YOUR LOGO

密码技术：保障网络安全的关键防线

2024

主讲人：郑冬贤

时间：2024

目录

YOUR LOGO

Part 01

密码学的基本概念及应用

密码学的定义与分支

密码学的定义

密码学是研究编制和破译密码的技术科学，包含编码学和分析学两个分支。

编码学负责设计加密算法，分析学专注于破解密码系统。

数据加密技术在网络安全中的应用

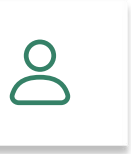
数据加密技术在网络安全中的应用极为广泛。在网络通信中，无论是个人用户通过浏览器访问网站，还是企业之间进行数据传输，加密技术都能确保信息的保密性。例如，我们在网上购物时，输入的银行卡信息、个人地址等敏感数据会通过加密算法转化为密文后传输，防止被黑客在网络传输过程中窃取。在企业层面，商业机密、客户资料等重要数据的存储和传输都依赖加密技术，避免因数据泄露导致的巨额经济损失和声誉损害。对于政府机构和军事领域，加密更是关乎国家安全，确保情报、指令等信息的安全传递，防止敌对势力的窥探和破坏。

加密技术确保信息保密性

加密技术在网络通信中确保信息的保密性，如网上购物时银行卡信息的加密传输。

企业数据传输依赖加密技术，防止数据泄露导致的经济损失和声誉损害。

加密技术在政府和军事领域的应用



01

加密技术关乎国家安全

对政府和军事领域而言，加密技术确保情报和指令的安全传递，防止敌对势力的窥探。

YOUR LOGO

Part 02

数据加密、传送及解密过程

加密算法的选择与应用

对称加密算法的应用

对称加密算法使用相同的密钥进行加密和解密，适用于大量数据的快速加密。

企业内部文档加密保护常采用对称加密算法，通过共享密钥确保数据安全。

非对称加密算法的应用

非对称加密算法使用公钥加密和私钥解密，常用于数字签名和密钥交换。

网上银行交易中，用户使用银行公钥加密交易信息，保障交易的安全性。

数据的安全传送

使用安全的传输协议

HTTPS等安全传输协议在传输层对数据进行加密，防止数据被篡改或窃取。

数据解密与密钥管理

在数据传送阶段，加密后的数据通过网络进行传输。为了进一步确保数据的完整性和保密性，还会采用一些其他的安全措施，如使用安全的传输协议（如 HTTPS 协议），它在传输层对数据进行加密，防止数据在传输过程中被篡改或窃取。
数据解密是加密的逆过程。接收方使用相应的密钥（对称加密的共享密钥或非对称加密的私钥）对收到的密文进行解密，还原出原始的明文信息。对于一些复杂的加密系统，还可能涉及到密钥管理机制，确保密钥的安全生成、存储、分发和更新，因为密钥一旦泄露，整个加密体系将面临被破解的风险。

数据解密过程

接收方使用相应的密钥对收到的密文进行解密，还原出原始的明文信息。

密钥管理机制

密钥管理机制确保密钥的安全生成、存储、分发和更新，防止密钥泄露导致的风险。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024