

(1) 答案: 见下(2) 姓名: 于文明(3) 学号: 2011762(4) 专业: 信息安全

**1. 举例说明基于 ChatGPT 或其他大模型的应用你认为会有哪些问题?**

风险和责任问题、隐私和安全问题等

**2. 你认为为什么会有这样的问题?**

比如责任问题, 大型语言模型生成的内容可能包含错误、有害或有争议的信息。这可能导致不准确的答案或误导性的建议。再比如数据安全问题, 大型语言模型需要大量的数据进行训练, 这可能涉及用户的个人信息和敏感数据。在应用中使用这些模型需要确保数据的安全和隐私保护, 并采取措施防止恶意使用或数据泄露的风险。