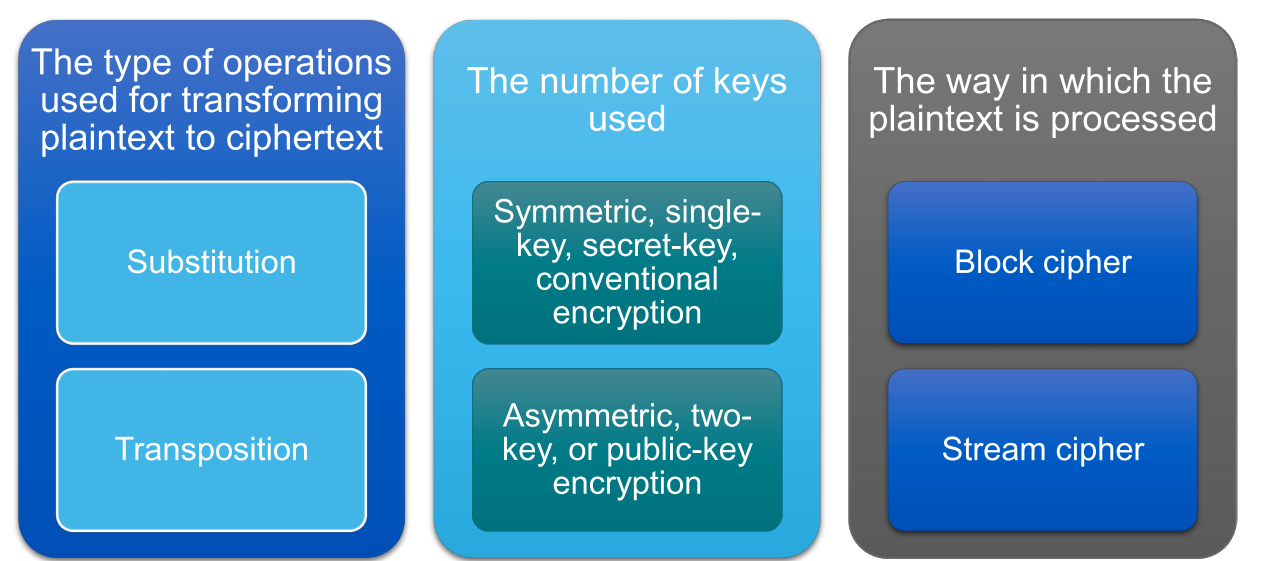
Lecture 2: Introduction to Cryptography

* Conventional Encryption Principles
  + An encryption scheme has five ingredients: Plaintext Encryption algorithm Secret Key Ciphertext Decryption algorithm
  + **Security depends on the secrecy of the key, not the secrecy of the algorithm**
* **Characteristics of Cryptographic Techniques**
  + The type of operations used for transforming plaintext to ciphertext
  + The number of keys used - symmetric (single key) - asymmetric (two-keys, or public-key encryption)
  + The way in which the plaintext is processed

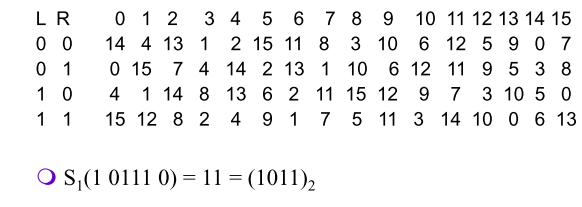


替换 移位 对称 非对称 块 流

* Symmetric Encryption
  + or conventional / private-key / single-key
  + sender and recipient share a common key
  + all classical encryption algorithms are private-key
  + was only type prior to invention of public-key in 1970’s
  + and by far most widely used
* Asymmetric Encryption
  + or public-key encryption
  + uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner
  + **often relies on cryptographic algorithms based on mathematical problems that currently admit no efficient solution,** particularly those inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships.
* Cryptanalytic Attacks
  + May be classified by how much information needed by the attacker: • Ciphertext-only attack • Known-plaintext attack • Chosen-plaintext attack • Chosen-ciphertext attack
* Encryption Scheme Security
  + Unconditionally secure • No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
  + Computationally secure • The cost of breaking the cipher exceeds the value of the encrypted information • The time required to break the cipher exceeds the useful lifetime of the information
* Classical Substitution Ciphers
  + Caesar Cipher
  + Monoalphabetic Ciphers frequency attack
  + One-Time Pad
    - Two difficulties
      * There is the practical problem of making large quantities of random keys
      * Mammoth key distribution problem
    - limited utility 实用性有限
    - **The one-time pad is the only cryptosystem that exhibits perfect secrecy 唯一的**
* Steganography 隐写术
  + hide your plaintext in a graphic image
  + Drawback: high overhead
* Steganography vs. Encryption •
  + **Steganography has a number of drawbacks when compared to encryption**
    - **It requires a lot of overhead to hide a relatively few bits of information**
    - **Once the system is discovered, it becomes virtually worthless**
  + **The advantage of steganography** 
    - **It can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered**
    - **Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide**

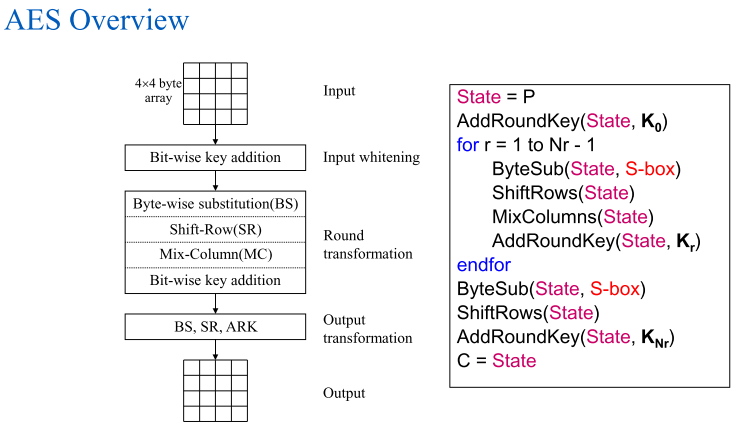
Lecture 3: 对称密码

* Feistel network
  + Feistel network is used in many block ciphers such as DES, RC5
  + not used in AES
  + in DES, each Li and Ri is 32 bits long ki is 48 bits long
* DES characteristics:
  + **Security must depend on hidden key, not algorithm**
  + **Economically implementable in electronic device**
  + key size is 56 bits
  + block size is 64 bits
  + number of rounds is 16
  + Ri= Li−1⊕f(ki, Li) Li=Ri-1 compute Ri−1=Li
* DES S-box

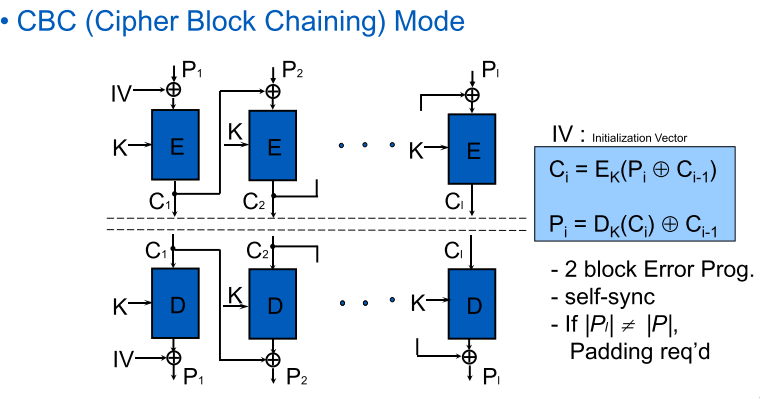


* Known Weakness of DES
  + Complementary Prop.
    - qIf C= E(K,P), C = E(K, P)
  + Weak Key : 4 keys E(K, E(K,P))=P
  + Semi-weak Keys : 12 keys (6 pairs) E(K1, E(K2,P))=P
  + Key Exhaustive Search : 255
  + Current Strength: 243 known plaintext by linear cryptanalysis
* AES/Rijndael characteristics:
  + has 128/192/256 bit keys, 128 bit data
  + Ciphers like Rijndael were referred to as XSL ciphers, because their rounds are composed of the XOR of key material, a nonlinear substitution provided by an S-box, and a linear diffusion stage.

XSL=XOR + S-BOX + LINEAR

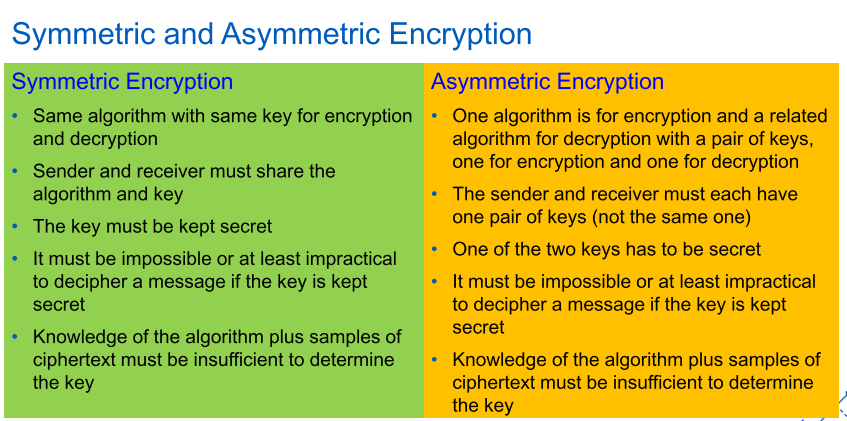


* ECB
  + Identical blocks of plaintext produce identical blocks of ciphertext同样的明文块得到同样的密文块
  + No integrity checks: can mix and match blocks
  + 一位错导致一个块都会错
* CBC
  + 一个密文块失真，两个明文块会错

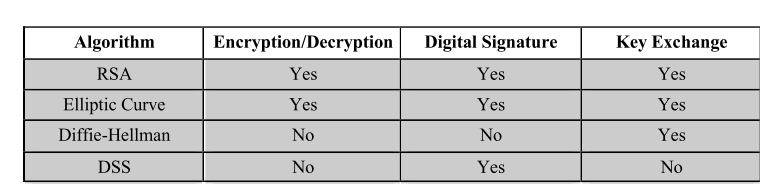


Lecture 4: 非对称密码

* 公钥密码系统解决的两个对称密钥中的重要问题
  + Key-distribution
  + Digital signatures
* 对称密码与非对称密码的对比



* Applications for Public-Key Cryptosystems
  + Encryption/decryption
  + Digital signature
  + Key exchange

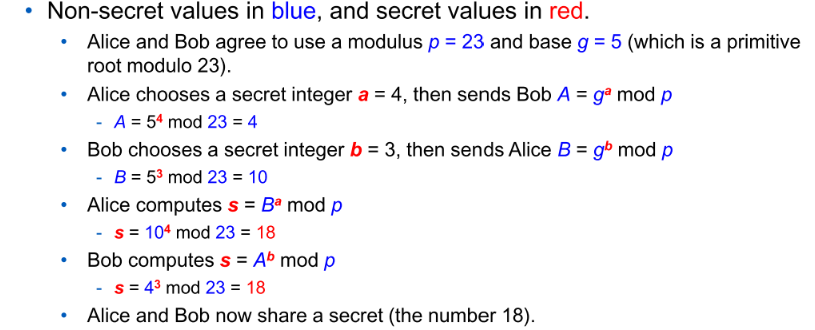


* 公钥密码要求
  + 生成密钥简单
  + 知道明文和公钥得到密文简单
  + 知道密文和私钥得到明文简单
  + 知道公钥没法得到私钥
  + 知道公钥和密文无法得到明文
  + 单项函数
* A public-key encryption scheme is vulnerable to a brute-force attack •
  + Countermeasure: use large keys
* RSA
  + Is a cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some n 明文密文都在n之内
  + E，n作公钥，d，n作私钥
  + C = Me mod n
  + M = Cd mod n = (Me)d mod n = Med mod n
  + 要求。要找到edn满足Med mod n = M
    - 找两个大素数p q
    - 计算n=p\*q note ø(n)=(p-1)(q-1)
    - Selecting at random the encryption key e, where 1<e<ø(n), gcd(e, ø(n))=1
    - Solve following equation to find decryption key d, e\*d=1 mod ø(n) and 0≤d≤n
  + 公钥e常用65537（216+1），3，17 因为只有两位是1，做幂可以做最少次的乘法，但是3太小了，不安全
  + 用d解密时可以用中国剩余定理CRT加速
  + 大素数通过概率验证即可，不一定严格素数
* RSA攻击
  + 分解n获得质因数p q从而得到ø(n)，获得公钥e就可以算出d
  + 时间攻击：通过加密所需的时间来获得明文
    - 对抗方式：Constant exponentiation time • Ensure that all exponentiations take the same amount of time before returning a result; this is a simple fix but does degrade performance确保每次取幂花费时间相同

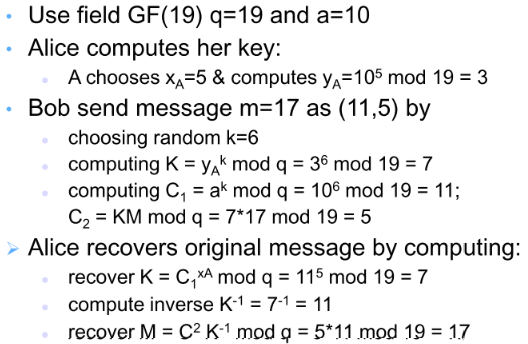
Random delay • Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack加入随机的延迟

Blinding • Multiply the ciphertext by a random number before performing exponentiation; this process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack加密前随意给明文乘上随机数

* + Fault-Based Attack基于故障的攻击
  + Chosen Ciphertext Attack (CCA)
    - 对抗方法：OAEP optimal asymmetric encryption padding
* DH算法 离散对数discrete
  + 第一个公钥算法
  + 只能用来交换密钥
  + abp越大越好，p达到600数字位的质数，无法爆破。

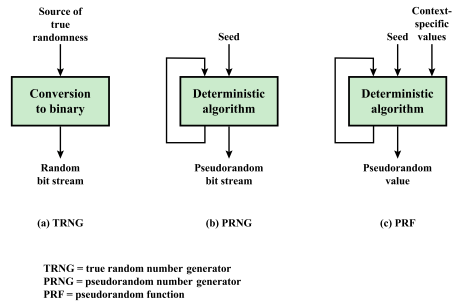
 

* ElGamal Cryptography 离散对数discrete
  + 用在了数字签名标准digital signature standard (DSS)和S/MIME e-mail standard
  + 不加密信息大质数q，q的原根a
  + 同样基于离散对数的难计算

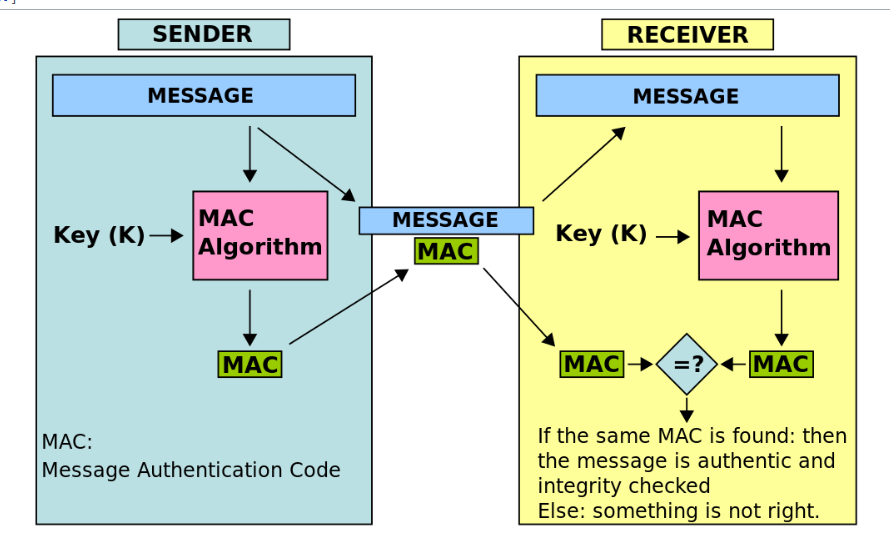


Lecture 5: Random Bit Generation and Cryptographic Hash Functions

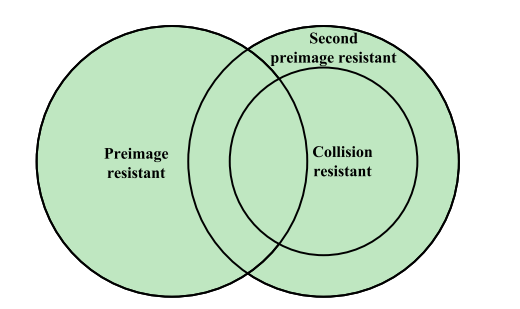
* 随机数的两大需求
  + Randomness
    - 验证随机的方法：
      * Uniform distribution均匀分布 0和1的数量基本相同
      * Independence 独立性 每个随机数之间都没关系
  + Unpredictability



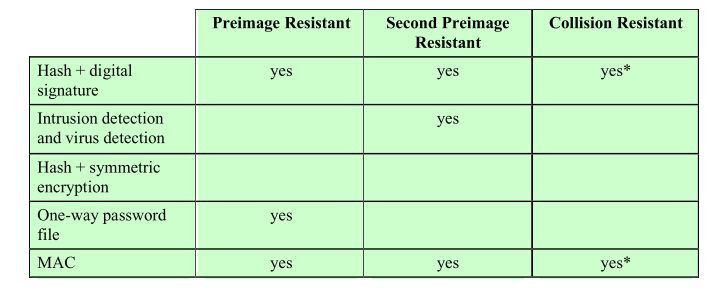
* True Random Number Generator (TRNG)
  + 输入源叫熵源，entropy source，从PC环境获得（类似于键盘敲击特点，磁盘的电子活动，鼠标移动之类的，系统时钟的瞬时值）这些源或者叠加起来
* Pseudorandom Number Generator (PRNG)
  + 输入一个种子，产生一系列的随机数
  + 种子一般使TRNG获得的
  + 获取了算法和种子就能获得所有随机数
* Pseudorandom Number Function(PRF)
  + 种子和明文作输入，获取随机输出。
* 伪随机数的特性
  + Randomness
    - NIST SP800-22检测方法：uniformity scalability consistency
* 种子需求
  + 安全且不可预测
  + 种子必须是TRN或者PRN
* 哈希函数
  + 符合单项性质和无冲突性的函数
  + PRNG一般来说是very weak hash functions
  + 哈希或者MAC（消息认证码）可以用来制造PRNG
* 哈希函数用途
  + Message Integrity Check (MIC) • 验证文件是否被修改 MD5校验
    - send hash of message (digest) •
    - MIC always encrypted, message optionally
  + • Message Authentication Code (MAC) •
    - send keyed hash of message •
    - MAC, message optionally encrypted
  + • Digital Signature (non-repudiation) •
    - Encrypt hash with private (signing) key •
    - Verify with public (verification) key
* MAC



* + 又叫做keyed hash function
  + 不知道key的attacker改了mesg也没法改mac 收信方就可以知道被改了
* 数字签名
  + 对mesg得到摘要，然后对摘要私钥加密
* 其他用处
  + 数据库存密码的hash
  + 通过看hash的变化检查病毒入侵
  + 作为PRF和PRGN
* Preimage原象
  + 就是hash h = H(x)里的自变量x
  + 对于同样的h值有多个原象
* 碰撞
  + 自变量不等，hash值相等
* 输入大小任意 输出固定
* Hash计算需要高效
* Hash输出要符合伪随机
* 三个攻击
  + One way 给出hash值，破解出自变量x
  + 二次原象second preimage
    - 给出自变量x，找到自变量y，两个hash相同
  + Collision
    - 找到一对x和y 他们hash相同



* 需要抵抗的攻击

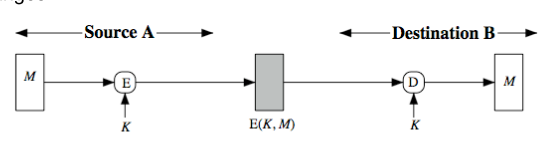


\* Resistance required if attacker is able to mount a chosen message attack

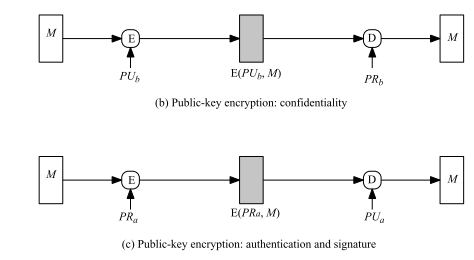
* 可以利用类似CBC的模式多次hash 提高安全
* 常见hash
  + MD5 SHA家族
  + 一般来说迭代hash
    - 会用一个压缩函数
    - 输入被分块
    - a compression function is used on the current block mi and the previous output hi−1 to compute: hi = f(mi, hi-1)
* MD
  + 128bit输出
* SHA后面跟着就是bit SHA512是512bit SHA512/是224bit

Lecture 6: Random Bit Generation and Cryptographic Hash Functions

* 基于加密的MA
  + 对称密钥加密

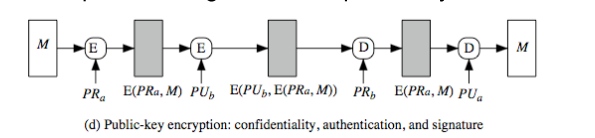


* + 非对称密钥加密



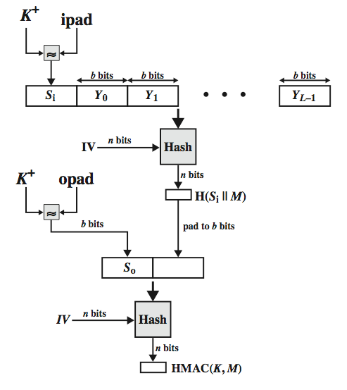
安全性和认证性无法同时保证

* + 综合非对称密钥加密

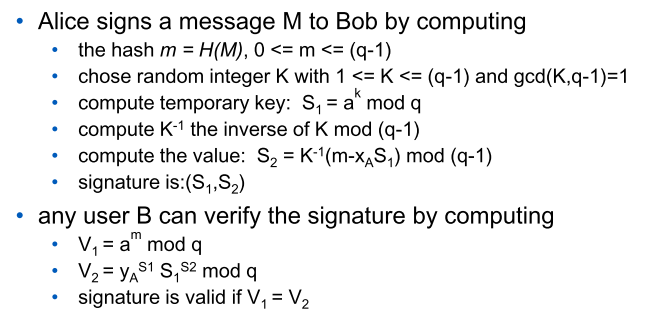


先私钥加密再公钥加密

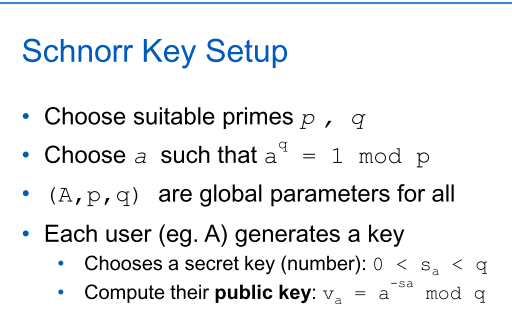
* 基于MAC的MA
  + 两种模式
    - 先算出MAC再拼起来加密发出去
    - 先加密再算出MAC再拼起来发出去
* MAC的要求
  + 抵抗二次原象
  + 均匀分布
  + MAC值和明文所有bit有关
* MAC的攻击
  + 攻击密钥空间
  + 攻击MAC值
* HMAC MAC with hash
  + HMACK(M)= Hash[(K+ XOR opad) || Hash[(K+ XOR ipad) || M)] ]

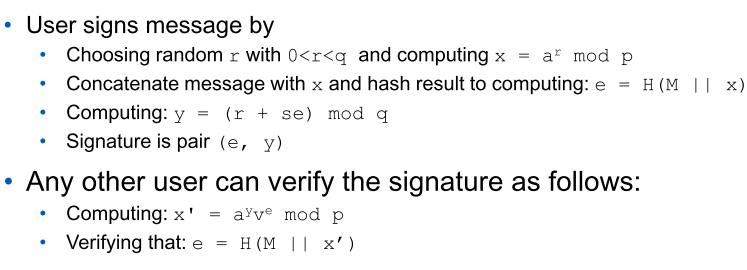


* 用于MAC的对称密码
  + 可以用块加密做的最后一块当作MAC
  + Data Authentication Algorithm DAA广泛应用于MAC 基于DES-CBC
    - using IV=0 and zero-pad of final block
    - encrypt message using DES in CBC mode
    - and send just the final block as the MAC or the leftmost M bits (16≤M≤64) of final block
    - 但是这样的MAC太短了，不够安全‘
* CMAC Cipher-Based MAC
  + 就是刚刚的DAA
* 数字签名
  + 是有附加功能（不可否认）的包含了认证功能的一种code
* 对数字签名的攻击
  + Key-only attack •
  + Known message attack •
  + Generic chosen message attack •
  + Directed chosen message attack •
  + Adaptive chosen message attack
* 数字签名的要求
  + 签名必须防伪造防否认
  + 容易生成签名 容易校验
  + 无法通过签名获得消息，无法制造假签名
  + 依赖于mesg生成
  + 可留档
* 直接签名
  + 用私钥对消息加密
    - 存在的问题：
    - 发送者可能说她的私钥被盗窃了，不是他发的，导致被否认
    - 解决：消息加时间戳并上报中央
* ElGamal Digital Signatures

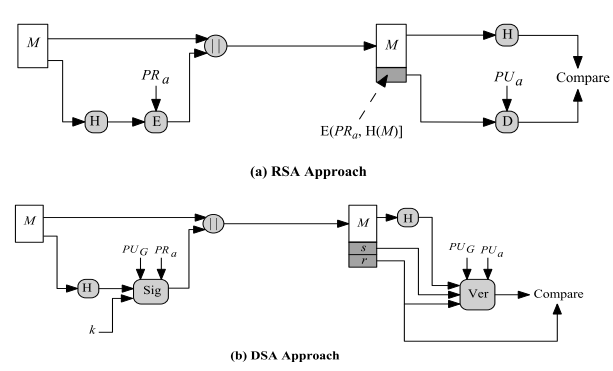


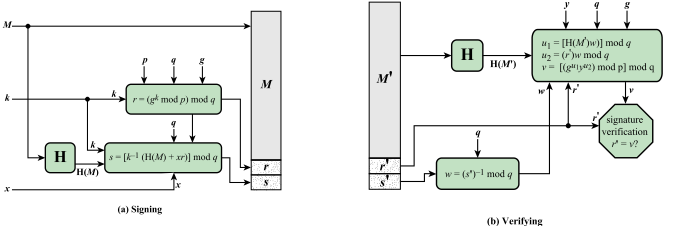
* Schnorr Digital Signatures

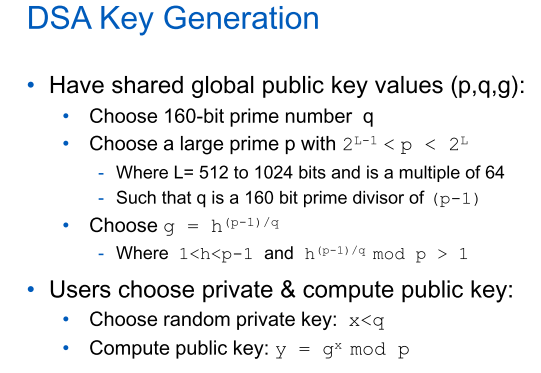


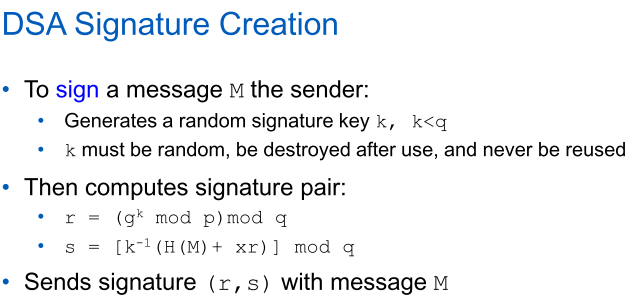


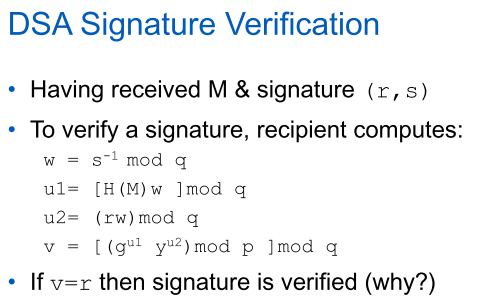
* NIST Digital Signature Algorithm (DSA) 320 bit



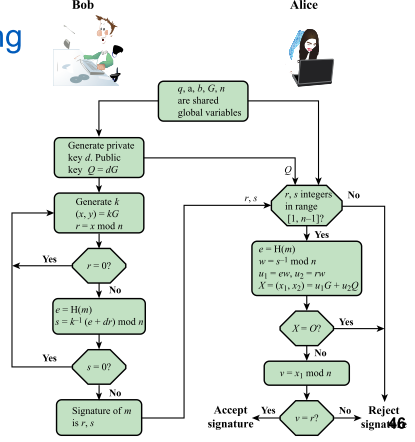






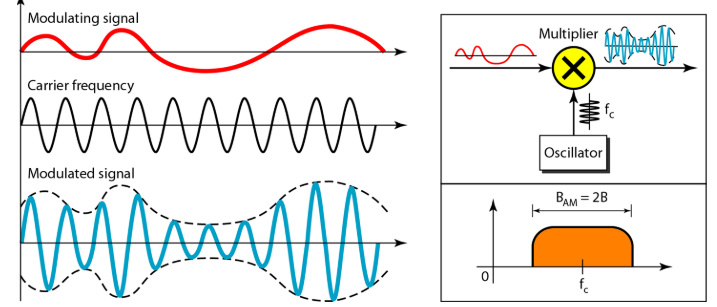


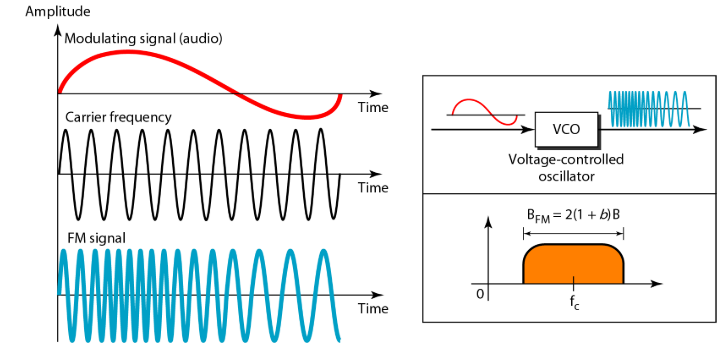
* 椭圆曲线

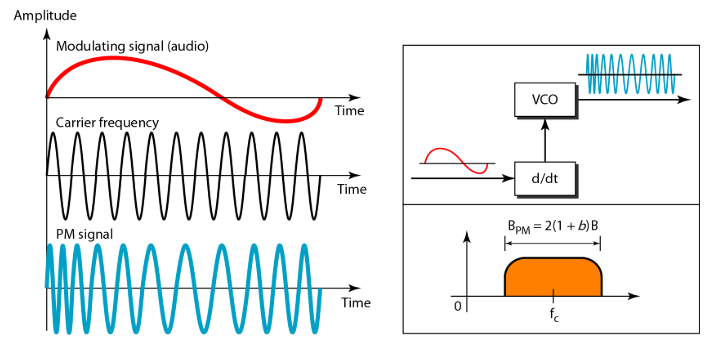


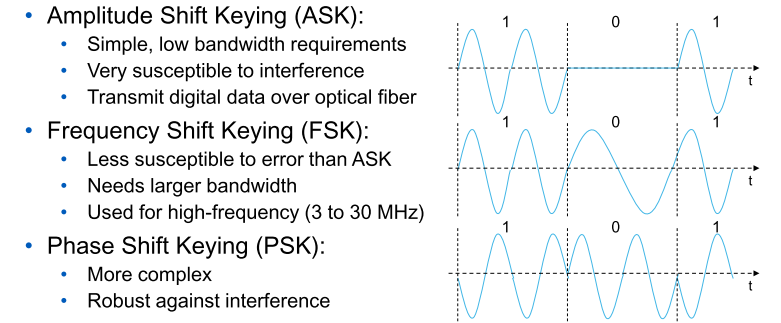
Lecture 7: Basics of Wireless Networking I

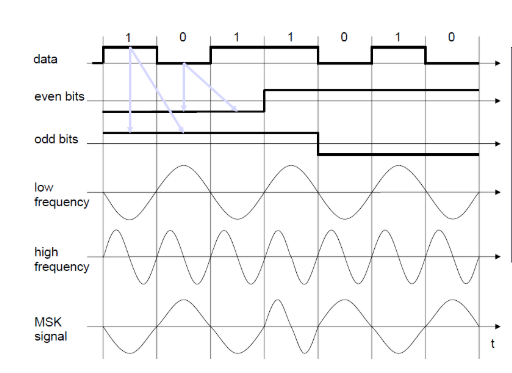
* EM spectrum
  + 全部的频谱
* Radio spectrum or radio frequency (RF)
  + 3k~300G hz
* 带宽
  + 能包含大部分能量的频率宽度
* FCC Licensed bands: licensed by government authority
  + “Narrow-band” - channel width 6.25, 12.5 or 25KHz
* ISM License-free bands: industrial, scientific, & medical (ISM)
  + Wide-bandwidth 5Mhz
* 手机一般用授权频段
* WLAN用非授权2.4G 5.8G 一共11个频道，每个5Mhz
* 容量与最大传输速率相关
  + 用bps单位
  + 主要由带宽决定
* 特定服务的贷款是固定的
* Nyquist Formula
  + Capacity (measured in bps) C = 2B - B is the allocated bandwidth, measured in Hz
  + C = 2B log2 M - M = number of discrete signals or voltage levels
* White Noise Channel 香农
  + The capacity is C=Blog(1+S/N)
  + S/N is the signal strength / noise (SNR)
  + SNR in db = 10 log10 signal power/noise power
  + SNR受到环境影响
* 信号传输
  + 路径损失
    - 收到的信号是发射时的1/d2，d为收发者距离。
    - 实际中应该是1/da，a在2-5之间
  + 传输模式
    - Groud wave地波
      * 最高2Mhz，跟随地球轮廓传输，例如AM radio
    - Sky wave空波
      * 在地表和电离层（ionosphere）反射传播 可以走几千公里 2-30Mhz Amateur Radio, Military Comm.
    - Line of sight
      * 视线距离内传播
      * 超过30Mhz
      * TV, satellite, optical comm.
* 信号衰落 fading
  + 无线传输中的主要问题
  + 定义：由传输介质或路径的变化引起的接收信号功率的时间变化。
  + 衰落来源
    - 自由空间损失 大气层吸收 **多径传播（反射 散射 衍射 折射） 可动性 （快速衰落 小衰落**） 其他发射器的干扰
    - Free space loss •
    - **Multi-path propagation - Reflection, scattering, diffraction, refraction**
    - Interference with other transmitters
    - Atmospheric absorption
    - **Mobility - Fast fading, small fading**
* 多径传播
  + 信号会随着时间分散，time dispersion
    - 会受到邻居的干扰，ISI Inter Symbol Interference
  + 信号到达后会有相位变化，不同相变有不同的失真度
* 可动性的影响 mobility
  + 收发可能在移动
  + 快速衰落
    - 小距离移动，移动距离是波长的一半，导致的小规模衰落
  + 缓慢衰落
    - 在距离大于波长时，导致大规模衰落
* 信号传输三个范围 由近到远
  + 传输范围 transmission range
    - 可以通讯 低错误率
  + 检测范围 detection range
    - 信号可检测 不可以通讯 高错误率
  + 干扰范围 interference range
    - 信号无法被探测 信号成为背景噪声
* 多路复用 multiplexing
  + 多个信号源公用一个传输介质
  + 解复用是从一个信号组合中分理到单独的信号流 demultiplexing
  + 四种方法 Frequency (f) • Time (t) • Space (si) • Code (c)
* FDM Frequency Division Multiplexing
  + 将频谱分成多个频段，一个频道在整个时间内获得某个频段
  + 优点：
    - 无需动态协调 no dynamic coordination necessary
    - 对模拟信号也OK
  + 缺点
    - 流量分布不均匀（unevenly）时会浪费带宽
    - 不够灵活
    - 需要Guard spaces 守卫空间
* TDM
  + 一个频道在整个时间内的一段时间占据整个频谱
  + 优点：
    - 在任何时候，介质中只有一个载体 （only one carrier）
    - 多用户时仍然有高吞吐量
  + 缺点
    - 需要精确的同步 precise synchronization
* TFDM
  + 上面两个的结合
  + 一个用户在特定的时间获取特定的频段 GSM就是这样
  + 优点
    - 防止频率选择性干扰 frequency selective interference
    - 防窃听 tapping
  + 缺点
    - 需要精确的协调 precise coordination
* CDM
  + 用在蜂窝电话和一些卫星通讯
    - 例如手机的CDMA
  + 所有频道同时使用同样的频谱
  + 数学原理
    - 来自正交矢量空间的值可以无干扰的组合和分离 orthogonal space
  + 每一个发送方有一个唯一的二进制code ci，叫做chip sequence
    - Chip sequence 是正交向量，任意两个点积为0
  + 发送发要发Vi时，就用Ci和Vi叉乘，然后传输结果
  + 优点：
    - 带宽效率高
    - 不需要协调和同步
    - 可以抗干扰抗窃听
  + 缺点
    - 信号重现复杂
* Modulation 调制
  + 将源信号（0 1）转化为载波信号 carrier signal
  + 两个步骤：
    - 模拟调制 将基带信号的中心频率提升到radio carrier
    - 数字调制 将数字数据转化为模拟信号
* Analog modulation
  + Analog-to-analog conversion is the representation of analog information by an analog signal. Modulation is needed if the medium is bandpass in nature or if only a bandpass channel is available to us. 带通信号就是把基带信号经过载波调制后的信号
  + Analog-to-analog conversion包含amplitude frequency phase modulation三种 振幅 频率 相位



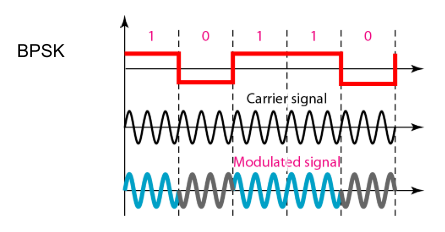




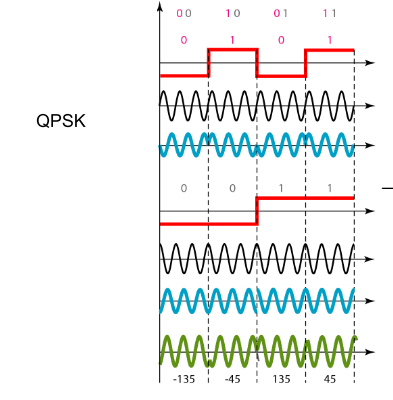
* Digital modulation
  + 数字信号的调制也叫shift keying 键控 SK
  + 同样三种ASK FSK PSK 振幅 频率 相位 抗干扰越来越强，但是也越来越复杂
* AFSK advanced FSK中的MSK
  + FSK所需的贷款依赖于载波频率的距离以及源信号的bit速率
  + 特殊的预计算可以避免突然的相变 MSK就是这样工作 minimum
  + Bits separated into even and odd bits, the duration of each bit is doubled 比特分为偶数和奇数位，每个比特的持续时间加倍
  + 根据比特值（偶数，奇数），选择较高或较低频率，保持或反转
  + 一个载波的频率是另一个的两倍



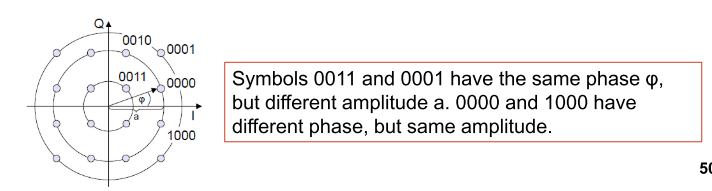
* APSK
  + BPSK binary PSK
    - Bit为0 正弦波 bit为1 反正弦
    - 频谱效率低
    - 用在卫星系统



* + QPSK quadrature 正交
    - 2个bit作为一个符号
    - 符号决定正弦波的移动
    - 比BPSK带宽低 但是复杂

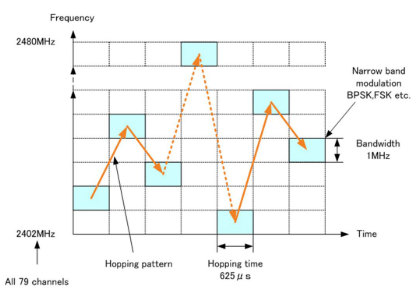


* QAM 正交 quadrature amplitude modulation
  + 结合A和F的modulation
  + 使用一个符号编码n位
  + 需要2n个离散等级，n=2时就是QPSK

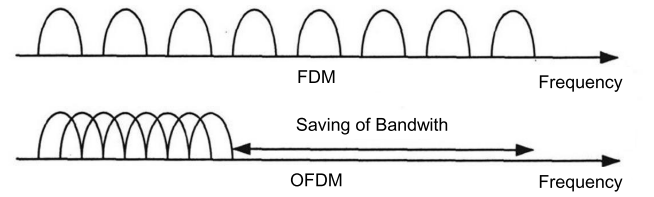


Lecture 8: Basics of Wireless Networking I

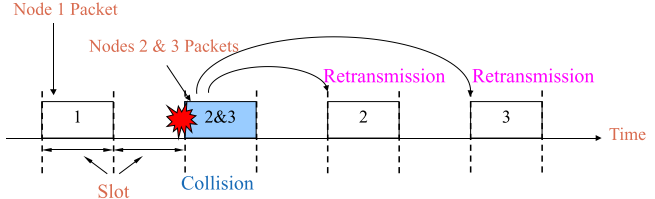
* Spread Spectrum Technology 扩频技术 SS
  + 问题：
    - 在这些调制技术之后产生的带宽，窄噪声或衰落可以消除整个窄带信号！
  + 解决：将窄贷款信号扩展为宽带宽信号
  + SS的两种技术
    - Frequency Hopping Spread Spectrum (FHSS) 跳频扩频
    - Direct Sequence Spread Spectrum (DSSS) 直接序列扩频
  + SS的好处
    - 抗噪声强
    - 共享带宽
    - Tap-proof 可以用来隐藏或者加密信号 由于功率很小，很难探测
* FHSS
  + 信号在看似随机的一系列radio frequency上广播
    - 信号以固定的间隔跳跃频率



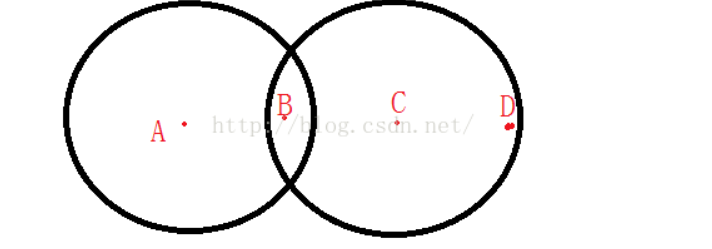
* + 优点：
    - 由于Jammer需要阻塞所有频率，因此对窄带推断具有很强的抵抗力
    - 窄带宽的窃听者会在背景噪声中更加明显
  + 缺点
    - 需要同步
* DSSS
  + 在更宽的频段上扩频
  + 使用xor把数据和扩频码组合在一起
  + 优点：
    - 减少了频率的选择性衰弱 selective fading
    - 在蜂窝网络中
      * 基站可以使用相同的频率范围
      * 多个基站可以检测和恢复信号
      * 软切换
  + 缺点
    - 需要精确的功率控制
* FHSS和DSSS对比
  + 吞吐量上
    - DS连续传输 PSK
    - FS需要重同步来hop FSK
  + 抗干扰
    - DS会受到其他使用同频段的DS的干扰，干扰太强时DS会停止工作
    - FS不会有上述情况
  + 多路径容差 Multipath tolerance
    - DS有很高的传输率，对回声（echo）和延迟（delay）更加敏感
* OFDM orthogonal frequency DM正交频分复用
  + 目的：提高传输率
  + 问题：衰减和干扰
    - Frequency selective fading频率选择性衰减：小规模衰减，不同频率的信号衰减程度不同
    - Inter-symbol interference ISI 符号间干扰：一个符号干扰后续符号的情况。
  + 解决：多载波调制，和FDM有关
    - 高比特率信号被分成许多低比特率信号
    - 每一个低比特率信号都用不同的载波调制
* FDM和OFDM对比
  + FDM需要guard bands，出现了贷款浪费。
  + OFDM可以重叠，这是因为正交性



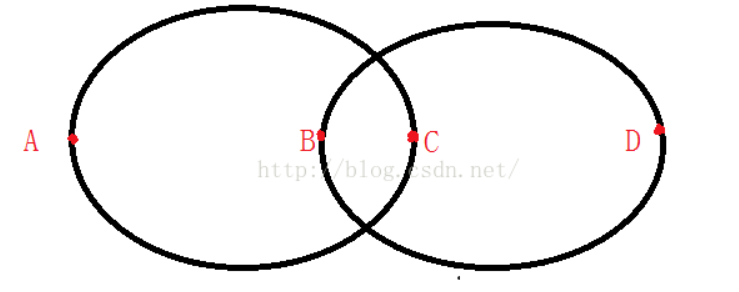
* OFDM可以减少ISI，相比DSSS来收，OFDM的bit time更长，有助于减少前后符号之间的干扰
* 频率选择性衰减只发生在OFDM中的几个子载波中
* MAC协议 Medium Access Control (MAC) protocols
* 理想的多址协议 Ideal Multiple Access Protocol
  + 速率R的广播信道，发送者可以以R来发，M个接收者可以以R/M接受，没有同步，没有协调
* MAC的分类
  + Channel Partitioning
    - 把信道分为很多小片（时间槽，频率，码）
    - 为不同的用户分配小片
  + Random access
    - 允许冲突发生，但是要能从冲突中恢复
  + Taking turns
    - 进行紧密协调来避免冲突
* Channel partition MAC
  + 有FDMA TDMA CDMA A指access 前面就是FDM的FDM
  + TDMA
    - 按轮次（round）访问信道
    - 每一个站点在每一轮中获取到固定长度的时间槽
    - 没人用的槽就空闲（idle）
    - 在低负载时效率比较低
  + FDMA
    - 采用FDM
  + CDM
    - 用CDM 叉乘后传输
    - 在无线广播信道中用得很多 蜂窝 卫星
* Random Access Protocols MAC
  + 必须探测冲突并且从冲突中恢复（例如延迟传输）
  + ALOHA
    - 只要有站点有数据，就执行传输
      * 发送者通过收听目标的广播确定是否发送成功还是冲突了
      * 冲突就隔一段时间重发
    - 最大吞吐量18%
  + 带槽的ALOHA slotted ALOHA
    - 时间分槽
    - 在时间槽的开始站点才能发送
    - 需要同步
    - 同一个槽有多个传输时，所有节点都检测碰撞
    - 优点
      * 单个活跃节点可以满速连续传输
      * 高度分散，只有槽内节点需要同步
    - 缺点
      * 存在碰撞，有槽浪费
      * 空闲槽的存在



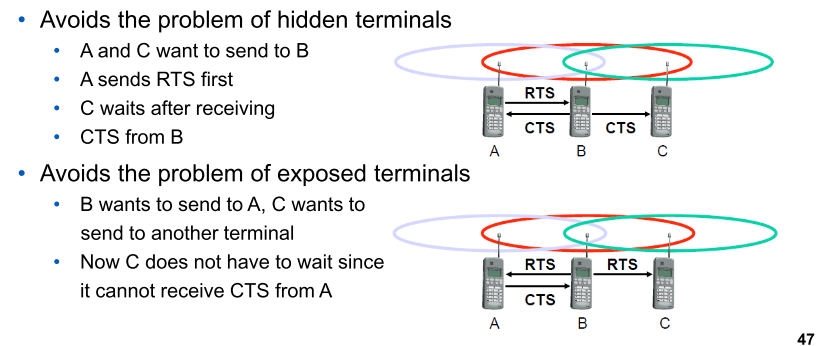
* + CSMA Carrier Sense Multiple Access
    - 改进
      * 发送数据前先监听信道
      * 如果没有传输再发送
    - 依旧存在碰撞
      * 由于非零传输延迟导致
      * 即使发生了冲突，也没法处理，继续传输导致信道完全浪费
      * 传输延迟越大，冲突概率越高
  + CMSA/CD collision detection
    - 用在以太网里
    - 改进
      * 检测到冲突后停止发送
    - CD
      * 每一帧要变为两倍 来完成CD（也就是2\*最大传输延迟）
      * 碰撞发生时，所有站点随机等待
    - 问题
      * 无线时CD（“listen while speak”）无法工作
      * CD开销很大
  + CSMA/CA collision avoidance
    - 改进：
      * 发现信道可以传输时，通过一个随机的退避定时器 back-off timer来最小化碰撞概率
    - 核心
      * 载波感知器carrier sensor采用CCA Clear Channel Assessment
        + 载波存在->不传输
        + 载波不存在->**可能**可以进行传输（还要等待**DIFS**，就是一个等待时间）
      * CA
        + 使用IFS Inter-Frame Spaces (IFS) 帧间弓箭
        + 随机避让机制 back-off mechanism
        + 可能实现不同的固定优先级（QoS）
    - 问题
      * 隐蔽终端问题
        + A和C互相不在范围内，不知道对方的存在，同时向能同时知道A和C的B 发送数据，发生了冲突。



* + - * 暴露终端问题
        + 当B向A发送数据的时候，终端C也想给D发送数据：但是，终端C检测到信道处于忙状态，则不会向D发送数据，但是，B向A发送数据是不会影响C向D发送数据的。



* + CSMA/CA with RTS/CTS request to send clear to send
    - 发送发的RTS表明其想占据信道多久
    - 接收方CTS回应预期的传输持续时间
      * 帮助缓解了隐蔽终端的问题
    - 收到了CTS的发送方知道自己不能在这段时间传输
      * 帮助缓解了暴露终端的问题
    - 收信方在收到数据后会发送给发送方一个ACK
      * 所有的节点在开始传输前必须等到ACK



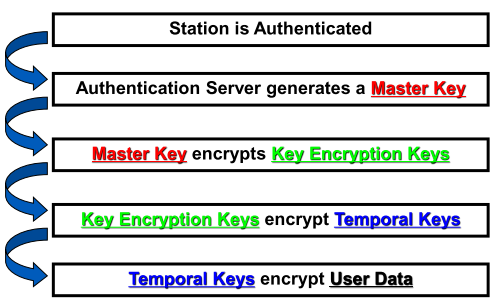
* “Taking Turns” MAC
  + 轮询 polling
    - 主节点按顺序邀请子节点来传输
    - 问题
      * 轮询开销大
      * 延迟大
      * 单点失败问题（主节点down了怎么办）
  + 令牌传递 token passing
    - 发送控制令牌在节点中按顺序传递
    - 问题
      * 令牌带来的开销
      * 延迟
      * 单点失败（有令牌的节点down了

Lecture 9: Wired Equivalent Privacy (WEP)

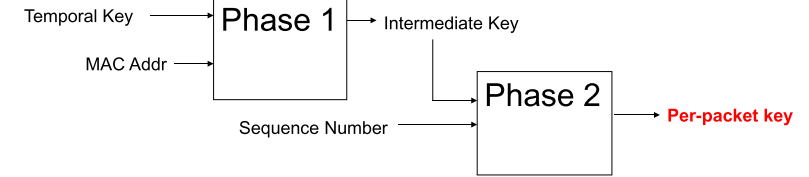
* 为什么无线领域中的安全十分重要
  + 没有固有的物理保护 inherent physical protection
  + 广播通信
  + 窃听相对简单
  + 假消息注入 重放攻击 非法访问 拒绝服务攻击
* 无线安全需求
  + 保密性 confidentiality
  + 认证性 authenticity
  + 检测重放 replay detection
  + 完整性 integrity
  + 访问控制 access control
  + 防止拥塞 Protection against jamming
* WEP
  + 802.11标准里定义
  + 目标
    - 保密性
    - 访问控制
    - 数据完整
  + 使用RC4加密
  + 最初64bit 40的key 24的IV
  + 后来变成104+24
  + 最后232+24
* WEP加密过程
  + Message: What you’re encrypting •
  + CRC: To verify the integrity of the message •
  + Plaintext: The message + CRC •
  + Initialization vector (IV): A 24-bit number which plays two roles that we’ll meet in a moment
  + Key: A 40 or 104-bit number which is used to build the keystream
  + Keystream: What is used to encrypt the plaintext •
  + Ciphertext: What we end up post-encryption
* WEP encry step
  + Compute CRC for the message
    - CRC-32 polynomial is used
  + Step 2: Compute the keystream •
    - IV is concatenated with the key •
    - RC4 encryption algorithm is used on the 64 or 128 bit concatenation
  + Step 3: Encrypt the plaintext •
    - The plaintext is XORed with the keystream to form the ciphertext
    - The IV is prepended to the ciphertext
* WEP的主要问题
  + 密钥重用 IV
  + 密钥管理与分发
  + 弱消息认证 ICV
  + 共享密钥认证
    - 可以在不知道密钥时，与AP进行认证
    - 但是无法进行下一步，因为没有key
* WEP密钥流
  + WEP种子放进PRNG里生成一个keystream
    - WEP seed = 24-bit IV + fixed key
    - 然后keystream和明文与checksum异或得到密文
  + 每次相同的IV使用相同的fixed key也就是主密钥，那么keystream也就相同
  + 出现了keystream重用现象，十分不安全
  + 但实际上，由于密钥管理问题，主密钥不太会被更改，那么问题就很大了
  + 24bit的IV太小了，2\*\*24的IV会在5小时内重复一轮（11mbps），随机分配IV的话，5000个包之后就会冲突（50%）
  + 按顺序分配的话肯定会冲突
* 弱IV与RC4中的弱Key
  + 弱IV对应弱key
    - 弱key的特点
      * 第一个字节从3到7，第二个字节255，第三个字节随便
    - 40bit的WEP密钥里，由9000个弱IV，达到了IV的5%，太不安全
* 弱消息完整性 ICV
  + ICV通过cyclic redundancy check (CRC-32)获得，这个算法不安全
  + 攻击者可以改掉数据包，算出ICV获得AP响应，便于重放和注入
* WEP没有密钥管理协议
  + 密钥必须手动更新
* 获取keystream后就可以完成认证，无需key
* 攻击总结
  + IV/key重用
    - 已知明文攻击，通过已知的IP ICMP ARP攻击
    - 部分明文已知攻击 通过已知的IP头攻击
  + 弱ICV
    - 缺乏重放攻击的抵抗
    - 可以实时反转bit
  + 没有密钥管理或者交换机制
  + 缺少认证
    - 欺诈攻击 DoS攻击
* 常见攻击手法
  + 爆破/字典
    - 截获两个包，通过第一个算IV和KEY然后算ICV，然后用第二个包验证算没算对
  + FMS攻击
    - 知道前面几个字节就可以攻破RC4
  + Chopchop攻击
    - 截获一个包
    - 砍掉最后一个字节，猜测其值，
    - 用猜测的值和原有的拼接，计算新的ICV看看AP是否接收
    - 接收证明猜对
    - 直到所有都被解开
  + Fragmentation攻击
    - 将包拆分为几个碎片包分析
    - At this point, arbitrary data of (8 − 4) · 16 = 64 bytes (4 byte CRC tag) may be sent
* 对抗措施
  + 提高密钥空间，防止FMS
  + 消除IV重用
  + 防止密钥重用
  + 使用EAP协议Extensible Authentication Protocol
  + 经常换密码
  + 部署Intrusion Detection Systems (IDS)防止注入

Lecture 10: Wi-Fi Protected Access WPA

* WPA wraps RC4 cipher engine in four new algorithms
  + A Message Integrity Code (MIC) called Michael
    - 专门为了硬件设计
  + 使用48bit IV
  + Key Derivation and Distribution 密钥推导和分配
    - 从主密钥创建密钥层次结构
    - 主密钥可以安全刷新
  + TKIP Temporal Key Integrity Protocol generates per-packet keys
* WPA概念
  + 加密方法RC4
  + 密钥大小 128bit 可变
    - 每一帧的密钥都会改变
  + 密钥管理 TKIP Temporal Key Integrity Protocol
  + Hash方法：Michael
    - 8 byte 在data和ICV之间 64bit
  + 802.1x认证
* MIC Michael 算法
  + 使用很多交换 转换甚至丢弃操作
  + 同时保护数据和头
  + MIC是基于计算每个分组的hash
  + MIC基于每个发送者和每个接收者
  + MIC需要seed（IV），源和目标的MAC地址以及有效载荷 payload
* 对抗重放攻击：IV序列执行 IV Sequence Enforcement
  + WPA利用16bit monotonically incrementing counter 单调自增计数器来对抗重放攻击
* TKIP机制
  + 给AP和站点提供新的密钥的机制
  + WPA密钥层次包含 主密钥 master key和会话密钥 session key
    - 主密钥 PMK， pairwise master key 成对主密钥，来自802.1x密钥交换或者密码短语
    - 会话密钥，PTK，pairwise transient key成对瞬态密钥，从主密钥推导得到
  + PMK
    - PMK被分为
      * Key Confirmation Key (KCK) , which is used by the EAPOL-key exchanges to provided data origin authenticity.
      * Key Encryption Key (KEK), which is used by the EAPOL-key exchanges to provide for confidentiality.
      * Temporal Key (TK), which is used by the data-confidentiality protocols (TKIP/CCMP)
    - Rekey过程



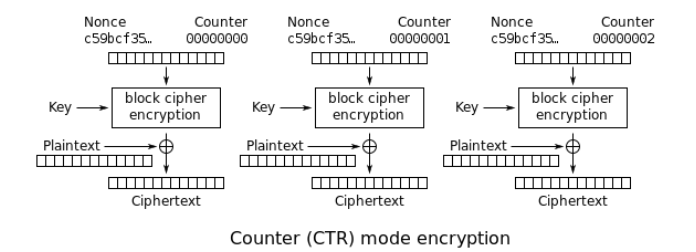
* + 每个分组的密钥混合
    - WEP通过连接借本密钥和IV来构造分组密钥
    - TKIP通过2个混合阶段构造分组密钥



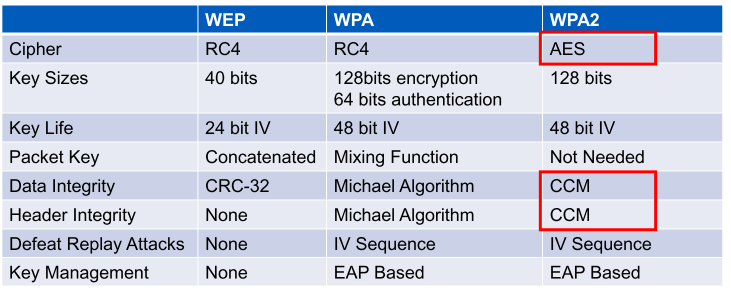
* + TKIP总结
    - 提供了看似薄弱但是是真正的安全
    - 满足软件部署目标 不会因为WEP降低效率
    - 有互操作性 interoperability
    - 通过TKIP计数器可以看到攻击 TKIP counters counter-measure invocation
* How to Negotiate a Passphrase and PTK?
  + 预共享模式和企业模式
* WEP-PSK弱于被动字典攻击
* 四路握手的弱点
  + 离线爆破和字典攻击
    - 攻击者记录4次握手消息
    - 回去在家中破解或者字典攻击
* WPA-PSK 彩虹表
  + 彩虹表是带索引的哈希表
    - 对于顶级SSID的百万个单词的预哈希
    - 2-3TB的数据量大小
    - 最多14个字符
    - Cracks WPA v1 and v2 with pre-shared key
    - Drastically faster checking onsite 现场检查速度快
* WPA要小心使用
  + 太短时，很容易被字典攻击
  + 失败后需要重定密钥
  + 降低或者消除超时在检测到假包后
  + 使用WPA+802.1x 目前还是很安全的
* WPA的攻击
  + Chopchop
  + Plaintext Recovery Attacks
    - 128bit随机密钥的RC4在初始密钥流中有明显的biases
    - 如果可以获得相同明文足够多的加密结果，那么就可以通过这种biases来恢复明文

Lecture 11: Wi-Fi Protected Access WPA2

* WPA2阶段
  + Phase 1: The AP and the client agree on the security policy
    - Capability Discovery
    - Open System Authentication
    - Association
  + Phase 2: Generate the master key
  + Phase 3: Creating temporary keys
  + Phase 4: All keys generated in phase 3 will be used by the CCMP protocol to provide data confidentiality and integrity
* WPA2 encryption
  + 在WPA基础上使用了AES
  + CCMP中的128bit AES
  + CTR模式加密 counter mode
    - The encryption service in WPA2 is based on the AES algorithm used in the CTR mode.



* + 消息完整性验证通过CBC-MAC获得 MAC的加密算法用AES，采取最后一块的结果作为消息完整性验证
  + CCMP可以防止重放攻击，攻击者无法在无知到key时破坏数据的保密性和完整性



* + WPA2抗基本所有的攻击，但是在物理层攻击上，同样没办法，这是wifi所限，如射频干扰 RF jamming 数据泛滥 data flooding 以及接入点故障
  + 无法防止第二层会话劫持 hijacking
  + 黑客可以通过分析未受保护的控制和管理帧来获取信息
  + 容易受到DoS攻击
  + 容易受到MAC地址七篇和大规模认证解除攻击
* KRACK
  + 大程

Lecture 12: Cellular Mobile Network

* GSM 2G
  + 结构 三大部分
    - Mobile Station (MS)
    - Base Station Sub-system (BSS)
    - Network Sub-system (NSS)
  + 安全管理措施
    - Authentication of a user
      * A3设备到GSM网络认证
      * A5/1 A5/2数据和声音的流密码
      * A8对称密钥生成算法
      * COMP128 A3和A8使用的hash函数
    - Ciphering of the data and signaling
    - Confidentiality of a user identity
    - Using SIM as security module
  + 弱点
    - 企业没有专业知识创造新的A3和A8，可以针对COMP128逆向
    - 算法位太小了
    - 身份认证只有一种方式
    - 存在短信或者电话号码欺诈
    - 利用IMSI保护机制中的漏洞 International Mobile Subscriber Identity (IMSI)
  + 其他限制
    - 设计仅仅提供了访问安全 通信和信号没有保护 communication and signaling
    - 设计不能解决主动攻击，网络元素是可以被模拟的 impersonated
    - 设计目标只能与GSM系统连接的网络一样安全
    - 密钥太小 Kc就64bit