1. #1 Character's Uniqueness

   Question

   - Create a function to print the first occurrence from left to right

```python
def first_occurrence(string):
    unique_string = ""
    seen = set()
    for char in string:
        if char not in seen:
            unique_string += char
            seen.add(char)
    return unique_string
```

   - Create a function to print the first in lexicographical order

```python
def first_lexico(string):
    return
"".join(sorted(set(string)))
```

2. #2 System Design

   1. define additional features to make a proper system

Additional Features

1. Forgotten password recovery: Allows users to reset their password if they have forgotten it. This can be done by sending a password reset link to their email.
2. Two-factor authentication: An additional layer of security to ensure that the user logging in is actually the person they claim to be. This can be done via text message or an authenticator app.
3. Role-based access control: Assigns different levels of access to different users based on their role (e.g. admin, user).

4. Session management: Keeps track of user sessions and logs out users after a certain period of inactivity.
5. Audit logs: Keeps track of user activity, such as login attempts, password reset requests, and access to sensitive information.

2. create architecture document (ex: what component will be need, how they interacted each other, db design, constraint).

Architecture Document

1. User Authentication & Authorization service: This component will handle the core functionality of the system, including login, forgotten password recovery, and two-factor authentication.
2. Database: This component will store user information, such as email addresses, hashed passwords, and roles.
3. Role-based access control service: This component will interact with the User Authentication & Authorization service to determine a user's level of access based on their role.
4. Session management service: This component will interact with the User Authentication & Authorization service to keep track of user sessions and log out users after a certain period of inactivity.
5. Audit logs service: This component will interact with the User Authentication & Authorization service to keep track of user activity.
6. Google Authentication service: This component will handle the functionality of logging in via google credentials
7. Constraints:
   - Passwords will be hashed before being stored in the database
   - Two-factor authentication will be optional for users to enable
   - Email addresses will be unique and verified before allowing login
   - Role-based access control will be implemented to prevent unauthorized access to sensitive information.