



**SUPER CYBER
KIDS**



**SUPER CYBER
KIDS**

Teacher Training Modules 5, 6, 7



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Module 5: Stronger Password



■ Goal – Objectives

The game introduces children to

- strategies for protecting against cyber attackers
- detecting and implementing actions against basic cyber-attacks
- understanding basic cyber threats
- basic prevention technologies
- using software tools to protect digital devices
- strategies to protect their personal information while surfing the web

■ Specific Topics Discussed

- basics of cryptography
- definition of password
- how to create a good password



Password



A string of characters that allows access to a computer system or service

Oxford Languages



Co-funded by
the European Union



Confidentiality

CIA

Availability

Integrity

- Confidentiality is limiting data access
- Integrity is ensuring your data is accurate
- Availability is making sure it is accessible to those who need it

Most commonly used password in 2024

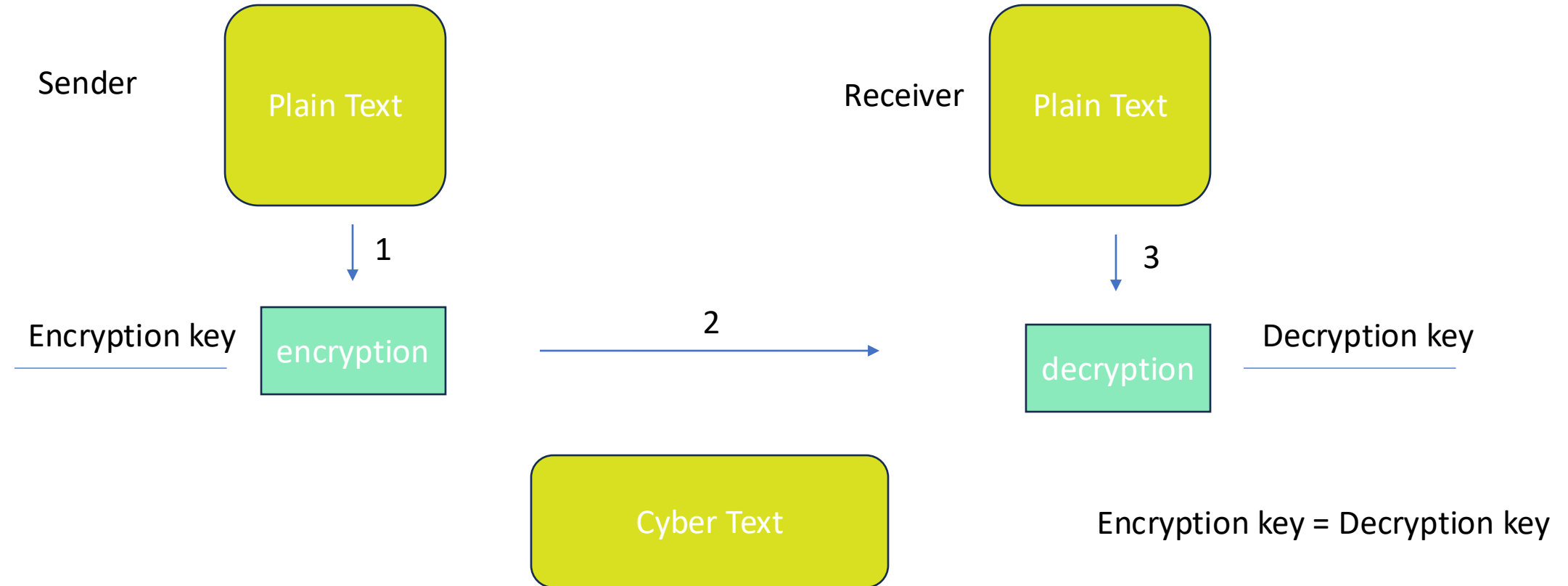
123456
password
123456789
12345
12345678
qwerty
1234567
111111
1234567890
123123

abc123
1234
password1
iloveyou
1q2w3e4r
000000
qwerty123
zaq12wsx
dragon
sunshine

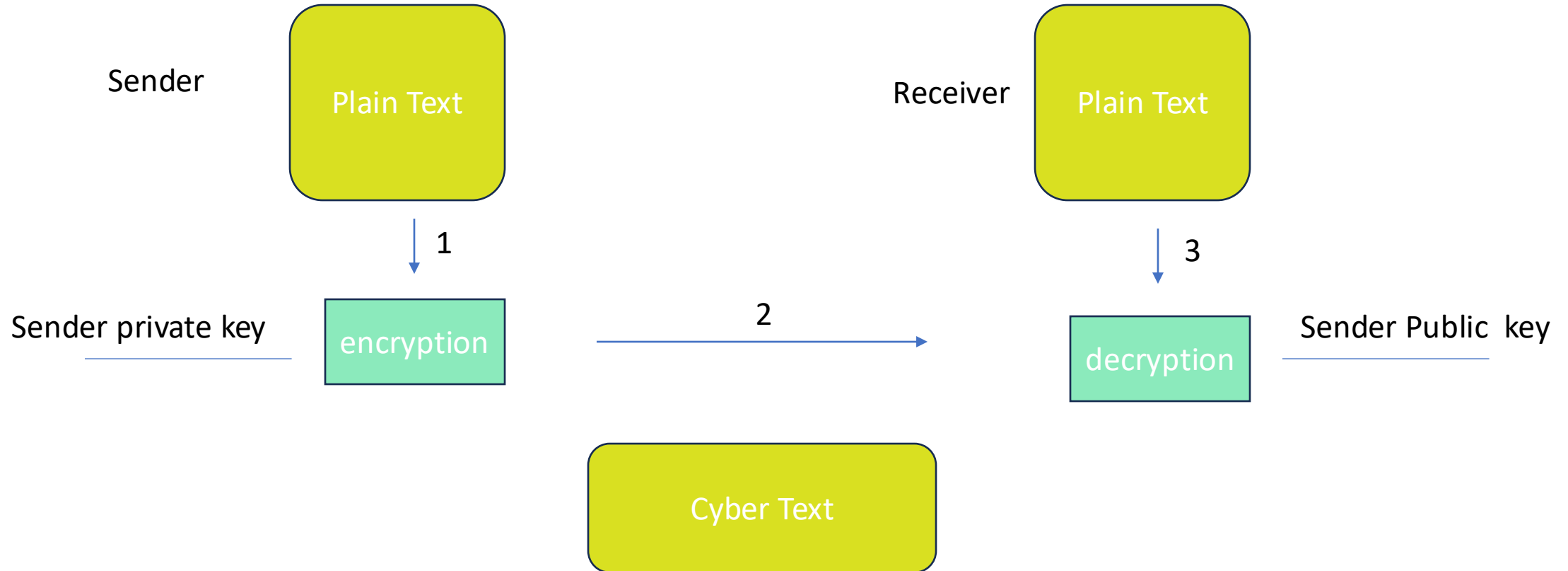
What do they have in common?



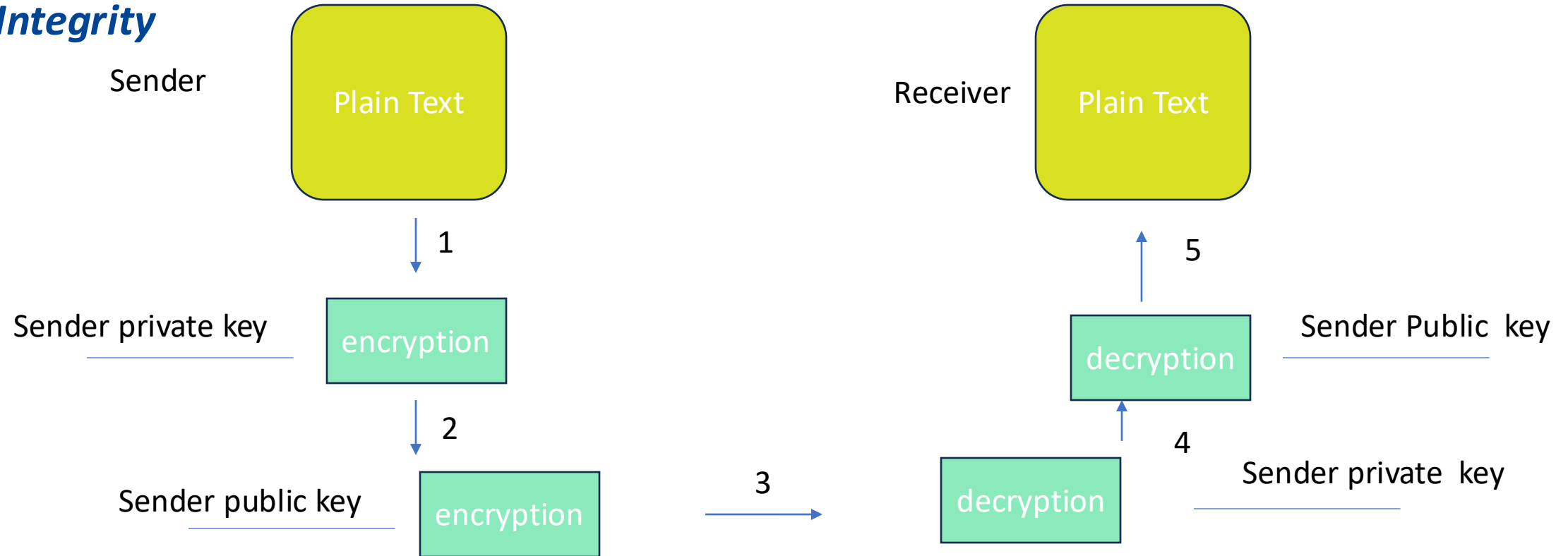
Confidentiality



Integrity



Confidentiality, Integrity





Tips to create a strong password:



1. Use a mix of uppercase and lowercase letters, numbers, and special characters.
2. Make it at least 12 characters long.
3. Avoid using easily guessable info like names, birthdays, or common words.
4. Use a passphrase or a series of unrelated words.



How to create a really good password? Use an acronym!



When I find myself in times of trouble, Mother Mary comes to me
Speaking words of wisdom, let it be

WifmitotMMctmswowlib!@



Co-funded by
the European Union



■ Goal – Objectives

The game introduces children to

- detecting and acting against suspicious emails
- what personal data is
- phishing attacks
- classifying abusive content
- threats associated with personal data
- identifying and protecting against untrue or untrustworthy information sources found online
- online etiquette and behavior
- classifying abusive content.

■ Specific Topics Discussed

- Definition of «hater» and «troll»
- Differences between a real and fake profile
- Good practices for sharing data online



Risks related to Social Media



- Data breach
- Privacy violation
- Malware
- Fake News
- Haters
- Cyberbullying



Co-funded by
the European Union



Any kind of communication in speech, writing or behavior that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, color, descent, gender or [any] other identity factor

United Nations Strategy and Plan of Action on Hate Speech

Examples of online hate are 'trolls' who:

- enter online meetings and use hateful, racial slurs targeting participants;
- hateful groups online who put out posts that dehumanize identifiable groups.



Difference between bullying and hate



Bullying targets an individual, while hate may incite violence towards an entire group of people



- Social media platforms are a real and powerful means of interaction between real people but are also populated by fake profiles
- Purposes of fake profiles: spreading fake news, scams, stealing personal information or damaging the reputation of a company or person
- How to recognize a fake profile: stolen or AI-generated profile picture, few post and few followers.





Good practices when sharing data online



- Use strong passwords
- Use only safe apps and programs
- Do not click on links or buttons without thinking first
- Use third-party apps with caution
- Think before sharing



Good practices on social media



- Use strong passwords
- Manage and update your privacy settings
- Use two-factor authentication
- Do not click on links or buttons without thinking
- Use third-party apps with caution
- Think before sharing

■ Goals- Objectives

The game introduces children to

- understanding basic cyber threats
- responding to inappropriate content by taking the correct actions
- using strategies to protect against and prevent cyberbullying
- utilizing strategies to stay safe in online social contexts
- strategies to identify online frauds
- classifying abusive content.

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems.



Cisco

- Detection and prevention of malicious code
- Usage of authentication
- Usage of cryptography





Examples of Malware



- **Viruses:** pieces of code that spread by copying themselves into other programs, so they are executed every time the infected file is opened
- **Worms:** do not need to infect other files to spread, as they are executed and replicated automatically, mostly by exploiting the Internet
- **Trojan Horses:** in addition to having "legitimate" functionalities, they contain malicious instructions that are executed without the user's knowledge. They do not have self-replication capabilities, so to spread they must be knowingly sent to the victim.



How to recognize malware



- The device freezes or crashes unexpectedly
- Reduced web browsing speed
- Files are modified or deleted
- Presence of unknown files, programs, or desktop icons
- Programs deactivate or reconfigure themselves automatically
- Emails are sent without the user's knowledge

- According to the report by IDEA:
 - approximately 3.5 million gamers aged between 6 and 14
 - approximately 4 million gamers aged between 15-24
- Nearly a quarter of online gamers experienced an account breach in 2021
- According to market surveys (e.g. Global Market Insight):
 - the online gambling market is expected to reach US\$ 370 billion by 2032
 - active online players could reach 210 million by 2025
- According to Osservatorio Nomisma:
 - in 2023, the percentage of frequent gamblers in Italy increased
 - 37% of 14-19 year olds have played online gambling games

- Privacy issues (use of chat, webcams, and microphones)
- Caution in managing credit cards
- Malware exposure to violent content
- Addiction: «Internet Gaming Disorder»
- Cyberbullying
- Hate speech
- Grooming
- Social isolation





Thank you!

Questions?



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.