MAKE SCHOOL

Computer Security

Check In

MAKE SCHOOL

It’s always good to take a break when things get stressful! What are some of your weekend plans that don’t involve school work?

What we're going to learn

MAKE SCHOOL

- What is computer security
- The main areas of computer security
- Intro to cryptography, ciphers, and algorithms

Computer Security

The study and application of how to protect information systems from theft, damage, misdirection or disruption

Computer Security usually focuses on four main areas:

1. Confidentiality
2. Integrity
3. Availability

MAKE SCHOOL

Why is computer security important?

Students, write your response!

MAKE SCHOOL

Types of vulnerabilities

MAKE SCHOOL

Write down as many different types of computer security vulnerabilities as you can think of

Students, write your response!

Common types of vulnerabilities

MAKE SCHOOL

- Backdoors
- Denial of Service Attacks
- Eavesdropping
- Phishing
- Privilege Escalation
- Social Engineering
- Spoofing
- SQL injection
- Malware

Confidentiality

MAKE SCHOOL

Controls access to information, protects from unauthorized viewing

This can be applied to data, objects, resources

Some examples of techniques to ensure confidentiality:

- Passwords
- Access tokens
- Policies/training
- Physical Controls

Integrity

MAKE SCHOOL

Protect data, objects, and resources from unauthorized alteration

Ensures accuracy and completeness

Some examples of techniques to ensure integrity:

- Hash verifications
- Digital signatures
- Access controls

Availability

MAKE SCHOOL

Make sure the information is available to authorized users

A system that no one can access is secure, but it's also useless, security is all about making sure those who should access the data can and those who shouldn't are blocked

Some examples of techniques to ensure availability:

- Hardware redundancy
- Monitoring system
- Countermeasures against attacks like DoS

Cryptography

The underlying concepts of cryptography have been around for a number of years

Cryptography is the practice and study of different techniques that are used to secure information from adversaries

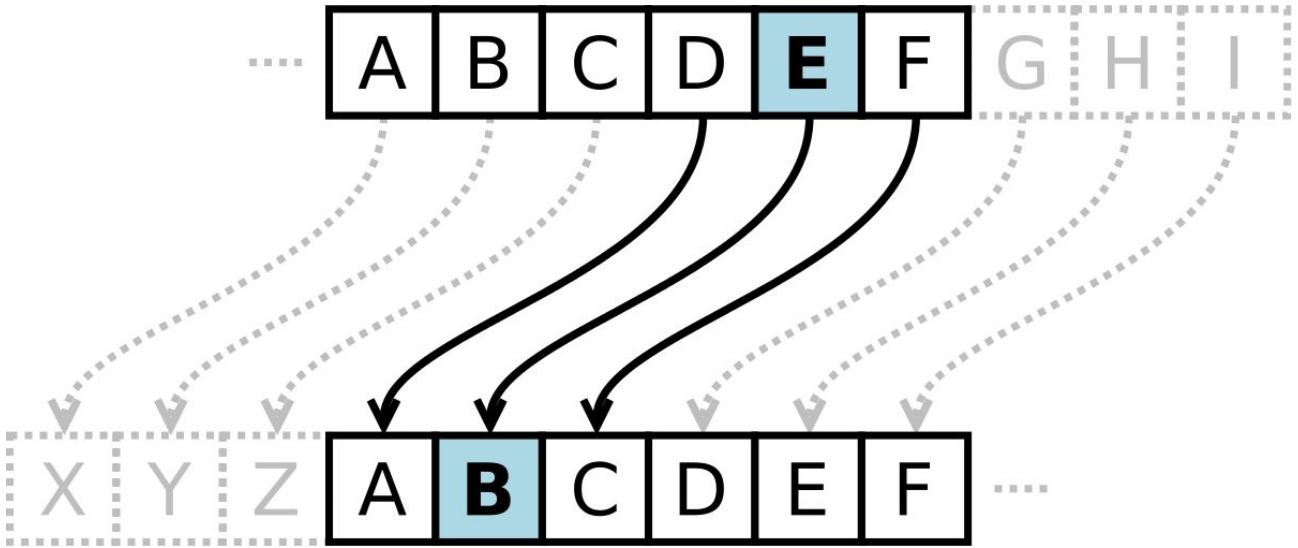
Cryptography Basics

MAKE SCHOOL

- Encryption: hiding the information
- Decryption: making sense of the hidden information
- Cipher: the algorithm used to encrypt or decrypt

Caesar Cipher

Let's watch a video explaining the Caesar cipher!



Caesar Cipher Challenge

MAKE SCHOOL

Now that we understand how the cipher works let's write some code to implement it

First write a function called encrypt() that takes in two arguments, the text to be encrypted and the shift, this function will return the encrypted text

Then write a function called decrypt that will take in encrypted text and a shift and return the decrypted text

Students browse: repl.it/@JessDahmen/CaesarCipher?lite=true

MAKE SCHOOL

How could we break the Caesar Cipher without knowing the shift (key)?

Students, write your response!

Caesar Cipher Challenge

Pretend you are a malicious person who has intercepted a secret message encrypted with a Caesar cipher. Write some code that will decode the message with an unknown key!

Modern Encryption Examples

MAKE SCHOOL

- Triple DES
- RSA
- Blowfish
- Twofish
- AES