Cipher Riddle:

Upon completing an introductory course on cryptography, Tom, a Computer Science student, decided to utilize a classical cipher to safeguard certain secrets.
In an attempt to enhance the secrecy of his cipher text, he altered the resulting ciphertext, believing that it would be difficult for anyone who gains access to it to decipher and obtain the confidential information

The resulting secret is as follows:
KDEwMTAwMDExMTAxMDEwMTAwMTEwMDExMTAxMDAxMDAwMDExMTEwMDAwMTEwMTAwMTAxMTAxMTAwMTAxMDEwMCwxMDAxKQ

-> Given one of Tom's encrypted secrets, obtain the original plaintext secret that Tom tried to safeguard

* Note: All Tom's secrets are valid English words and sentences that only contain alphabetic characters [A-Za-z].

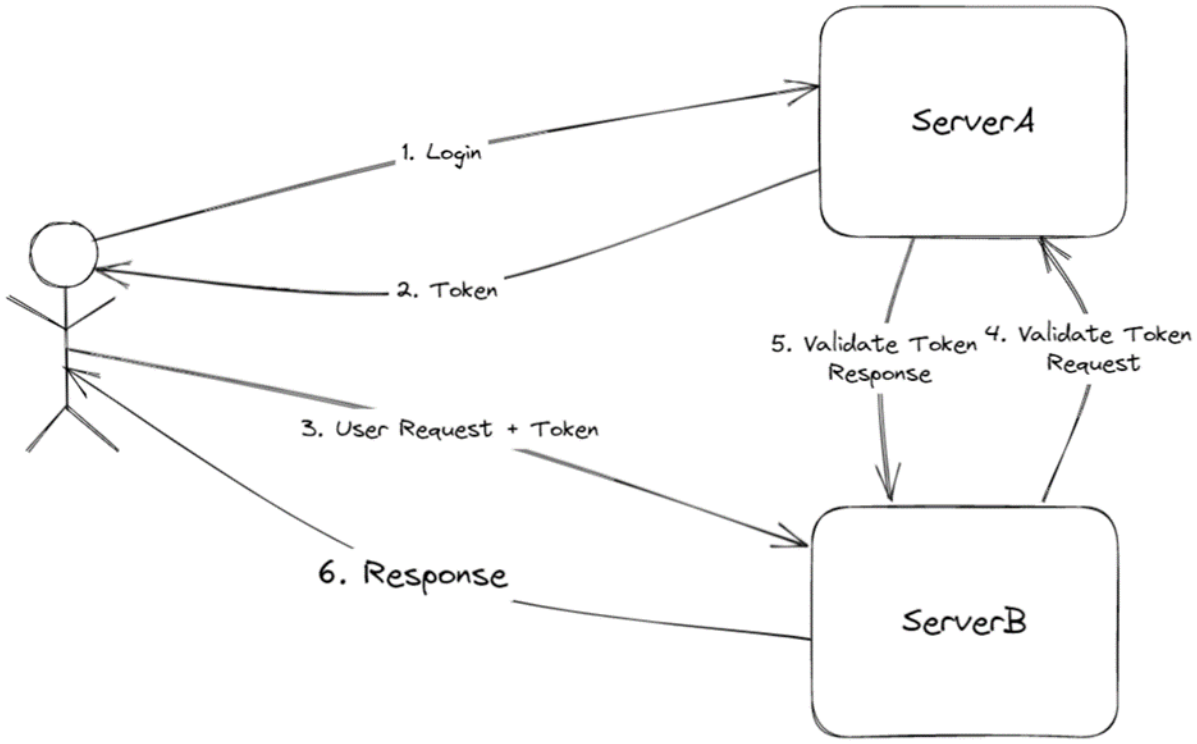
Example of supplied ciphertext:
KDEwMTAwMDExMTAxMDEwMTAwMTEwMDExMTAxMDAxMDAwMDExMTEwMDAwMTEwMTAwMTAxMTAxMTAwMTAxMDEwMCwxMDAxKQ

What we expect from you:
The secret encrypted by Tom
Note: this is not the solution! This is just an illustration for what we are expecting from you.

##

Server Riddle:

In a backend environment consisting of serverA and serverB, serverA is responsible for authenticating users by providing a session token (JWT) upon validating their credentials. However, when the user interacts with serverB, it cannot verify the token's legitimacy due to it being signed using a symmetric encryption algorithm, and only serverA has the key required for signing and validation.



To mitigate this issue, the maintainers of serverA proposed using Asymmetric Encryption (using RS256 algorithm) to sign and validate tokens. This approach involves token signing with a secret key kept on serverA, and token validation with a public key embedded as JWK within the JWT header. Consequently, any server can authenticate the token's legitimacy without requiring a call to serverA, reducing latency.

-> Given a JWT, your task is to modify the token by setting the "admin" attribute to "true" so that serverB will be deceived into believing that you have admin privileges.

Example of supplied JWT:

eyJraWQiOiI5MmM1YTU1MS0yNjFlLTQ5OTktOGQyMy0wMjM1YTg2NTM1NjEiLCJ0eXAiOiJK
V1QiLCJhbGciOiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSU0EiLCJlIjoiQVFBQiIsImtpZCI6IjkyYzVhNT
UxLTI2MWUtNDk5OS04ZDIzLTAyMzVhODY1MzU2MSIsIm4iOiI2dnNKVzdXQ1NfTnlXd0lBWkt
hYXNZMVVTa1lmdEdXOXlYeFhXWFlmcjZ3YnZXMDNpRkRaNDZaN09VS2hPZ0lVWGYzUzVa
VGF3NVY2WXdFNl8xTVJqUmhBdURlNmJvcFdtMzRIazVnbTFSSEdSWEIzTFJwU3UwTWlkT
GxwTkh5ZXFSekRHdDZDVTFhMWR0ZExkVTB0aThqeGNfNlJBdlpUTWJjdVZQaGU4d1o5LW
NYME9yZGlzZXF3bEVvZnNWdndEODZDd0g2TENXOF9RVUZmRXZZSzRXdm55XzJzc0Ffbn
MyMkpaLTZGdXpTLVNmTFFrUWlORXVhMWNnMVBaa1RHd09mVlZ0c1Y0NVRaOGpRYnF5d
Gc3T2p4VDBxU1pXWEZQamVCQTVNQ3o3MzQyWXlFSjlxbmZock9WTXZ6OEZjdERuaktiTT
MzLWplTlBwcHM1dVlxSHcifX0.eyJpc3MiOiJodHRwczovL3NlcnZpY2VBLmVudjo4MDgwIiwiYX
VkIjoiYWNjb3VudCIsImlkIjoiNTAxYTFiZjQtYjUyMy00OTNjLWI0NTctYWVmOTM1YTI0MWJhIiwi
c2NvcGUiOiJwcm9maWxlIiwibmFtZSI6IkJvYiBNYXJsZXkiLCJlbWFpbCI6ImJvYi5tYXJsZXlAaG
Fja3RyaWNrLmNvbSIsImFkbWluIjoiZmFsc2UiLCJyYW5kIjoiMzgifQ.d18LyHFFtBO9gxiwtc3A_
M77kc1u7E8S9QuD5fE8haG0F_b9NvbSP83a5p0gcrIOebb0hHH1Wk-4L6mqj2QC9bDbKIVvx2
bmWW8kVyGmMRDs9ccn8PIfT1T3Gsgi-9Smqmf196MHBV5BxGsGFo8ah8o6RP8NKsmuLZm
VNFg0bbcs81ndR2hwYzZBeuUQxZfCedqsoQkAie9zFjWu92gMsDqlzM-KdeUi6OyQn3l-iD2N0p
QuqlmhHq8P_pAHsETgQ6RnugylkPsKMDs0cotaun8cBrltFIKGcrwRbpGqf75Golv10BO0q1xu8
pAWW7LEsZ3x7xxfz0lW0ZBVbfTuXw

What we expect from you:

A valid JWT with "admin" attribute set to “true”

Note: this is not the solution! This is just an illustration for what we are expecting from you.

##

Pcap Riddle:

A network security analyst received an alert for a suspicious activity where a certain machine was sending multiple DNS queries to an unknown DNS server (188.68.45.12).
Upon examining sample packets, he suspected a data exfiltration process and immediately disabled network access for the machine to initiate an investigation.
After analyzing the packets, the analyst was certain that a malicious actor was leaking the company's data. However, he could not determine the exact nature of the leaked information, as it was being sent in an obfuscated manner that he could not decipher.

-> Your task is to examine a PCAP file and uncover the complete secret that was leaked by the malicious actor.

Example of supplied PCAP:
PCAP file encoded in Base64 format.

What we expect from you:
The secret leaked by the malicious actor
Note: this is not the solution! This is just an illustration for what we are expecting from you.

##

Captcha Riddle:

You have been presented with a challenging security task - developing a solution to bypass the CAPTCHA generated by Amazon.com such as the one accessible via the URL "https://www.amazon.com/errors/validateCaptcha"
The objective of this challenge is to develop a solution that can evade the security measures put in place by Amazon.com and successfully solve the CAPTCHA, without requiring any human intervention.

*Note: Solution can make use of open source libraries.

Example of supplied CAPTCHA:
Numpy array representing the CAPTCHA image.

What we expect from you:
The solution for the CAPTCHA
Note: this is not the solution! This is just an illustration for what we are expecting from you.