1. IPsec协议的基本信息

基本概念：IPSec是IPv6的一个组成部分，是IPv4的一个可选扩展协议。IPSec弥补了IPv4在协议设计时缺乏安全性考虑的不足。IPSec定义了一种标准的、健壮的以及包容广泛的机制，可用它为IP以及上层协议（比如TCP或者UDP）提供安全保证。

目标：为IPv4和IPv6提供具有较强的互操作能力、高质量和基于密码的安全功能，在IP层实现多种安全服务，包括访问控制、数据完整性、机密性等。

利用的技术：IPSec通过支持一系列加密算法如DES、三重DES、IDEA和AES等确保通信双方的机密性。

2.IPsec协议包含的模式和具体协议

#认证头标AH和封装安全净载ESP两种安全协议

#传输模式用在主机到主机的通信，隧道模式用在其它任何方式的通信。

