Mock Semifinals 2025 Web-Based Challenge
Challenge 1: Cryptography Pop Quiz

Description
The following are several problems frequently encountered in cryptography. Solve them, and provide the answers.

Problem 1 (JSON Web Token): Cryptography is often used in websites to ensure the integrity of web tokens. The following is a JSON Web Token (JWT) that is signed, but not encrypted. What is the answer contained within?

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnN3ZXIiOiJvY2JkRWlaWE9mQ3ZSbnpwZ0NQY1dQVlNwZnh3RGJlQiIsImlhdCI6MTczNzEwMjc5OH0.-msNIOHKcZEe4VeT_xAGMgRewKrNend7vF7DVMonxZ0

Problem 2 (Integer Factorization): The integer factorization problem is considered a computationally "hard" problem for computers to do, for large enough numbers. This makes it useful for cryptography. The following numbers both are made up of two primes multiplied together. Find the two factors of each number. Submit the larger prime factor of the first number, and the larger prime factor of the second number.

- 90145323082886043 13
- 53642063165796301873163365194801401508596126636 1972067591207

Problem 3 (Hash Cracking): Hashes are one-way (irreversible) functions. However, you can "crack" a hash by trying a bunch of different strings until you get a string with the same hash. I hashed with MD5 a sentence that was in the format "Pratham and Priyam picked ___ peppers by the pier", with the blank filled in with a number. I got the hash "23823491c561afa2295e0fa9de3fbd71". How many peppers did Pratham and Priyam pick by the pier?

Problem 4 (One-time Pad): The one-time pad is an example of a perfectly secure cipher, with its downside being that the key must be as long as the message. It works by XORing each byte of the key with each byte of the plaintext to get the ciphertext. If the key (in hex) and the ciphertext (in hex) are listed below, what is the plaintext, ASCII decoded (not in hex)?

- Key: 95fd40b01fe3d9ae4a4852c0a5d385f6
- Ciphertext: dab334d44c809fda1d3d3bb5c3a7f683

(continued on next page)

Submission Instructions

You must submit your answer as a .csv file, in the following format:

- ☐ The first line of the submission should contain your team number. In the case of this practice competition, please use your unique ID instead.
- ☐ The second line should contain the answer contained in the JWT.
- ☐ The third line should contain the two prime factors found, separated by commas, with the factor for the first prime first.
- ☐ The fourth line should contain the number of peppers picked.
- ☐ The fifth line should contain the decrypted plaintext.

Each ciphertext is weighted equally in scoring. You will get points for each field that is correct. You will get 10 tries to submit before you will not be able to submit anymore.

Example Submission

```
16-2250
zXEYnrRKdLaBSTAMrZIDTFFKOAMavSBt
9208413770544001,264171691710315098764448642995914749917
1424
QnZVbzEdIRVHxwMj
```