	Key Competences (EU)	Evaluation Criteria
Learn about Maryam Mirzakhani as a female role model in mathematics.	Cultural awareness and expression	The student identifies key contributions of Maryam Mirzakhani and reflects on her impact on mathematics and gender visibility.
Understand basic concepts of cryptography and codes.	Mathematical competence and basic competences in science and technology	The student explains the functioning of simple encryption systems like the Caesar cipher and binary code.
Apply mathematical concepts (modular arithmetic, numerical systems) in a real-world context.	Mathematical competence	The student accurately uses modular arithmetic and binary conversion to encode and decode messages.
Develop problem-solving, collaborative work, and critical thinking skills.	Learning to learn; Sense of initiative and entrepreneurship	The student collaborates effectively in groups to solve encryption challenges, adapts strategies, and proposes improvements.
Create inclusive and accessible code systems.	Digital competence; Cultural awareness and expression	The student designs and tests a cryptographic system that is inclusive (e.g., for visual impairments), integrating math, design, and creativity.

