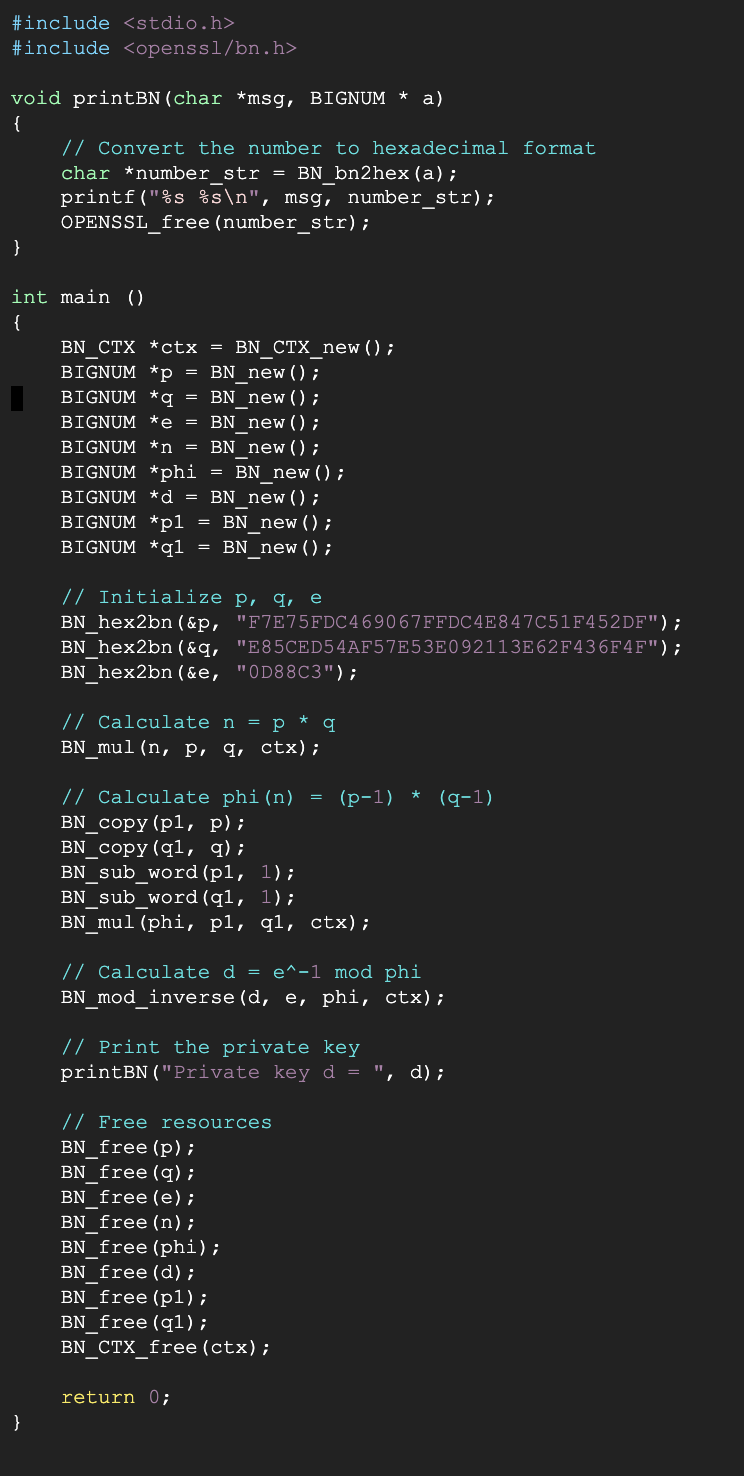
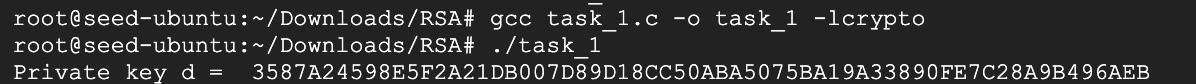
**Task 1:**

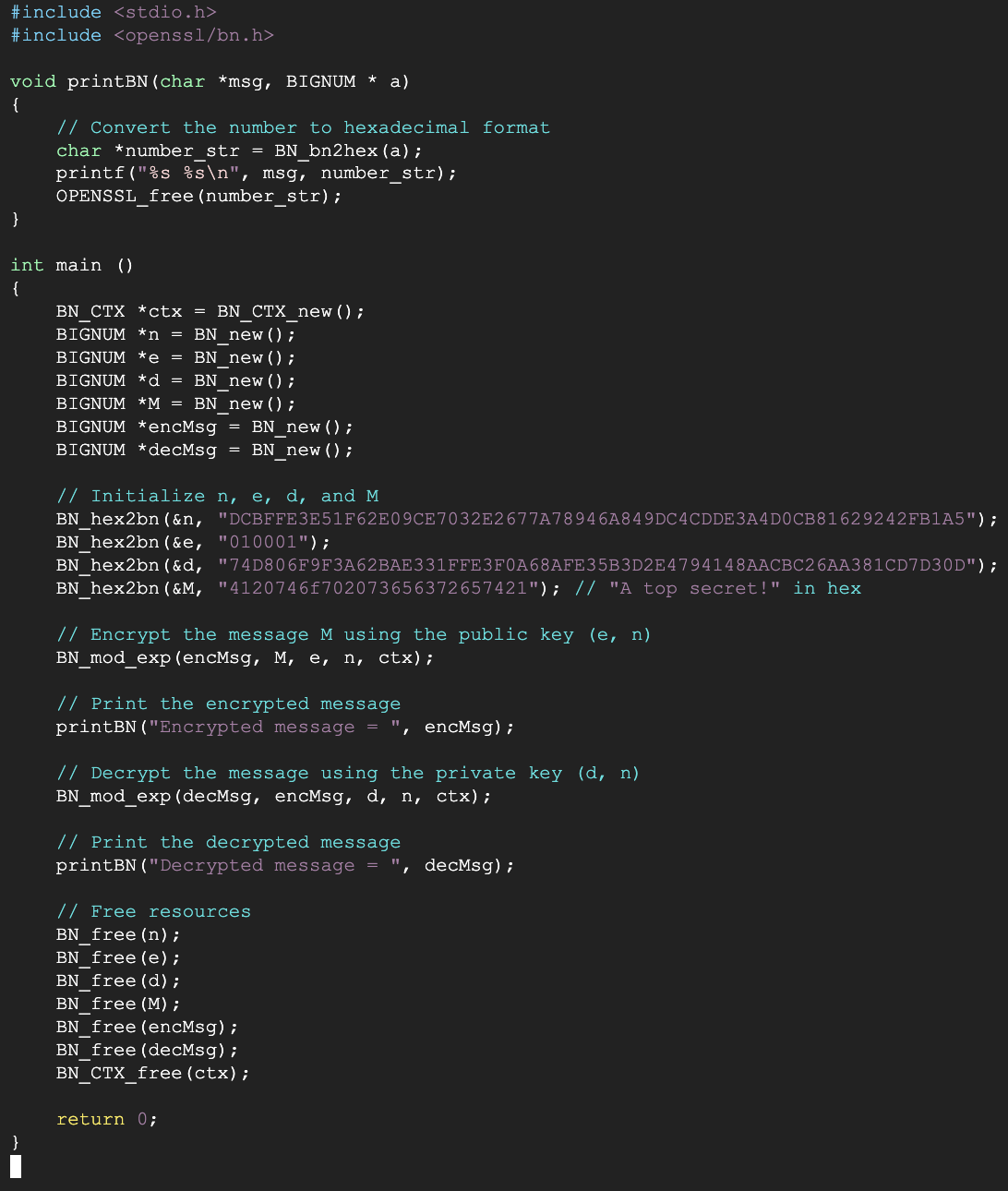
Code:  


Result:

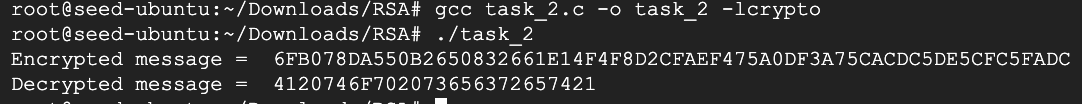


**Task 2:**

**Code:**

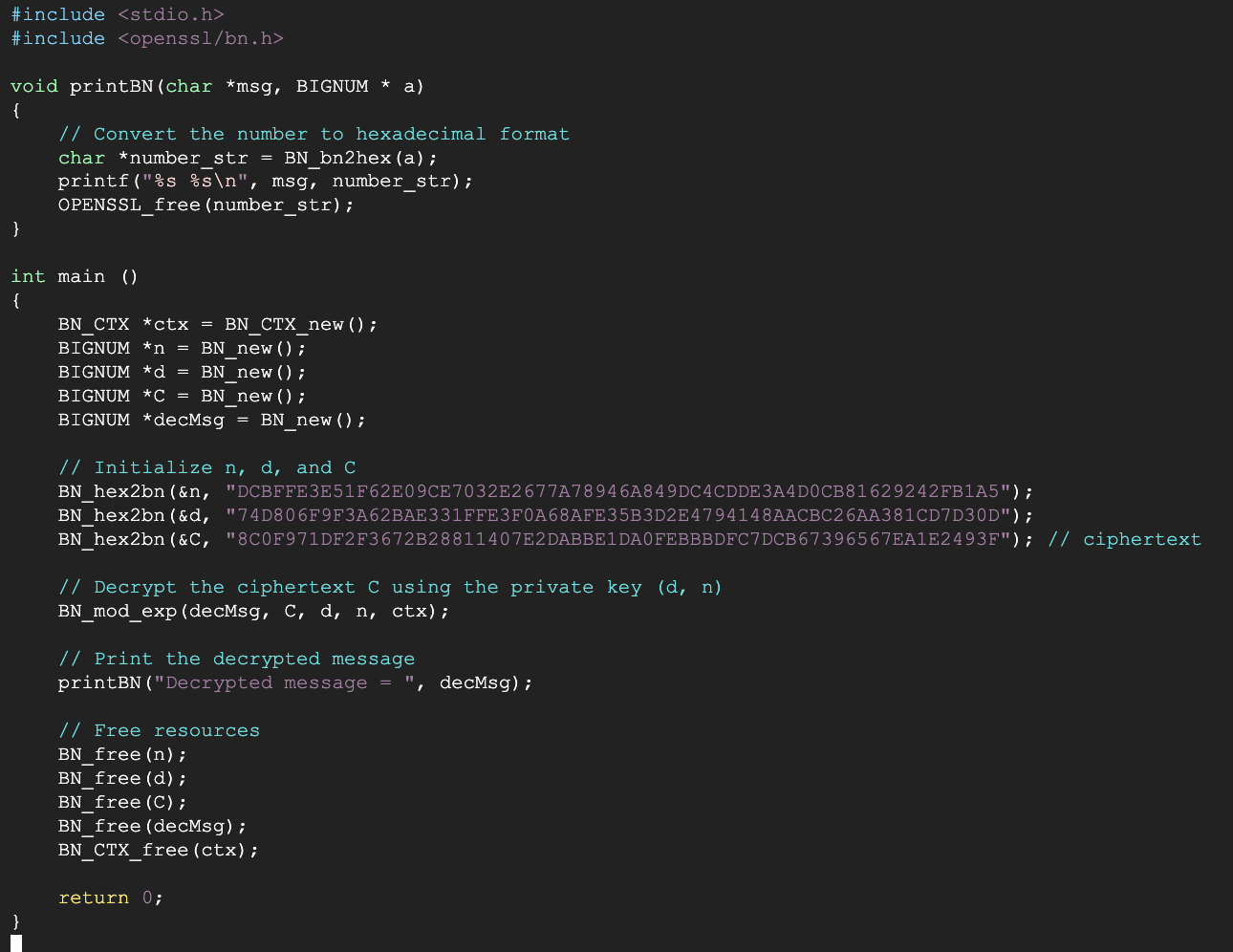
****

**Output:**

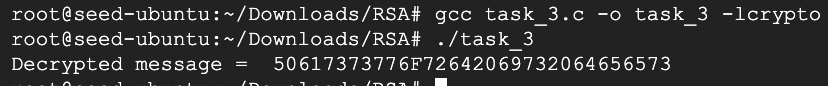
****

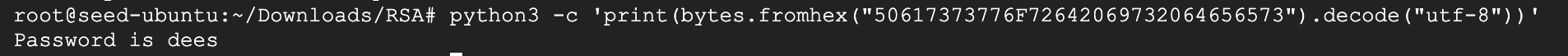
**Task 3:**

**Code:**

****

**Output:**

****

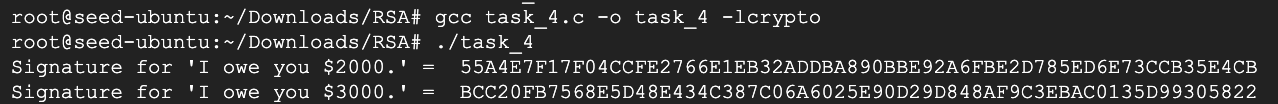
****

**Task 4:**

**Code:**

****

**Output:**

****

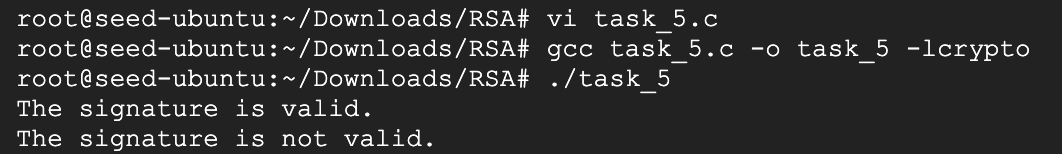
The task involves signing two similar messages and comparing the signatures. Even though the messages “I owe you $2000.” and “I owe you $3000.” are very similar, their signatures are completely different. This demonstrates the sensitivity of digital signatures to even minor changes in the message. Any modification, no matter how small, results in a completely different signature, ensuring the integrity of the signed message. This is a fundamental property of cryptographic systems.

**Task 5:**

**Code:**

****

**Output:**

****

The verification process involves checking if the signature S associated with the message M is indeed from Alice. This is done by computing m = s^e mod n and comparing m with the original message. If they match, the signature is valid.

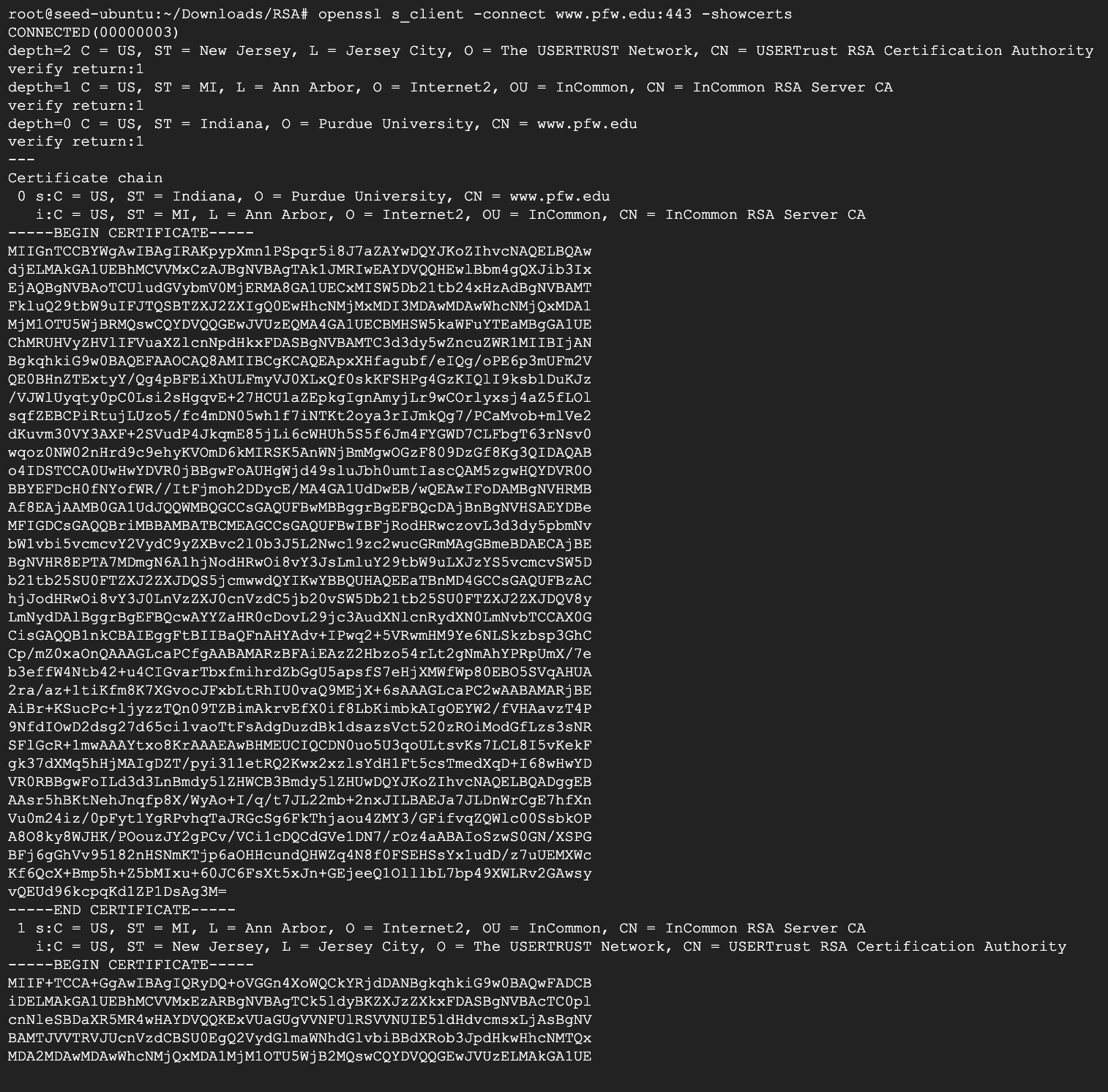
In the first part of the task, the signature S is valid because the computed m matches the original message M. This means that the signature S is indeed from Alice.

However, in the second part of the task, the signature S is corrupted (the last byte changes from 2F to 3F). When the corrupted signature is used to compute m, it does not match the original message M. Therefore, the verification process correctly identifies that the corrupted signature is not valid.

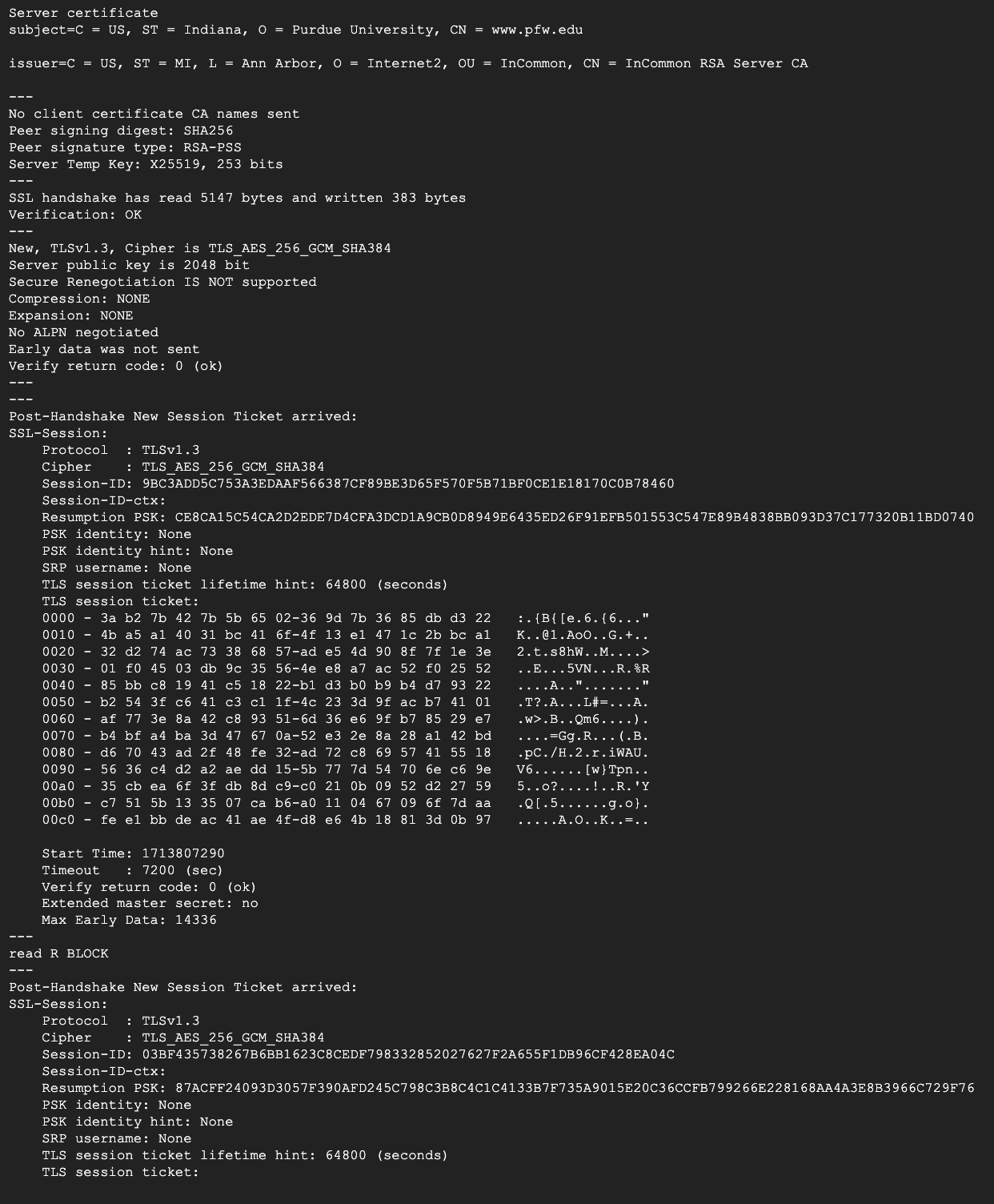
This demonstrates the sensitivity of the verification process: even a one-bit change in the signature results in a completely different output, leading to the failure of the verification process. This property is crucial for the security of digital signatures. It ensures that any tampering with the signature (even if it’s very minor) can be detected. This is a fundamental aspect of cryptographic systems. It’s important to note that while the signature is sensitive to changes, the process of signature verification remains the same. It always involves computing m and comparing it with the original message. The result of this comparison determines the validity of the signature.

**Task 6:**

**Step 1:**

****

****

****

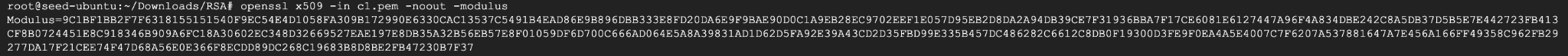
**c0.pem:**

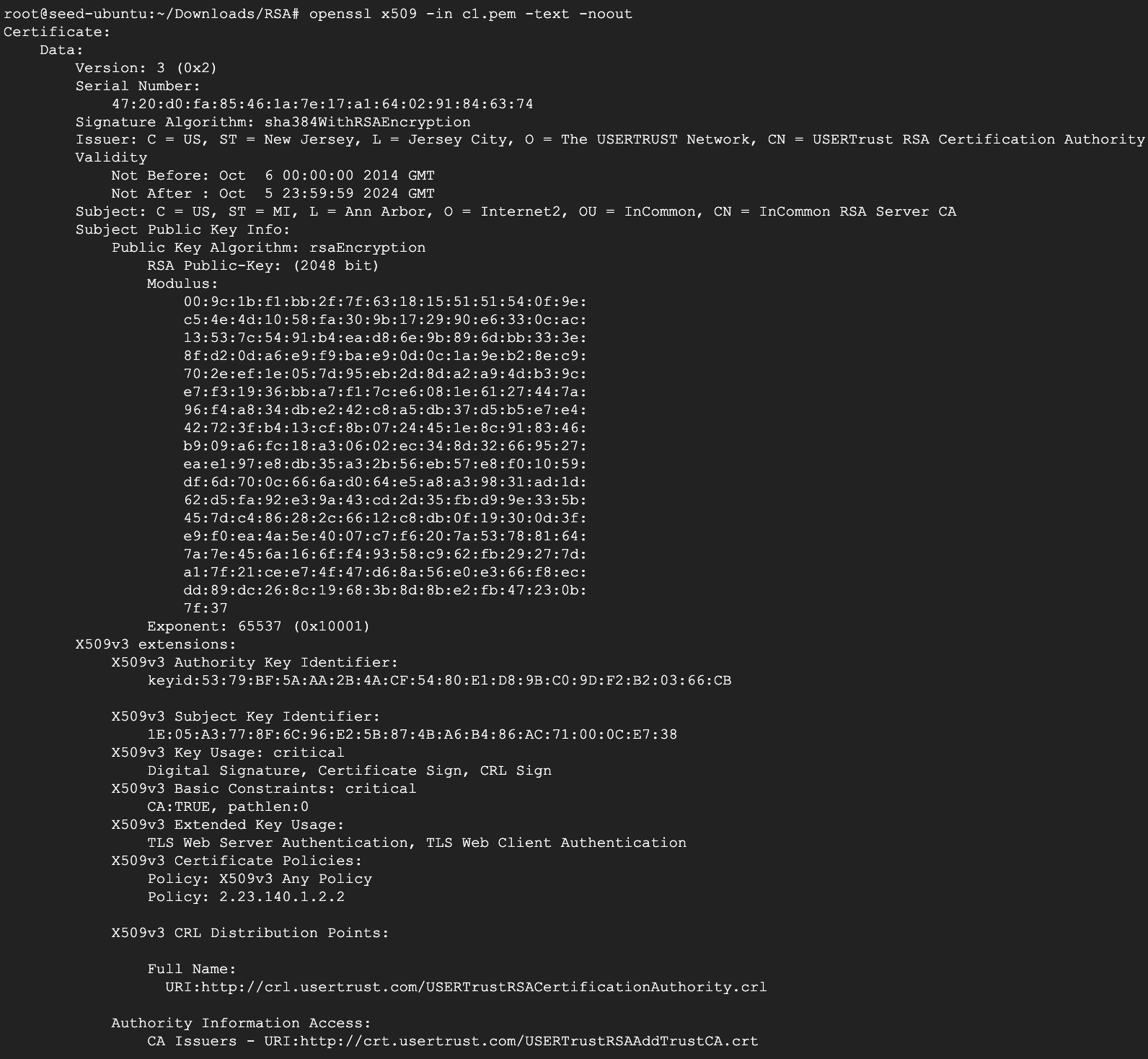
****

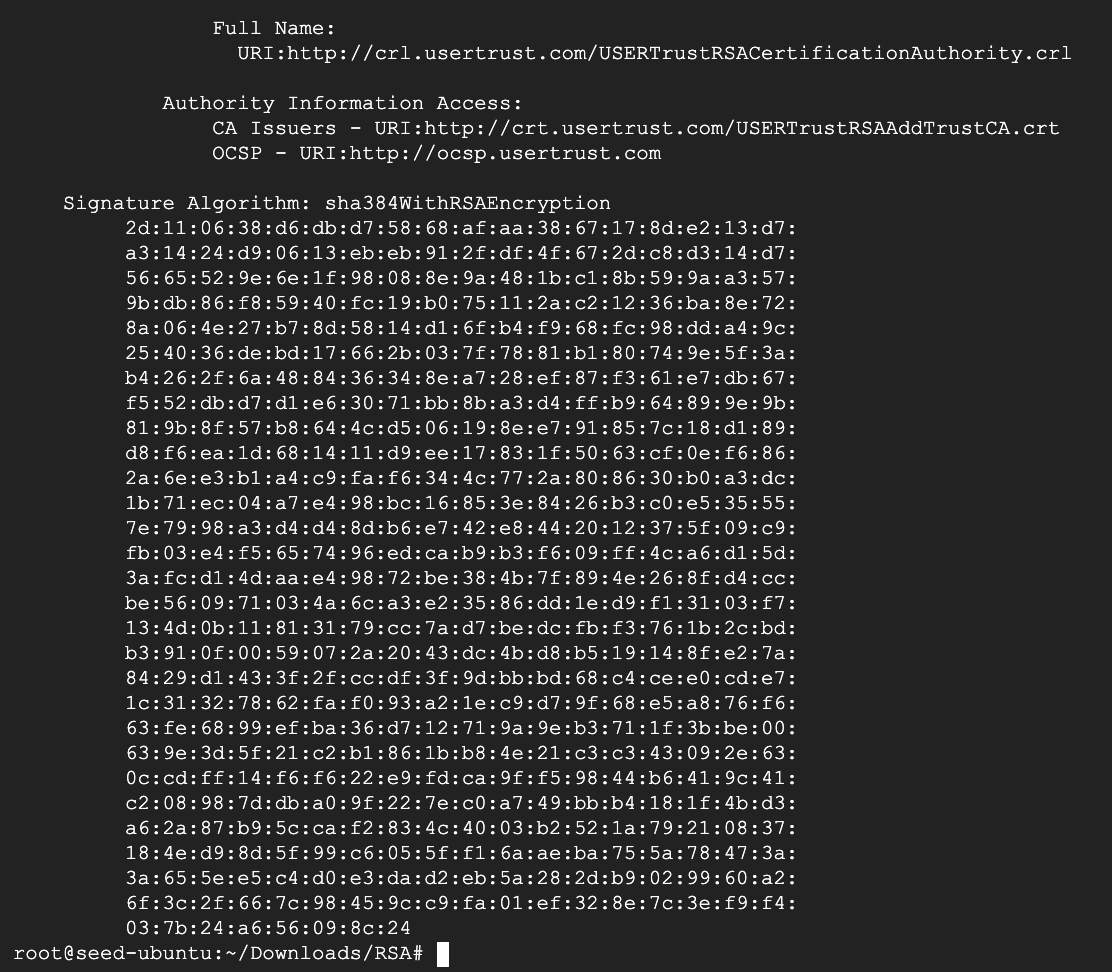
**c1.pem:**

****

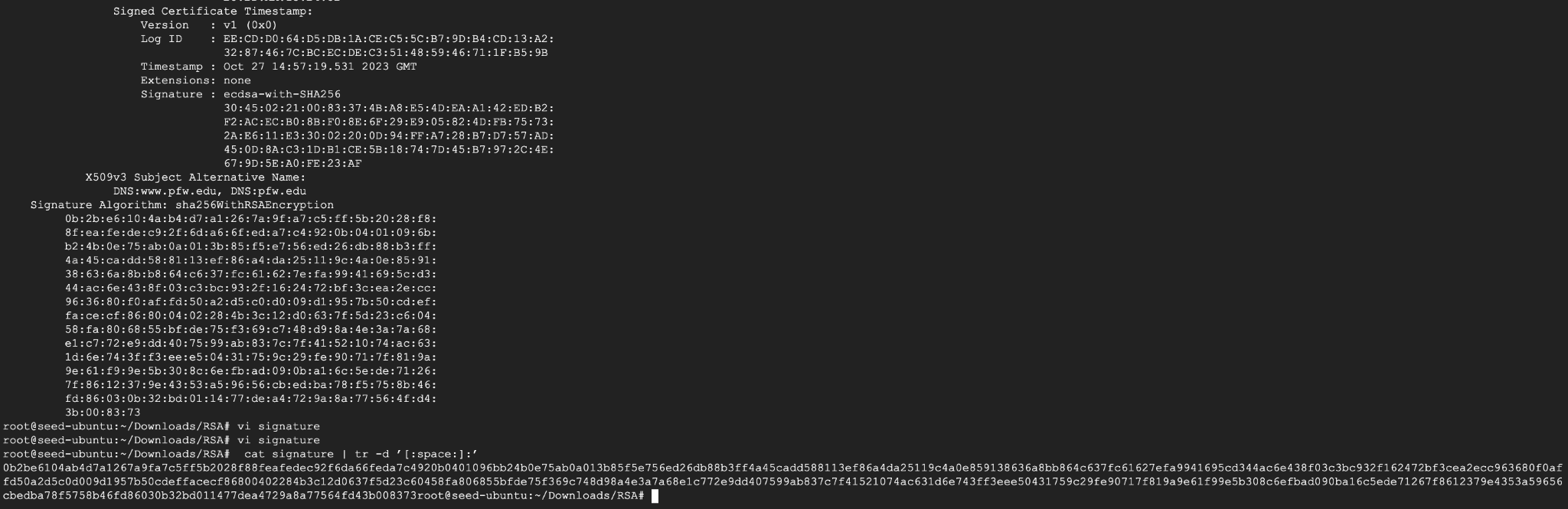
**Step 2:**

****

****

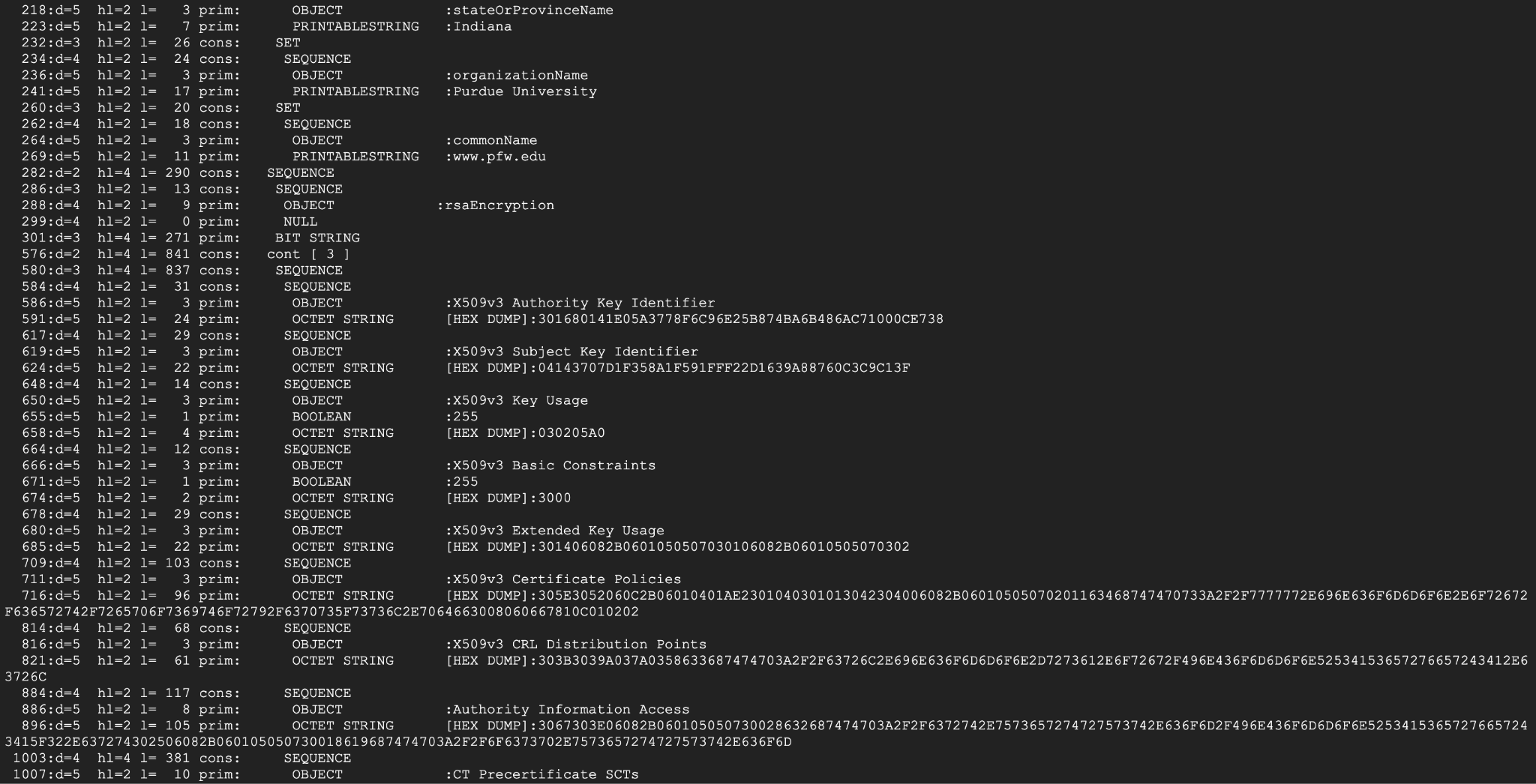
****

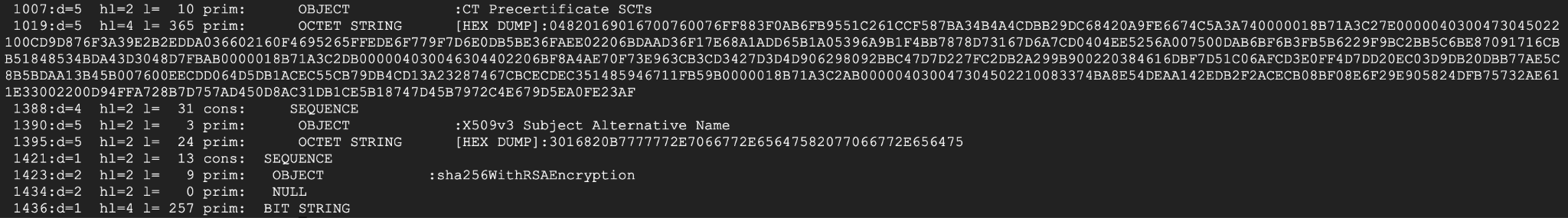
**Step 3:**

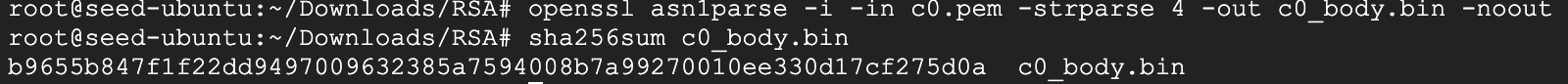
****

**Step 4:**

****

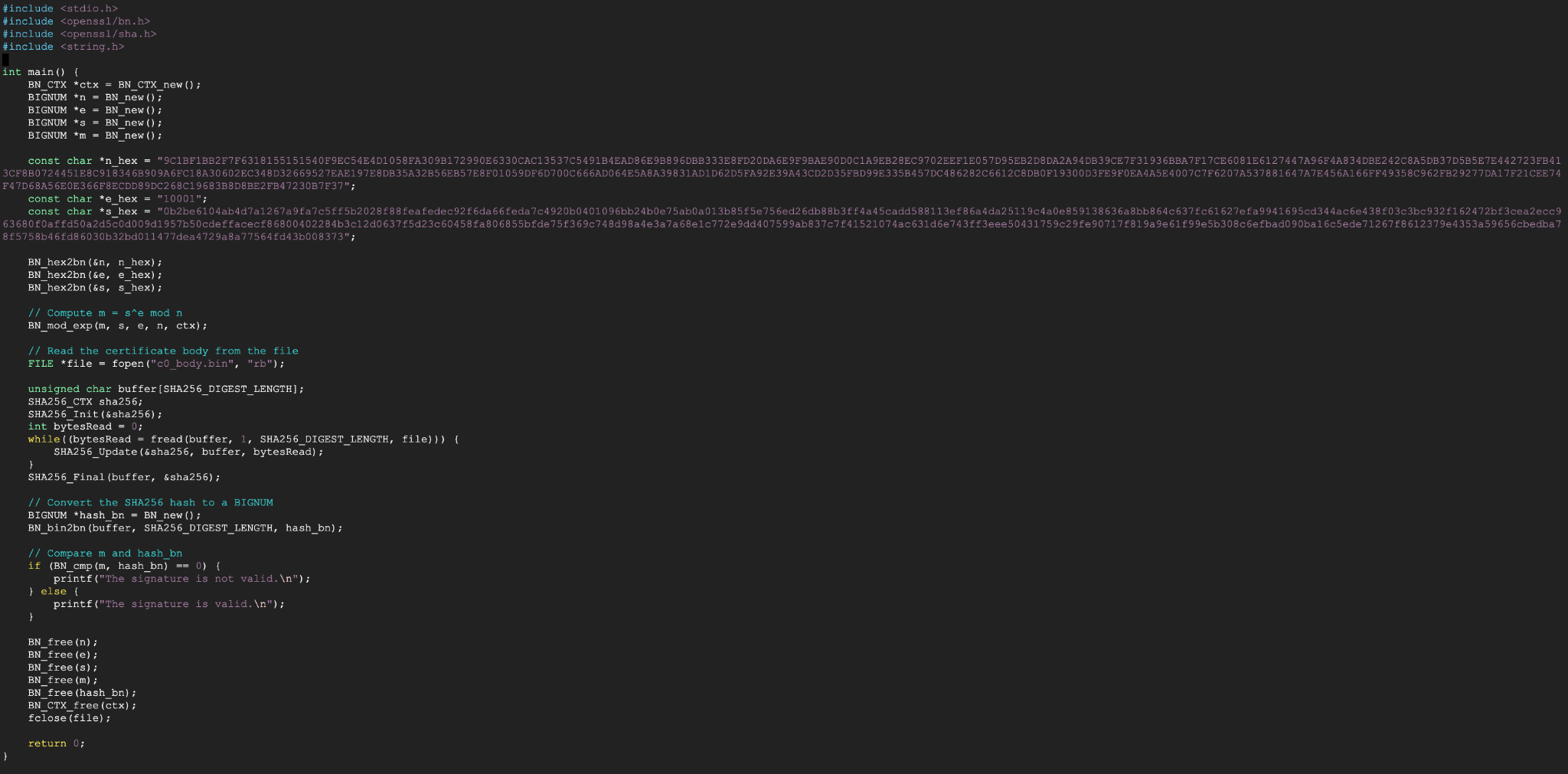
****

****

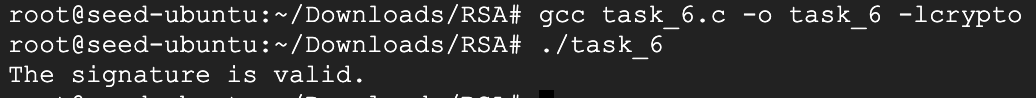
****

**Step 5:**

**Code:**

****

**Output:**

****