**Chapter 8 计算机网络中的安全**

**DES**：Data Encryption Standard 数据加密标准

**AES**：Advanced Encryption Standard 高级加密标准

**CBC**：Cipher Block Chaining 密码块链接

**IV**：Initialization Vector 初始向量

**RSA**：RSA Algorithm 取算法创立人名的首字母

**MAC**：Message Authentication Code 报文鉴别码

**CA**：Certification Authority 认证中心

**PGP**：Pretty Good Privacy 一种电子邮件加密方案

**SSL**：Secure Socket Layer 安全套接字层

**TLS**：Transport Layer Secure 运输层安全性

**MS**：Master Key 主密钥

**EMS**：Encrypted Master Key 加密主密钥

**AH**：Authentication Header 鉴别首部协议

**ESP**：Encapsulation Security Payload 封装安全性载荷协议

**SA：**Security Association 安全关联

**SPI**：Security Parameter Index 安全参数索引

**SAD**：Security Association Database 安全关联数据库

**SPD**：Security Policy Database 安全策略库

**IKE**：Internet Key Exchange 因特网密钥交换

**WEP**：Wired Equivalent Privacy 有线等效保密

**EAP**：Extensible Authentication Protocol 可扩展鉴别协议

**PMK**：Pairwise Master Key 成对主密钥

**TK**：Temporal Key 临时密钥