Stream Cipher

Tips:

- 一般说OTP 即为key 完全随机的加密流密码
- 一般说stream cipher 即为利用了 PRG加密的流密码

OTP (one time pad)

- 最安全的一种加密方式
- 需要一个和加密消息 message 等长的 key 进行 XOR 加密
- 每次加密都需要生成一个新的key , 且需要将key 共享

def of Secure cipher

- 如果定义不能恢复密钥key是安全的 , 那么 E(key, m) = m 也是安全 ???!!!
- 如果定义不能恢复所有的Plainttext就是安全的, 那么 E(key, m0 || m1 = Key XOR m0 || m1 也是安全的??!!!
- 香浓定理 : 密文中不应该含有明文的任何信息 即为安全的

Def: A cipher ***(E,D)*** over (K,M,C) has **perfect secrecy** if

$$\forall m_0, m_1 \in M \quad (|m_0| = |m_1|) \quad \text{and} \quad \forall c \in C$$

$$Pr[E(k,m_0)=c] = Pr[E(k,m_1)=c] \quad \text{where}$$

OTP 是 prefect secure 的

Pr[E(k, m_0) = c] $\frac{\#从m0到C的映射数量}{k的取值空间}$, 由于OTPm和c为一一对应的, 那么上下都为常数, 所以 为prefect secure

- OTP是prefect secure 的原因是 OTP的key是完全随机的, 且长度和message 等长

Stream cipher

- 定义一个 PRG G(k) -> k^2 意思是输入一个k , 输出一个两倍k长度的伪随机序列
- stream cipher 是基于PRG的 OTP
- PRG 使得 OTP 变得可以实践
- PRG(seed) 是一个决定性的函数
- PRG 是可以根据一个随机的种子seed , 然后生成一个和明文等长的key(伪随机)
- stream cipher 并不是安全的, **因为seed的长度是小于明文的长度的**

Never use two - time pad

Real - world strean cipher

1. Old type

- RC4 :
  - 软件层面
  - 128bits seed => 2048 bits 伪随机 , 1 bytes 怎重新生成一次
  - 用于Https , wep 等
- CSS :
  - 硬件层面
  - 用了移位寄存器

2. morden type

- Salar 20
  - 对于PRG做了改进, 加入了nonce 参数 , 加大了伪随机生成器的随机性
  - Salar 20 PRG => {0, 1}$^{128 or 256}$ X {0, 1}^{64} ===> {0, 1}^{n} 最大可以到达 2^{73} bits

PRG的安全性

- 由于stream cipher 不是绝对安全了, 所以需要一个新的安全的定义
- A PRG is security only if PRG is unpredictable (∀i: no “eff” adv. can predict bit (i+1) for “non-neg” ε), 即给了前nbits , 也不能预测出 (n+1) bits
- 一个安全的PRG : 需要和一个位数相同的完全随机的序列是不可区分的.
  - e.g. 书写方式 : 假设一个数学统计A 为 stat.test A(x) as :

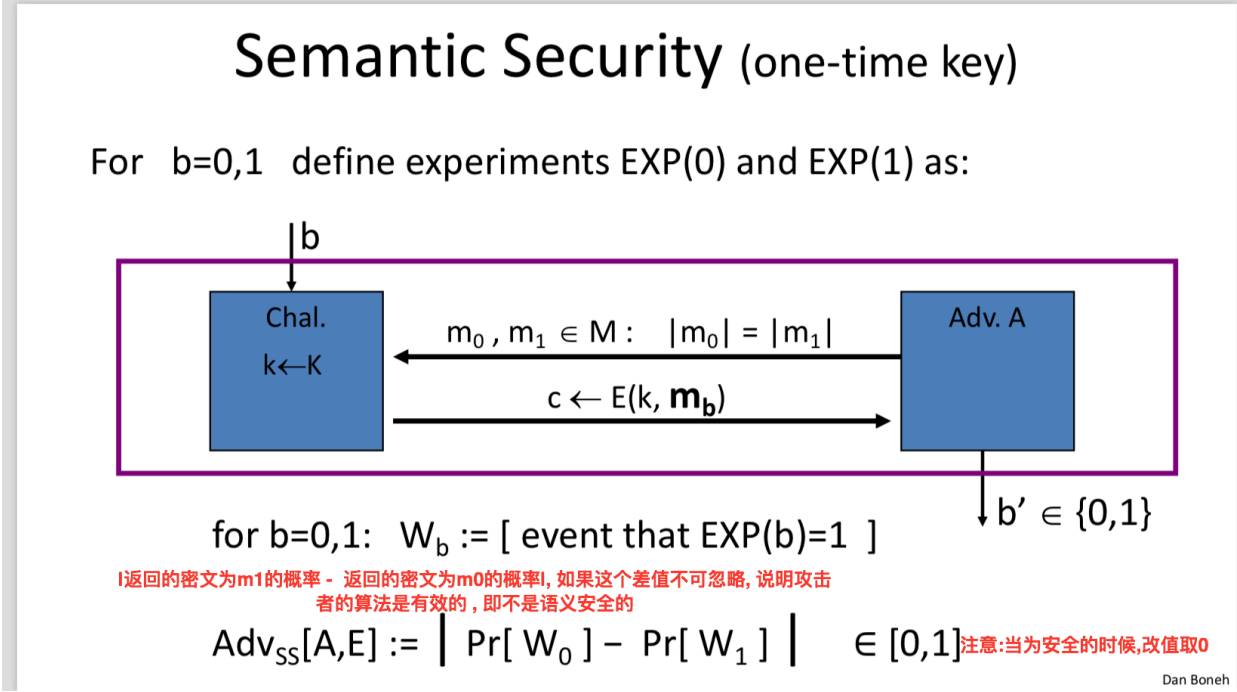
    if [msb(x) = 1] outputs "1" else output "0"

    Adv$_{PRG}$ [A, G] = |Pr(A(G(k))=1) - Pr(A(r) =1)| = Pi
  - if pi is negligible then PRG is secure under this attack

- THM : **an unpredictable PRG is secure**

Semantic Security (one - time key)

描述了one-time key 中的语义安全



|返回的密文为m1的概率 - 返回的密文为m0的概率|, 如果这个差值不可忽略, 说明攻击者的算法是有效的 , 即不是语义安全的

注意:当为安全的时候,改值取0

如果E是语义安全的, 那么这个攻击概率 Adv 应该是可忽略的 negligble

- **OTP is semantically secure** , OTP中key为均匀分步, 所以返回的密文也是均匀分布
- **如果PRG是安全的** ===> stream cipher 亦是安全的

$$\forall \text{ sem. sec. adversary A}, \quad \exists \text{a PRG adversary B} \quad \text{s.t.}$$

$$Adv_{SS}[A,E] \leq 2 \cdot Adv_{PRG}[B,G]$$