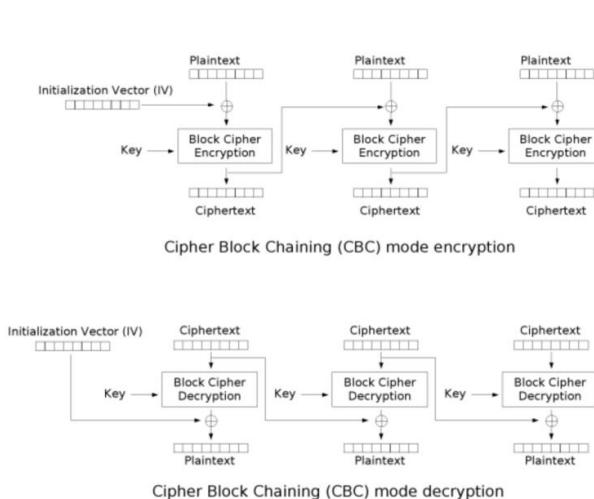


# 密码学概述

- 密码学（Cryptography）其中，古典密码学，作为一种实用性艺术存在，其编码和破译通常依赖于设计者和敌手的创造力与技巧，并没有对密码学原件进行清晰的定义。古典密码学主要包含以下几个方面：
  - 单表替换加密（Monoalphabetic Cipher）
  - 多表替换加密（Polyalphabetic Cipher）
  - 非对称加密（Asymmetric Cryptography），以 RSA, ElGamal, 椭圆曲线加密为代表。
  - 哈希函数（Hash Function），以 MD5, SHA-1, SHA-512 等为代表。
  - 数字签名（Digital Signature），以 RSA 签名, ElGamal 签名, DSA 签名为代表。
  - 对称加密体制主要分为两种方式：分组密码（Block Cipher）、序列密码（Stream Cipher）
  - 密码设计者的根本目标是保障信息及信息系统的：机密性（Confidentiality）完整性（Integrity）可用性（Availability）认证性（Authentication）不可否认性（Non-repudiation）其中，前三者被称为信息安全的 CIA 三要素。
  - 而对于密码破解者来说，一般是要想办法识别出密码算法，然后进行暴力破解，或者利用密码体制的漏洞进行破解。当然，也有可能通过构造虚假的哈希值或者数字签名来绕过相应的检测。
  - 一般来说，我们都会假设攻击者已知待破解的密码体制，而攻击类型通常分为以下四种：

攻击类型	说明
唯密文攻击	只拥有密文
已知明文攻击	拥有密文与对应的明文
选择明文攻击	拥有加密权限，能够对明文加密后获得相应密文
选择密文攻击	拥有解密权限，能够对密文解密后获得相应明文

## 对称加密——分组密码（CBC）



在 CBC 模式中，每个明文块先与前一个密文块进行异或后，再进行加密。在这种方法中，每个密文块都依赖于它前面的所有明文块。同时，为了保证每条消息的唯一性，在第一个块中需要使用初始化向量。

优点：  
加密结果与前文相关，有利于提高加密结果的随机性。  
可并行解密。1.不容易主动攻击,安全性好于ECB,适合传输长度长的报文,是SSL、IPSec的标准

缺点  
无法并行加密。  
一个分组损坏，如果密文长度不变，则两个分组受影响。如果密文长度改变，则后面所有分组受影响。

# Session Key

session key（会话密钥），是保证用户跟其它计算机或者两台计算机之间安全通信会话而随机产生的加密和解密密钥。会话密钥有时称对称密钥，因为同一密钥用于加密和解密。在此连接结束该密钥即无效，如需重新通信则需要再重新进行一次密钥的产生及交换等步骤。

会话密钥可使用CryptDeriveKey函数从杂乱信号数值中导出（这一方法称会话密钥推导方案）。贯穿各个会话始终，这个密钥与各个消息一起传输，并使用接收者的公共密钥加密。由于其大部分安全性依赖于其使用时间的短暂性，会话密钥常常频繁更改。各个消息可能使用不同的会话密钥

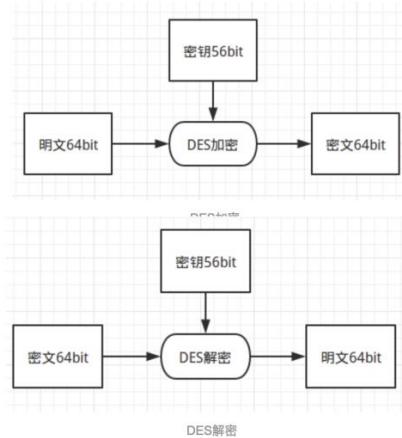
A **session key** is a single-use [symmetric key](#) used for [encrypting](#) all [messages](#) in one [communication session](#). A closely related term is **content encryption key(CEK)**, **traffic encryption key (TEK)**, or **multicast key** which refers to any key used to encrypt messages, as opposed to other uses, like encrypting other keys (**key encryption key (KEK)** or **key wrapping key**).

Session keys can introduce complication into a system. Two primary reasons to use session keys:

Several cryptanalytic attacks become easier as more material encrypted with a specific key is available. By limiting the amount of data processed using a particular key, those attacks are made more difficult.

[asymmetric encryption](#) is too slow for many purposes, and all [secret key algorithms](#) require that the key is securely distributed. By using an asymmetric algorithm to encrypt the secret key for another, faster, symmetric algorithm, it's possible to improve overall performance considerably. This is the process used by [PGP](#) [GPG](#).<sup>[1]</sup> Like all [cryptographic keys](#), session keys must be chosen so that they cannot be predicted by an attacker, usually requiring them to be chosen randomly. Failure to choose session keys (or any key) properly is a major (and too common in actual practice) design flaw in any crypto system.

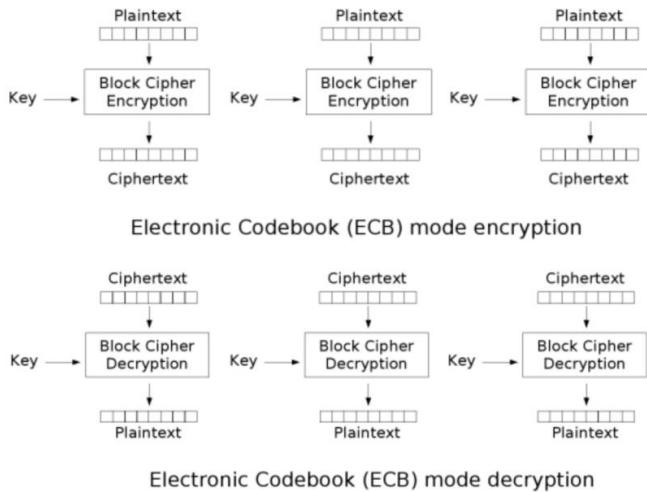
## 对称加密——分组密码（DES）



**密钥：**DES是一种将64bit的明文加密成64bit的密文的对称密码算法，它的密钥长度是64bit（每隔7bit会设置一个用于错误检查的bit，因此实际使用密钥长度56bit）

**分组：**DES是以64bit的明文作为一个单位来进行加密的，这64bit的单位称为**分组**。一般来说，以分组为单位进行处理的密码算法称为**分组密码 (block cipher)**，DES就是分组密码中的一种。DES每次只能加密64比特的数据，如果要加密的明文比较长，就需要对DES加密进行迭代。

## 对称加密——分组密码 (ECB)



最简单的加密模式：需要加密的消息按照块密码的块大小被分为数个块，并对每个块进行独立加密。

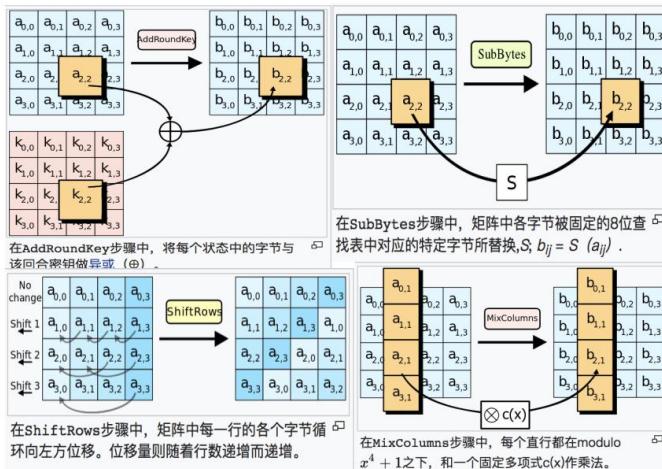
优点：

- 1.简单；
- 2.有利于并行计算；
- 3.误差不会被传送；

缺点：

- 1.不能隐藏明文的模式；
  - 2.可能对明文进行主动攻击；
- ECB模式也会导致使用它的协议不能提供数据完整性保护，易受到重放攻击的影响，因此每个块是以完全相同的方式解密的。

## 对称加密——分组密码 (AES)



AES加密过程是在一个4×4的字节矩阵上运作，这个矩阵又称为“体（state）”，其初值就是一个明文区块

AddRoundKey—矩阵中的每一个字节都与该次回合密钥（round key）做XOR运算；每个子密钥由密钥生成方案产生。

SubBytes—通过一个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节。

ShiftRows—将矩阵中的每个横列进行循环式移位。

MixColumns—为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每内联的四个字节。最后一个加密循环中省略MixColumns步骤，而以另一个AddRoundKey取代。

\* 这个标准用来替代原先的DES

## 对称加密——数据流加密

加密和解密双方使用相同伪随机加密数据流（pseudo-random stream）作为密钥，明文数据每次与密钥数据流顺次对应加密，得到密文数据流。实践中数据通常是一个位（bit）并用异或（xor）操作加密。该算法解决了对称加密完善保密性（perfect secrecy）的实际操作困难。由于完善保密性要求密钥长度不短于明文长度，故而实际操作存在困难，改由较短数据流通过特定算法得到密钥流。

伪随机密钥流（keystream）由一个随机的种子（seed）通过算法（称为：PRG, pseudo-random generator）得到，k作为种子，则G（k）作为实际使用的密钥进行加密解密工作。

为了保证流加密的安全性，PRG必须是不可预测的。弱算法包括glibc random()函数，线性同余生成器（linear congruential generator）等。

线性同余生成器中，令r[0]为seed，r[i] = (a \* r[i-1] + b) mod p，其中a, b, p均为常数，则可轻易顺次推出整个密钥流，从而进行解密。

# PSK (共享秘钥)

PSK是预共享密钥，是用于验证 L2TP/IPSec 连接的 Unicode 字符串。可以配置“路由和远程访问”来验证支持预共享密钥的 VPN 连接。

预共享密钥模式（pre-shared key, PSK，又称为个人模式）是设计给负担不起 802.1X 验证服务器的成本和复杂度的家庭和小型公司网络用的，每一个使用者必须输入密语来取用网络，而密语可以是 8 到 63 个 ASCII 字符，或是 64 个 16 位数字（256 位元）。使用者可以自行斟酌要不要把密语存在电脑里以省去重复键入的麻烦，但密语一定要存在 Wi-Fi 取用点里。

安全性是利用密钥导出函数来增强的，然而使用者采用的典型的弱密语会被密码破解攻击。WPA 和 WPA2 可以用至少 5 个 Diceware 词或是 14 个完全随机字母当密语来击败密码破解攻击，不过若是想要有最大强度的话，应该采用 8 个 Diceware 词或 22 个随机字母。密语应该要定期更换，在有人使用网络的权利被撤消、或是设定好要使用网络的装置遗失或被攻破时，也要立刻更换。

WPA-PSK 加密方式尚有一漏洞，攻击者可利用 spoonwpa 等工具，搜索到合法用户的网卡地址，并伪装该地址对路由器进行攻击，迫使合法用户掉线重新连接，在此过程中获得一个有效的握手包，并对握手包批量猜密码，如果猜密的字典中有合法用户设置的密码，即可被破解。建议用户在加密时尽可能使用无规律的字母与数字，以提高网络的安全性。

## PSK (共享秘钥) 优缺点

+

PSK 验证不需要在公钥结构 (PKI) 方面上进行硬件投资与配置，只在使用计算机证书进行 L2TP/IPSec 验证时需要用到它。在远程访问服务器上配置预共享密钥很简单，在远程访问客户端上配置它也相对容易。如果预共享密钥是以放在“连接管理器”配置文件内的方式发行，则对用户可以是透明的。如果您要建立 PKI 或者在管理 Active Directory 域，则可以配置“路由和远程访问”以接受使用计算机证书或预共享密钥的 L2TP/IPSec 连接。

-

PSK 是在远程访问服务器和 L2TP/IPSec 客户端上都要配置的字符序列。PSK 可以是至多 256 个 Unicode 字符任意组合的任意非空字符串。当选择 PSK 时，请考虑到使用“新建连接”向导创建 VPN 客户端连接的用户必须手动键入预共享密钥。为提供足够的安全性，密钥通常很长也很复杂，这对大部分用户来说很难准确地键入。如果 VPN 客户端出现的 PSK 与远程访问服务器上配置的预共享密钥有任何不同，客户端身份验证将失败。

使用预共享密钥验证 L2TP/IPSec 连接被认为是一种安全性相对较差的身份验证方法。如果需要一种长期、可靠的身份验证方法，则应考虑使用 PKI。

802.1X 认证技术是针对于无线客户端需要接入网络时的准入认证技术，一般通过输入账户密码，向 radius 认证服务器发起准入请求，认证通过就可以正常接入网络访问指定的网络资源，认证失败的话就不能接入网络。

这个认证技术的关键协议是 EAP，需要知道客户端和中间网络设备以及认证服务器之间经历了哪些交互过程。客户端参与那些过程，中间网络设备参与哪些过程，认证服务器参与哪些过程。

基于 802.1x 的认证系统在客户端和认证系统之间使用 EAPOL 格式封装 EAP 协议传送认证信息，认证系统与认证服务器之间通过 RADIUS 协议传送认证信息。由于 EAP 协议的可扩展性，基于 EAP 协议的认证系统可以使用多种不同的认证算法，如 EAP-MD5, EAP-TLS, EAP-SIM, EAP-TTLS 以及 EAP-AKA 等认证方法。

认证通过之后的保持：认证端 Authenticator 可以定时要求 Client 重新认证，时间可设。

重新认证的过程对 User 是透明的(应该是 User 不需要重新输入密码)。

下线方式：物理端口 Down；重新认证不通过或者超时；客户端发起 EAP\_Logoff 帧；

网管控制导致下线；

现在的设备（switch）端口有三种认证方式：

- (1) ForceAuthorized：端口一直维持授权状态，switch 的 Authenticator 不主动发起认证；
- (2) ForceUnauthorized：端口一直维持非授权状态，忽略所有客户端发起的认证请求；
- (3) Auto：激活 802.1X，设置端口为非授权状态，同时通知设备管理模块要求进行端口认证控制，使端口仅允许 EAPOL 报文收发，当发生 UP 事件或接收到 EAPOL-start 报文，开始认证流程，请求客户端 identify，并中继客户和认证服务器间的报文。认证通过后端口切换到授权状态，在退出前可以进行重认证。

802.1x 协议的认证端口

受控端口：在通过认证前，只允许认证报文 EAPOL 报文和广播报文（DHCP、ARP）

通过端口，不允许任何其他业务数据流通过；

逻辑受控端口：多个 Supplicant 共用一个物理端口，当某个 Supplicant 没有通过认证前，

只允许认证报文通过该物理端口，不允许业务数据，但其他已通过认证的 Supplicant 业务不受影响。

## 802.1X认证

现在的设备（switch）端口有三种认证方式：

- (1) ForceAuthorized：端口一直维持授权状态，switch的Authenticator不主动发起认证；
- (2) ForceUnauthorized：端口一直维持非授权状态，忽略所有客户端发起的认证请求；
- (3) Auto：激活802.1X设置端口为非授权状态，同时通知设备管理模块要求进行端口认证控制，使端口仅允许EAPOL报文收发，当发生UP事件或接收到EAPOL-start报文，开始认证流程，请求客户Identify并中继客户和认证服务器间的报文。认证通过后端口切换到授权状态，在退出前可以进行重认证。

802.1x协议的认证端口

受控端口：在通过认证前，只允许认证报文EAPOL报文和广播报文（DHCP、ARP）通过端口，不允许任何其他业务数据流通过；

逻辑受控端口：多个Supplicant共用一个物理端口，当某个Supplicant没有通过认证前，

只允许认证报文通过该物理端口，不允许业务数据，但其他已通过认证的Supplicant业务不受影响。

现在在使用中有下面三种情况：

- (1)仅对使用同一物理端口的任何一个用户进行认证（仅对一个用户进行认证，认证过程中忽略其他用户的认证请求），认证通过后其他用户也可以利用该物理端口访问网络服务。
- (2)对共用同一个物理端口的多个用户分别进行认证控制，限制同时使用同一个物理端口的用户数目（限制MAC地址数目），但不指定MAC地址，让系统根据先到先得原则进行MAC地址学习，系统将拒绝超过限制数目的请求，若有用户退出，则可以覆盖已退出的MAC地址。
- (3)对利用不同物理端口的用户进行VLAN认证控制，即只允许访问指定VLAN，限制用户访问非授权VLAN；用户可以利用受控端口，访问指定VLAN，同一用户可以在不同的端口访问相同的VLAN。

## 802.1X的wpa认证流程——4way handshake

WPA系统在工作的时候，先由AP向外公布自身对WPA的支持，在Beacons、Probe Response等报文中使用新定义的WPA信息元素（Information Element），这些信息元素中包含了AP的安全配置信息（包括加密算法和安全配置等信息）。STA根据收到的信息选择相应的安全配置，并将所选择的安全配置表示在其发出的Association Request和Re-Association Request报文中。WPA通过这种方式来实现STA与AP之间的加密算法以及密钥管理方式的协商。

支持WPA的AP工作需要在开放系统认证方式下，STA以WPA模式与AP建立关联之后，如果网络中有RADIUS服务器作为认证服务器，那么STA就使用802.1x方式进行认证；如果网络中没有RADIUS，STA与AP就会采用预共享密钥（PSK，Pre-Shared Key）的方式。

STA通过了802.1x身份验证之后，AP会得到一个与STA相同的Session Key，AP与STA将该Session Key作为PMK（Pairwise Master Key，对于使用预共享密钥的方式来说，PSK就是PMK）。随后AP与STA通过EAPOL-KEY进行WPA的四次握手（4-Way Handshake）过程，如图所示。

在这个过程中，AP和STA均确认了对方是否持有与自己一致的PMK，如不一致，四次握手过程就告失败。为了保证传输的完整性，在握手过程中使用了名为MIC（Message Integrity Code）的检验码。在四次握手的过程中，AP与STA经过协商计算出一个512位的PTK（Pairwise Transient Key），并将该PTK分解成为五种不同用途的密钥，如图所示：

## IPsec (IP Security)

### 概述

在实施VPN时，除了实现隧道功能以外，还要实现数据安全，两者缺一不可；在隧道方面，之前所讲到的GRE就是最常用的隧道技术，而在数据安全方面，其实就是要让数据加密传输，至于如何对数据进行加密传输，有一个使用最广泛，且最经典的技术方案，这就是IPsec (IP Security)，IPsec最突出，也是最主要的功能就是保证VPN数据的安全传输。

IPsec定义了使用什么样的方法来管理相互之间的认证，以及使用什么样的方法来保护数据，IPsec只是定义了一些方法，而IPsec本身并不是一个协议，就像OSI (Open System Interconnect) 参考模型一样，OSI并不是一个协议，OSI只是一个框架，一个模型，OSI里面包含着多个协议，如TCP, UDP, IP, ICMP等等；IPsec中同样也包含着为之服务的各种协议去实现IPsec要完成的各个功能，只有这样，IPsec才能起到作用。

为IPsec服务的有三个协议：IKE (Internet Key Exchange) ESP (Encapsulating Security Protocol) AH (Authentication Header)  
虽然总共是三个协议，但分为两类：

IKE是个混合协议，其中包含部分Oakley协议以及内置在ISAKMP (Internet Security Association and Key Management Protocol)协议中的部分SKEME协议，所以IKE也可写为ISAKMP/Oakley，它是针对密钥安全的，是用来保证密钥的安全传输、交换以及存储，主要是对密钥进行操作，并不对用户的实际数据进行操作。

ESP (Encapsulating Security Protocol) 和AH (Authentication Header) 主要工作是如何保护数据安全，也就是如何加密数据，是直接对用户数据进行操作的。

因为在实施VPN时，除了实现隧道功能以外，还要实现数据安全，两者缺一不可；在之前我提到的隧道技术中，只能实现隧道而不能实现安全，而IPSec则可以为隧道提供数据保护功能，从而构建一个完整的VPN体系。IPsec除了能够为隧道提供数据保护来实现VPN之外，IPsec还可以自己单独作为隧道协议来提供隧道的建立，如果IPsec自己单独作为隧道协议来使用，那么IPsec就不需要借助任何其它隧道协议就能独立实现VPN功能；IPsec到底是只使用数据保护功能再配合其它隧道协议，还是自己独立实现隧道来完成VPN功能，可以由配置者自己决定。

## IKE (Internet Key Exchange)

由于公钥加密算法的速度明显慢于私钥加密算法，IPsec在保护数据时选择了使用私钥加密算法，而使用私钥加密算法的重点就是要保证密钥的安全传递与交换，所以如何保证密钥的安全，成了头等工作；之前我们曾说过使用公钥加密算法来保证私钥算法的密钥安全传递与交换，但是事情并非想象的那么简单，即使使用公钥加密算法来保证密钥的安全交换，仍然存在以下问题：

### 认证 (Authentication)

IKE会在VPN对等体之间采用认证机制 (Authentication)，认证可以有效确保会话是来自于真正的对等体而不是攻击者，因为如果最开始本身就是在一个攻击者或黑客进行会话和协商，那么后面的所有工作都是白废，所以保证只和合法的对等体会话是非常重要的；IKE的认证方式有三种：

#### Pre-Shared Keys (PSK)

#### Public Key Infrastructure (PKI) using X.509 Digital Certificates

#### RSA encrypted nonce

其中Pre-Shared Keys (PSK)是最简单的，使用由管理员事先在双方定义好的密码，认证时，只有双方密码匹配之后，后续的工作才能继续；配置时通常可以包含IP地址，子网以及掩码，也可以指定为任意地址来代替固定地址，适用于IP地址不固定的环境。

PKI是使用第三方证书做认证，叫做Certificate Authority (CA)，里面包含名字、序列号，有效期以及其它可以用来确认身份的参数；证书也可以被取消。

#### 注：

★ RSA encrypted nonce我们不做介绍，包括在后续配置与示例中，我们只涉及Pre-Shared Keys (PSK)。

## A (Security Association)

IPsec的所有会话都是在通道中传输的，包括协商密钥，传递用户数据；这样的通道称为SA（Security Association），SA并不是隧道，而是一组规则，就好比是需要会话的对等体之间必须遵守的一份合同。SA中的规则能够保证所有数据的安全传递，因此SA中包含了之前提到的保证数据和密钥安全时必不可少的认证、加密等安全策略，这些需要用到的技术，都要在SA中定义。

因为VPN之间传输的数据需要加密才能保证安全，并且加密时所用到的密钥要更加安全，所以对待密钥，我们也要付出巨大的努力。在密钥的安全上，由IKE负责，而数据的安全，则由IPsec负责，虽然是这么说，但需要注意，IKE也是IPsec不可分割的一部分，IKE不是独立存在的。

SA并不是只有一个，由于密钥安全和数据安全我们是分开对待的，所以SA有两个，分别是定义了如何保护密钥和如何保护数据，这两个SA就是：

### ISAKMP Security Association (IKE SA)

### IPsec Security Association (IPsec SA)

每个SA都有lifetime，过期后SA便无效，lifetime使用time (second) 和volume limit (byte count)来衡量，在建立SA时就会协商出来，双方会比对，最终取值小的一方；通常是时间先过期，在要过期最后120秒之前，会自动重建另一条SA，避免活动的SA到期后无法传输数据，这样就能实现平滑过渡，以丢最少的包。

## 一、SSL协议的握手过程

第一步，爱丽丝给出协议版本号、一个客户端生成的随机数（Client random），以及客户端支持的加密方法。

第二步，鲍勃确认双方使用的加密方法，并给出数字证书、以及一个服务器生成的随机数（Server random）。

第三步，爱丽丝确认数字证书有效，然后生成一个新的随机数（Premastersecret），并使用数字证书中的公钥，加密这个随机数，发给鲍勃。

第四步，鲍勃使用自己的私钥，获取爱丽丝发来的随机数（即Premaster secret）。

第五步，爱丽丝和鲍勃根据约定的加密方法，使用前面的三个随机数，生成“对话密钥”（session key），用来加密接下来的整个对话过程。

## 二、私钥的作用

握手阶段有三点需要注意。

(1) 生成对话密钥一共需要三个随机数。

(2) 握手之后的对话使用“对话密钥”加密（对称加密），服务器的公钥和私钥只用于加密和解密“对话密钥”（非对称加密），无其他作用。

(3) 服务器公钥放在服务器的数字证书之中。

从上面第二点可知，整个对话过程中（握手阶段和其后的对话），服务器的公钥和私钥只需要用到一次。这就是CloudFlare能够提供Keyless服务的根本原因。

某些客户（比如银行）想要使用外部CDN，加快自家网站的访问速度，但是出于安全考虑，不能把私钥交给CDN服务商。这时，完全可以把私钥留在自家服务器，只用来解密对话密钥，其他步骤都让CDN服务商去完成。

上图中，银行的服务器只参与第四步，后面的对话都不再会用到私钥了。

## 三、DH算法的握手阶段

整个握手阶段都不加密（也没法加密），都是明文的。因此，如果有人窃听通信，他可以知道双方选择的加密方法，以及三个随机数中的两个。整个通话的安全，只取决于第三个随机数（Premaster secret）能不能被破解。

虽然理论上，只要服务器的公钥足够长（比如2048位），那么Premaster secret可以保证不被破解。但是为了足够安全，我们可以考虑把握手阶段的算法从默认的RSA算法，改为Diffie-Hellman算法（简称DH算法）。

采用DH算法后，Premaster secret不需要传递，双方只要交换各自的参数，就可以算出这个随机数。

## 四、session的恢复

握手阶段用来建立SSL连接。如果出于某种原因，对话中断，就需要重新握手。

这时有两种方法可以恢复原来的session：一种叫做session ID，另一种叫做session ticket。

session ID的思想很简单，就是每一次对话都有一个编号（session ID）。如果对话中断，下次重连的时候，只要客户端给出这个编号，且服务器有这个编号的记录，双方就可以重新使用已有的“对话密钥”，而不必重新生成一把。

上图中，客户端给出session ID，服务器确认该编号存在，双方就不再进行握手阶段剩余的步骤，而直接用已有的对话密钥进行加密通信。

session ID是目前所有浏览器都支持的方法，但是它的缺点在于session ID往往只保留在一台服务器上。所以，如果客户端的请求发到另一台服务器，就无法恢复对话。session ticket就是为了解决这个问题而诞生的，目前只有Firefox和Chrome浏览器支持。

上图中，客户端不再发送session ID，而是发送一个服务器在上一次对话中发送过来的session ticket。这个session ticket是加密的，只有服务器才能解密，其中包括本次对话的主要信息，比如对话密钥和加密方法。当服务器收到session ticket以后，解密后就不必重新生成对话密钥了。

## 4way handshake

其中前128位用做计算和检验EAPOL-KEY报文的MIC的密钥，随后的128位作为加密EAPOL-KEY的密钥;接下来的128位作为AP与该STA之间通信的加密密钥的基础密钥（即由该密钥再经过一定的计算后得出的密钥作为二者之间的密钥）;最后两个64位的密钥分别作为AP与该STA之间的报文的MIC计算和检验密钥。

由PTK分解出来的这一组（五个）密钥是AP与该STA之间使用的密钥（所以也叫每用户密钥，用于AP与STA之间的单播报文的加密），这些密钥永远也不会以任何形式出现在无线网络上。在确认双方所持的PMK一致后，AP会根据自身是否支持每用户密钥的能力来指示STA是否安装并使用这个每用户密钥。

为了使现有的设备能够通过软件/固件升级实现WPA，协议规定AP可以不采用PTK方式，而是利用下面将要描述的GTK作为AP向STA发送单播报文时的密钥。如果AP通知STA安装并使用PTK，那么STA在向AP发送一个EAPOL-KEY相应报文后，再把相应的密钥安装到无线网卡中。

四次握手成功后，AP要生成一个256位的GTK（Group Transient Key），GTK是一组全局加密密钥，所有与该AP建立关联的STA均使用相同的GTK，AP用这个GTK来加密所有与它建立关联的STA的通信报文，STA则使用这个GTK来解密由AP发送的报文并检验其MIC。该密钥可以分解为三种不同用途的密钥，最前面的128位作为构造全局“每报文密钥”（Per-packet Encryption Key）的基础密钥（Base Key），后面的两个64位的密钥分别作为计算和检验WPA数据报文的MIC的密钥。AP使用EAPOL-KEY加密密钥将GTK加密并发送给STA，并指明该GTK是否允许STA用作发送报文所使用，STA成功接收到该报文，将GTK解密后，向AP发送应答报文，并根据AP所指示的Key Index将其安装无线网卡的相应位置，如果AP使用GTK作为向某一STA单播传输的密钥，则该STA也需要使用GTK作为向AP发送单播报文的密钥。

TKIP并不直接使用由PTK/GTK分解出来的密钥作为加密报文的密钥，而是将该密钥作为基础密钥（Base Key），经过两个阶段的密钥混合过程，从而生成一个新的每一次报文传输都不一样的密钥，该密钥才是用做直接加密的密钥。通过这种方式可以进一步增强WLAN的安全性。密钥的生成方式如图所示：

在WPA中，AP支持WPA和WEP无线客户端的混合接入。在STA与AP建立关联时，AP可以根据STA的Association Request中是否带有WPA信息元素来确定哪些客户端支持使用WPA。但是在混合接入的时候，所有WPA客户端所使用的加密算法都得使用WEP，这就降低了无线局域网的整体安全性。

WLAN-RSN 这节PPT说的其实还是上面802.1X认证的事情，只不过这一节是站在无线网络安全的整体角度去概况当前要建立一个RSN（健壮安全的网络）有哪些技术可以实现，然后又落实到802.1X，因为PPT中说到了WEP,WPA等希望以，这些协议前面PPT有提到，但是他们都是无线传输过程中的数据加密协议，他们保证了无线数据在传递过程中的安全，而802.1X技术是保证了无线客户端接入到网络中的安全技术，保证网络中接入的客户端都是授权合法的。重点说的还是802.1X这个协议，所以这页PPT可以结合前面的WLAN-802.1X-Authentication PPT一起看，最好是先把我给你的这2个链接看完，再去看PPT

Bluetooth 和broadcast这2节可以并到一起看，因为当你看了Bluetooth的资料后你会发现Bluetooth通信基本上靠的就是broadcast。这里比较耗时间的就是你要多看Bluetooth的基础概念介绍，

先看这个<https://baike.baidu.com/item/%E5%BE%AE%E5%BE%AE%E7%BD%91%E6%8A%80%E6%9C%AF/17044035>和[https://wenku.baidu.com/view/15e4fb01f90f76c660371a26.html?rec\\_flag=default&sxts=1529258599757](https://wenku.baidu.com/view/15e4fb01f90f76c660371a26.html?rec_flag=default&sxts=1529258599757)

介绍的是蓝牙网络连接的基本架构。然后看看蓝牙经历了很多版本的更新他们之间有什么区别重点关注做了哪些改进[https://blog.csdn.net/xushx\\_bigbear/article/details/49303827](https://blog.csdn.net/xushx_bigbear/article/details/49303827)，这里多关注4.0的版本4.0版本的蓝牙也就是文中提到的低功耗BLE(Bluetooth low energy)这个讲的比较多。

之后再看看蓝牙当前已有的安全特性[https://blog.csdn.net/wendell\\_gong/article/details/49741223](https://blog.csdn.net/wendell_gong/article/details/49741223)有哪些，主要是认证/机密性/授权这三大机制，他们分别使用哪些技术点。

最后看看各个版本存在的漏洞风险和应对措施[https://blog.csdn.net/wendell\\_gong/article/details/50208215](https://blog.csdn.net/wendell_gong/article/details/50208215)也是重点看4.0版本

Broadcast security 这一节涉及到一个非常重要的算法ECDH和ECDSA <https://www.cnblogs.com/fishou/p/4206451.html>  
<https://blog.csdn.net/mrpre/article/details/72850644>

When an initialization vector is used as an input in the encryption process, it must always be a secret.

Select one:

- a. True
- b. False ✓

When an initialization vector is used as an input in the encryption process, it must always be a secret.

Select one:

- a. True
- b. False ✓

When an initialization vector is used as an input in the encryption process, it must always be a secret.

Select one:

- a. True
- b. False ✓

The initialization vector (IV) appended to the secret symmetric key in WEP protocol is encrypted before sending to the receiver.

Select one:

- a. False
- b. True ✗

The initialization vector (IV) appended to the secret symmetric key in WEP protocol is encrypted before sending to the receiver.

Select one:

- a. False
- b. True ✗

SSL/TLS uses two protocols. It first uses the record protocol and then the handshake protocol.

Select one:

- a. False ✓
- b. True

If an individual signs a message with his private key, this act carries with it non-repudiation.

Select one:

- a. False
- b. True ✓

RC4 is a \_\_\_\_\_.

Select one:

- a. Block cipher ✗
- b. None of the above
- c. Stream cipher

The correct answer is: Stream cipher

If a hash function produces a full-length hash value of 512 bits, then the collision resistance is approximately:

Select one:

- a. 256 bits
- b. 128 bits
- c. 512 bits
- d. 1024 bits ✗

The correct answer is: 256 bits

In Diffie-Hellman key exchange protocol if the private key of Alice and Bob are,  $a = 6$  and  $b = 15$  resp. and  $g = 5$  and  $p = 23$ , then the public key of Alice (A) and Bob (B) and shared secret key are:

Select one:

- a. A= 2, B = 18, S=5
- b. A= 18, B = 2, S=5
- c. A= 19, B = 8, S=2 ✗
- d. A= 8, B = 19, S=2

The correct answer is: A= 8, B = 19, S=2

The use of public key cryptography is much faster than the use of symmetric key cryptography.

Select one:

- a. False ✓
- b. True

The digital signature of a message is

Select one:

- a. The hash of the message encrypted with a shared key between the sender and receiver
- b. The hash of the message
- c. The hash of the message encrypted with the public key of the receiver
- d. The hash of the message encrypted with the private key of the sender ✓

Which of the following is true regarding WEP cracking?

Select one:

- a. Initialization vectors are small, get reused frequently, but are encrypted during transmission.
- b. Initialization vectors are small, get reused frequently, and are sent in clear text. ✓
- c. Initialization vectors are large, get reused frequently, and are sent in clear text.

A message digest can be inverted to obtain the original message.

Select one:

- a. False
- b. True ✗

Diffie-Hellman and the Digital Signature Algorithm are used to encrypt in SSL applications.

Select one:

- a. False ✓
- b. True

In SSL record, there is a field called sequence number that is to protect a session from replay attack.

Select one:

- a. False ✓
- b. True

Triple DES has an effective \_\_\_\_\_-bit key.

Select one:

- a. 256
- b. 64
- c. 56 ✓
- d. 128

In SSL Protocol, the handshake protocol uses symmetric key cryptography to establish a shared secret key.

Select one:

- a. False ✓
- b. True

The message authentication code HMAC uses:

Select one:

- a. Hash function ✓ both "Hash function" and "Cryptographic key". Due to Moodle shuffle issue, each correct answer is awarded full mark.
- b. Both a and b above.
- c. An encrypted Nonce
- d. Cryptographic key

The security of X.509 as deployed on the WWW is established by

Select one:

- a. None of the above
- b. CAs keeping their public key inaccessible to attackers ✗
- c. A proper Web of Trust between users
- d. CAs being added to browser root stores

The correct answer is: None of the above

If a sender proves his/her identity to the receiver by encrypting a random number by a secret key, then what is the drawback of this scheme?

Select one:

- a. Both parties must be aware of the key
- b. Playback attack
- c. Man in the middle attack
- d. All of the above ✗

The correct answer is: Both parties must be aware of the key

Consider a security protocol where the sender sends  $(m, H(m)s)$ , where  $H(m)s$  is the concatenation of  $H(m)$  and  $s$ .  $H()$  being the hash function,  $m$  the message and  $s$  the secret key. This scheme is clearly flawed because:

Select one:

- a. An attacker can sniff and obtain shared secret
- b. An attacker can sniff and derive the hash function ✗
- c. An attacker can sniff and derive the original message
- d. An attacker can sniff and invert the message

The correct answer is: An attacker can sniff and obtain shared secret

### Internet Checksum provides better check than a hash function.

Select one:

- a. False ✓
- b. True

Consider WEP for 802.11. Suppose that the data is 10001101 and the keystream is 1101010. Which of the following is the resulting ciphertext:

Select one:

- a. 11010110
- b. 10011010
- c. 01101101
- d. 11100111 ✓

Suppose Bob initiates a TCP connection to Eve who is pretending to be Alice. During SSL handshake, Eve sends Bob Alice's certificate. Which of the following statement is true for this scenario

Select one:

- a. Eve sends to Bob a MAC of all the handshake messages, using a guessed authentication key which is accepted by Bob. The MAC test will fail, and Bob will end the TCP connection.
- b. Eve will be able to capture Alice's private key during protocol exchange and generate MAC of all the handshake messages. The MAC test will pass, and Bob will accept the TCP connection. ✗
- c. Eve will be able to use her private key, decrypt the shared secret key and succeed in generating authentic MAC of all the handshake messages. The MAC test will pass, and Bob will accept the TCP connection.
- d. Eve sends to Bob a MAC of all the handshake messages, using the guessed authentication key. The MAC test will pass, and Bob will accept the TCP connection.

The correct answer is: Eve sends to Bob a MAC of all the handshake messages, using a guessed authentication key which is accepted by Bob. The MAC test will fail, and Bob will end the TCP connection.

### Cryptographic hash function takes an arbitrary block of data and returns

Select one:

- a. fixed size bit string ✓
- b. both (a) and (b)
- c. variable size bit string
- d. none of the mentioned

The correct answer is: fixed size bit string

From your knowledge of security protocols at Transport layer, when shopping at amazon.com, the client's credit card number is encrypted by

Select one:

- a. A symmetric key established in the handshake protocol ✓
- b. Client's private key
- c. Amazon's public key
- d. Amazon's private key

In epidemic propagation model Nodes can request data from which of the following:

Select one:

- a. from its nearest neighbours caching the data
- b. from cloud resident remotely in the Internet
- c. All of the other choices ✗
- d. the source of the information (e.g. a base station)

The correct answer is: from its nearest neighbours caching the data

Which algorithm is used to encrypt the Protocol Data Unit (PDU) in bluetooth?

Select one:

- a. AES-CCM ✓
- b. RSA
- c. HMAC
- d. Ecliptic Curve Cryptography

A Security Association...

Select one:

- a. describes both AH and ESP settings for a simplex connection
- b. is a multinational organisation in charge of security standards
- c. describes both AH and ESP settings for a duplex connection ✗
- d. describes either AH or ESP settings for a simplex connection

The correct answer is: describes either AH or ESP settings for a simplex connection

What is the maximum number of active Bluetooth devices in a piconet?

Select one:

- a. 8 ✓
- b. 10
- c. 9
- d. 7

In the D-H key exchange protocol, D-H may be used over ECC.

Select one:

- a. False ✗
- b. True

When a new client is connected to an authenticator using the 802.1X protocol, the authenticator's port is enabled and set to the "authorized" state.

Select one:

- a. True
- b. False ✓

Select the right key combination from the following that is broadcast and multicast 802.11 frames in 802.11 Enterprise security

Select one:

- a. Pairwise Transient, Group Temporal
- b. Master Session, Pairwise Transient
- c. Pairwise Master, Group Temporal ✗
- d. Group Master, Group Temporal

The correct answer is: Pairwise Transient, Group Temporal

A Security Policy Database...

Select one:

- a. is commonly implemented in Oracle SQL
- b. contains rules how IPsec must be applied to incoming and outgoing packets
- c. contains rules how the assets of an organisation must be insured to protect against losses ✗
- d. contains rules how security mechanisms are applied in a given system, e.g. the kernel using TLS

The correct answer is: contains rules how IPsec must be applied to incoming and outgoing packets

Which of the following characterizes the wormhole attack best:

Select one:

- a. An attacker creates a worm and floods the network
- b. A worm is created and launched via the Internet ✗
- c. An attacker records packets at one location in the network, tunnels them to another location.
- d. A hole is created in user's disk to destroy the data

The correct answer is: An attacker records packets at one location in the network, tunnels them to another location.

What information in Bluetooth is firstly known to attacker for packet interception without any efforts?

Select one:

- a. Preamble
- b. Channel Hopping Increment
- c. Protocol Data Unit (PDU) ✗
- d. Channel Hopping Interval

The correct answer is: Preamble

Which of the following is correct:

Select one:

- a. TLS can be used together with IPsec ✓
- b. TLS runs on the application layer
- c. TLS runs above IPsec, which runs above IP
- d. TLS runs above IP, which runs above IPsec

Which Layer 2 protocol is used for authentication in an 802.1X framework?

Select one:

- a. PAP
- b. EAP ✓
- c. CHAP
- d. MS - CHAPv2

What type of information is used by the authenticator and authentication server to validate each other?

Select one:

- a. Username and password
- b. Server-side X.509 digital certificate ✗
- c. Client-side X.509 digital certificate
- d. Shared secret

The correct answer is: Shared secret

Which of the following variable is not used during the 4 - Way Handshake to produce a pairwise transient key (PTK)?

Select one:

- a. Group Master Key
- b. Authenticator MAC address ✗
- c. Pairwise Master Key
- d. Nonces

The correct answer is: Group Master Key

How many data channels are available in Bluetooth Smart, except for device advertisement?

Select one:

- a. 37 ✓
- b. 38
- c. 39
- d. 40

Which of the following best characterizes a Sybil attack:

Select one:

- a. A new node is introduced in the network to launch MiTM
- b. All of the other choices
- c. A node presents several identities to break fault tolerance or reputation systems ✓
- d. A Sybil server is created in the cloud to capture packets for passive analysis

The authentication server used in conjunction with 802.1X employs such things as

Select one:

- a. LDAP
- b. RADIUS
- c. Active Directory
- d. All of the other choice ✓

What is the difference between the inner and outer identity in EAP Tunnelled methods?

Select one:

- a. The outer identity is in plain text; the inner identity is securely transmitted inside a TLS tunnel. ✓
- b. Only the authentication server provides its credentials in the outer identity response.
- c. The inner identity is only for authentication server credentials provided to the supplicant.
- d. The inner identity must correspond to the outer identity for realm – based authentications.

How does a RADIUS server communicate with an authenticator? (Choose all that apply.)

Select one or more:

- a. TCP ports 1645 and 1646
- b. Encrypted IPsec tunnel
- c. UDP ports 1812 and 1813 ✓
- d. Encrypted TLS tunnel

Which of the following is true Signature Based Attack:

Select one:

- a. A user's signature is forged to access the system.
- b. Attacker keeps sending forged data to since one of them would eventually succeed
- c. Attacker keeps sending forged data to deplete Node's energy in performing signature verification ✓
- d. Attacker fools a node and obtains the key used to generate the signature

Comparing IPsec to TLS, which statement is true:

Select one:

- a. IPsec is more secure because it uses RSA and TLS does not
- b. None of the choices are true ✗
- c. TLS is more secure than IPsec because it uses Diffie-Hellman key exchanges
- d. IPsec may have better performance if no TCP is used

The correct answer is: IPsec may have better performance if no TCP is used

IPsec...

Select one:

- a. is more secure than TLS because it does not use X.509
- b. is more secure than TLS because it uses X.509
- c. is activated on-demand when an applications requires it ✗
- d. requires administrative effort as it runs in kernel space

The correct answer is: requires administrative effort as it runs in kernel space

Which of the following is true for a Merkle Tree: (choose all that apply)

Select one or more:

- a. A user has choice to pre-configure revelation either sequentially or in any order
- b. Values can be revealed only sequentially.
- c. Values can be revealed in any order. ✓