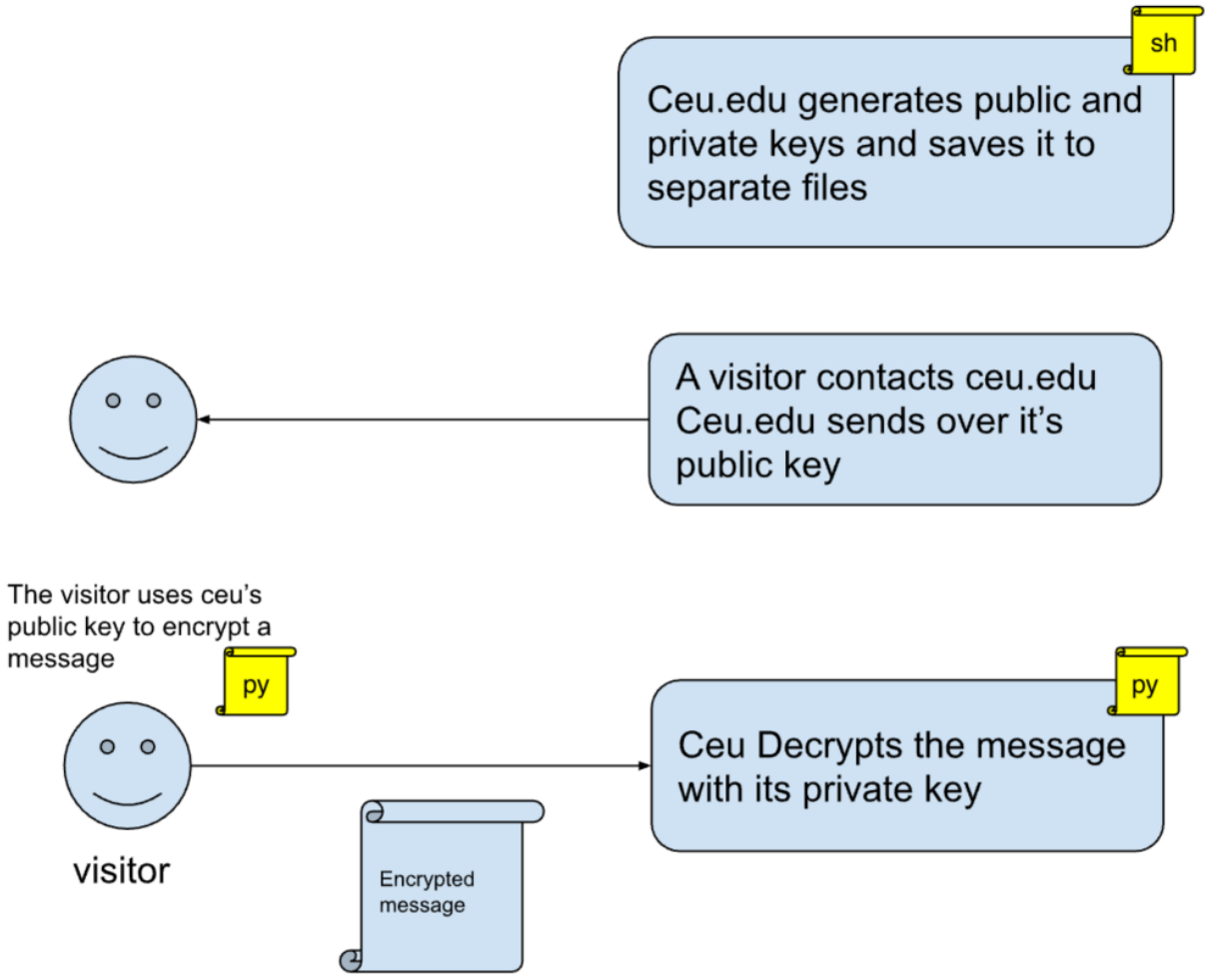
Homework - PKI

Assignment

Let's simulate a simplified message passing with https://www.ceu.edu



Get in groups of two (a single group of three students is allowed if needed). One group peer acts as ceu.edu and the other as a visitor. If you are in groups of three, let's simulate two different visitors (so one peer acts as ceu.edu and two pees act as independent visitors).

1. (At the webserver installation time), ceu.edu generates a key pair. It saves it to two files, *ceu_key* and *ceu_key.pub*.
   Write a shell command script that does exactly this: Generates the two keys. Write this command into a new file called *key_generation.sh*

2. When a visitor contacts the CEU website, ceu.edu sends the public key to the visitor.
   Distribute the public key file among the team. (in email, messenger, … it doesn't matter how you get this done)
3. The visitor creates a (short) message and encodes it with CEU's public key.
   Write a Python script that does exactly this. That's two Python scripts in total if you are in a group of 3.
4. The visitor writes the encrypted message to a file and sends it to ceu.edu.
   Send the file containing the encrypted message back to your peer. This logic comes into the same Python file as (3)
5. CEU (in a new Python script) Loads its private key and the encrypted message from the disk. Then, it decrypts the message and prints it to the screen.
   Write a Python script that does exactly this.

You must create at least six files: key_generatio.sh, two Python scripts, a private key, a public key, and one encrypted message per visitor.

Delivery

Please deliver the following files via email:

1. In a single PDF: Copy the source code for the scripts and the keys you wrote as a team.
   This is a single PDF created by the group.
   a. The ceu.edu key generation command
   b. The contents of the private key and the public key files (print each of them to the screen and add it to the pdf)
   c. Python file: Visitor encrypts a message with CEU's public key and writes it to disk (that's 2 Python scripts if you are in a group of 3)
   d. Python file: CEU reads its private key and the message, decrypts it, and prints it to the screen.

2. Attach to email separately:
   a. The file that contains the encrypted message (That's two files if you are in a group of 3)

Make sure that you add the CEU student IDs of your team to BOTH the PDFs and to the email body.

Send everything to: ceu-data@googlegroups.com

Getting help

@ mention me and Mike on Slack.

Deadline on the next page

Deadline: Tuesday 21 Nov, 11:59 pm

Late submissions

1% of “homework completeness” points are deducted every hour between the deadline and the submission date. Missing delivery counts as 0%.