**对称加密定义**：

一个对称密钥加密方案是概率多项式时间算法的三元组:

(1)密钥生成算法的输入为安全参数,输出密钥k;记为(Gen

是一个随机算法)。不失一般性,假设任何由输出的密钥k,都满足。

(2)加密算法将密钥k和明文消息作为输入,并且输出一个密文c。因为

Enc可能是随机化的,记为。

(3)解密算法将密钥人和密文c作为输入,输出一份消息m。假设Dec是确定性的,所

以记为。

注:对每个n、每个由输出的密钥k、每个,都满足.

如果满足:对每个由输出的密钥k,算法只对消息

有定义,则是一个消息长度为定长的对称密钥加密方

案。

**窃听者存在情况下的不可区分性：**

窃听不可区分实验

(1)给定输入给敌手输出一对长度相等的消息。

(2)运行生成一个密钥k,选择一个随机比特。一个密文被计算并且给A。把c叫做挑战密文。

(3)A输出一个比特b’

(4)该实验的输出被定义为:如果,则为1,否则为0。如果,则称A成功。

如果对于所有的概率多项式时间敌手A,存在一个可忽略函数negl使得

:

则一个对称密钥加密方案具备在窃听者存在的情况下不可区分的加密,

其中概率的来源是A的随机性以及实验的随机性(选择密钥、随机比特b,以及在加密过程中

使用到的任何随机性)

**窃听不可区分的等价定义：**

对于每个敌手,在观察到的密文或者的密文(长度相等)时,其行为是相同的。因为A只输出单个比特,“行为相同”意味着在每种情况下,输出1的概率几乎相等。定义,使用一个固定比特b(而不是随机的选择)。此外,用来表示A在中的输出比特b’。 A无法判断是在实验中运行还是在中运行。

如果对所有的概率多项式时间的敌手A,存在一个可忽略函数neg使得:

则对称密钥加密方案具有窃听者存在的情况下不可区分性。

**对称密钥加密方案的CPA不可区分：**

CPA不可区分实验:

(1)一个密钥k是通过运行来生成的。

(2)输入给敌手A,敌手A可以访问预言机,输出一对长度相等的消息。

(3)选择一个随机比特,计算出一个密文,交给A。c叫做挑战

密文。

(4)敌手A继续访问预言机Enck(.),输出一个比特b'。

(5)如果b=b’,该实验的输出被定义为1,否则定义为0。(若,则认为A成功。)

一个对称密钥加密方案,如果对所有的概率多项式敌手A,存在一个可忽略函数negl,使得

则是选择明文攻击(CPA)条件下的不可区分加密

**对称密钥加密方案的CCA不可区分：**

CCA不可区分实验:

(1)通过运行生成一个密钥k。

(2)敌手A被指定输入1^n,可使用预言机和。它输出一对长度相等的消息

。

(3)随机选择比特,则计算挑战密文并将其提供给A。

(4)敌手A继续使用预言机和,但是不允许用挑战密文本身来问询。最终,A输出一个比特b'。

(5)如果b=b,实验的输出为1,否则输出0。

一个对称密钥加密方案满足如下条件:对所有的概率多项式时间敌手A,存在一个可忽略的函数negl,使得

则称其为选择密文攻击条件下不可区分加密(或者是CCA安全的)

**伪随机发生器(PRG)定义:**

令为多项式,令G为确定多项式时间算法,该算法满足:对于任何输入,算法G输出一个长度为的字符串。如果满足下面两个条件,则称G是一个伪随机发生器:

(1)(扩展性:)对每个n来说,满足。

(2)(伪随机性:)对所有的概率多项式时间的区分器D来说,存在一个可忽略函数negl,满足

其中r是从中均匀随机选择的,种子s是从中均匀随机选择的,并且概率来源为D的随机性和对r,s的选择。

函数被称为G的扩展系数。

**单向函数(OWF)定义:**

求逆实验:

(1)选择输入,计算。

(2)A给定和输入y,输出x'。

(3)当且仅当时,实验的输出定义为1。

如果满足下面两个条件,则函数是“单向函数”

(1)(容易计算:)存在一个多项式时间算法,输入x,输出f(x)。

(2)(求逆困难:)对任意概率多项式时间算法A,存在一个可忽略函数negl,满足

**伪随机函数(PRF)定义:**

令是有效的、长度保留的、带密钥的函数。如

果对所有多项式时间区分器D,存在一个可忽略函数negl,满足:

则称是一个伪随机函数,其中是均匀随机选择的,并且是从将n比特字符串映

射到n比特字符串的函数集合中均匀随机选择出来的。

**强伪随机置换(PRP)定义:**

令是有效的带密钥的置换。如果对于所有概率多项式时间区分器D,存在一个可忽略函数negl,使得

则称F是强伪随机置换,其中是随机均匀选择的,是从n比特字符申置换的集合

中均匀随机选择的。

**消息认证码(MAC)定义和伪造实验:**

MAC是一个概率多项式时间算法的三元组满足:

(1)密钥产生算法:输入参数,输出密钥k,其中。

(2)标记生成算法:输入密钥和消息输出标记t,该算法是概率性的,记作。

(3)校验算法:输入密钥、消息和标记输出比特位。意味着有效,

则无效,不失一般性,假设算法是确定的,有。

对于每一个输出的每一个k,以及每一个,都有。

如果满足:对输出的每一个k,算法仅对消息有定义(且在任意时输出0),称是一个固定长度的,其消息长度为。对私钥加密而言,通常是均匀随机地选择。

MAC伪造实验 :

(1)运行产生一个随机密钥k;

(2)敌手被给予输入值,并能访间预言机。最后输出一对的值,并用表

示所有A对预言机的询问集合;

(3)实验的输出结果为1,当且仅当:。

如果没有敌手能在上述实验中,以不可忽略的概率成功,则认为MAC是安全的。

一个消息鉴别码,如果对所有的多项式时间敌手A,存在一个可忽略函数,满足

则它是适应性选择消息攻击下存在性不可伪造的,或者说是安全的。

**散列函数(Hash)定义和抗碰撞实验：**

密钥并不是保密的。它只是用在一个特定的函数中。

散列函数是一对概率多项式时间算法满足如下条件:

(1)是一个概率算法,输入参数并输出密钥。假设隐含在中。

(2)存在一个多项式l满足;对H输入一个密钥s和一个字符串,并输出一个字符串(n是隐含在s中的安全参数)。

如果当输入和就称是输入长度为的定长散列函数。

碰撞发现实验:

(1)运行得到密钥s。

(2)敌手输入并输出和。(如果是输入长度为的定长散列函数,我们要求)

(3)当且仅当且时,实验的输出被定义为1。在这种情况下,称A发现了一个碰撞。

散列函数是抗碰撞的,如果对于所有的概率多项式时间敌手A,存在着一个可忽略的函数negl,满足

。

**Reduction方法的做法：**

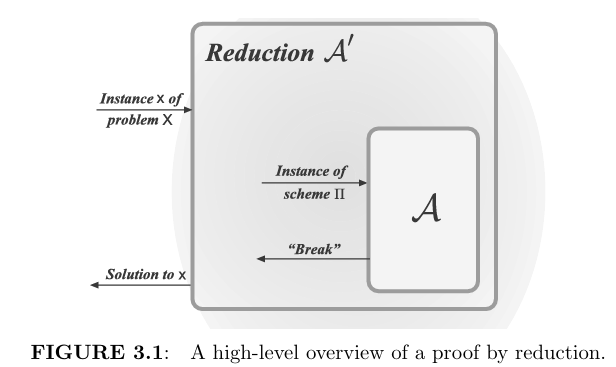
假设某个难题×不能通过任何多项式时间算法以不是可忽略的概率被解决(

想要证明某个密码构造是安全的。做法如下:

(1)指定某个有效的(即概率多项式时间)敌手攻击。将敌手的成功概率表示成为。

(2)构造一个叫做“Reduction”的有效算法,该算法将敌手A作为子程序来使用,试图解决难题X。A’对A是“如何”工作的一无所知;A’知道的唯一的事情就是A想要攻击。所以,指定难题X的某个输入实例x,算法A’将会对A模拟出一个的实例,满足:

1. 就A而言,它和交互。更正式地说,当A被作为子程序被A’运行时,A的分布应该和当A自身和交互时的分布是相同的(或至少是很接近的)。
2. 如果A成功“攻破了”由A’模拟的的实例,则这将允许A’解决给出的难题实例x,成功的概率至少为多项式的倒数,即1/p(n)。



(3)即,如果不是可忽略的,则A’解决难题×的概率为不可忽略的概率。因为A是有效的,将PPT敌手A作为子程序来运行,意味着存在一个有效的算法能够以不可忽略的概率解决X,与原假设矛盾。

(4)因而结论是,给定一个关于×的假设,不存在有效的敌手A能够以不可忽略的概率成

功攻破。换句话说,是计算上安全的。

**公钥加密定义：**

公钥加密方案是概率多项式时间算法的元组:

(1)生成密钥算法用安全参数作为输入,输出一对密钥。把称为公钥,把称为私钥。

(2)加密算法Enc把公钥k和来自某个明文空间的一个消息m作为输入。输出密文c,记

为。

(3)解密算法Dec把私钥sk和密文c作为输入,输出一个消息m或一个定义为失败的特殊

符号⊥。不失一般性,假设Dec是确定的,记为。

满足例外的概率是可忽略的,概率的计算来源于由输出的和使用的任何随机性。

**窃听者存在情况下的不可区分：**

窃听不可区分实验

(1)执行来获得密钥。

(2)敌手A被给予pk,输出一对相同长度的消息(消息必须在与pk相关的明文空间中)。

(3)随机选择然后计算出并且给A。称c是挑战密文。

(4)A输出一位b’。

(5)如果b=b’实验输出1,否则输出0。

如果对于所有概率多项式时间的敌手A存在可忽略函数negl,满足

则公钥加密方案在窃听者存在情况下具有不可区分加密。

**CPA不可区分（等价于窃听者存在下的不可区分）**

CPA不可区分实验

(1) 执行来获得密钥。

(2)敌手A被给予pk,并且敌手能够访问预言机,敌手输出一对相同长度的消息(消息必须在与pk相关的明文空间中)。

(3)随机选择然后计算并且给A。称c是挑战密文。

(4)A继续使用,输出一位b'。

(5)如果b=b’实验输出1,否则输出0。

如果对于所有概率多项式时间的敌手A存在一个可忽略函数negl,满足

则公钥加密方案在选择明文攻击下具有不可区分加密。

**CCA不可区分：**

选择密文攻击不可区分实验:

(1)执行来获得密钥。

(2)给敌手pk,并且可以使用解密预言机Dec(.)。输出一对有相同长度的消息(消息来自于与pk相关联的明文空间。)

(3)选择随机的一个比特},然后计算出密文,并把密文给A。

(4)A继续使用解密预言机,但是不能问询c本身的解密。最后,A输出一个比特b’。

(5)如果b=b’,则实验的输出定义为1,否则为0。

公钥加密方案是选择密文攻击下不可区分加密(或是CCA安全的加密),如果对于所有的概率多项式时间的敌手A,存在可忽略的函数neg,满足

**数字签名定义和伪造实验：**

一个数字签名方案是一个由概率多项式时间算法组成的三元组,满足下列条件:

(1)密钥生成算法以安全参数为输入,并且输出一对密钥,分别称为公钥和私钥。

(2)签名算法以一个私钥和消息作为输入。输出一个签名,表示为。

(3)确定的验证算法Vrfy以一个公钥pk、消息m和一个签名作为输入。输出一位b,当

b=1时意味着签名有效,当b=0时为签名无效。将其表示为。

此方案需要对于任意n,所有由输出的(pk,sk),以及任意,必须满足

签名伪造实验:

(1)运行得到密钥。

(2)将pk和访问“签名预言机”的权利给敌手A。(此预言机对于敌手选定的任意消息m返回一个签名。)然后敌手输出。设Q表示A在执行期间问询签名的消

息的集合。

(3)当且仅当且时,实验输出定义为1。

一个签名方案如果对任意概率多项式时间敌手A存在一个可忽略函数negl,满足

则此签名方案在适应性选择消息攻击下是存在性不可伪造的。

离散对数和 Diffie-Hellman 假设:

离散对数实验:

(1)运行而得到,其中G是一个阶为q的循环群,g为G的一个生成元。

(2)选择(可以通过选择,并且设置来完成)。

(3)A给定,输出。

(4)如果定义实验输出为1,其他情况下输出为0。

如果对于任意概率多项式算法A,存在一个可忽略函数neg满足

则与G相关的离散对数问题是困难的。

如果对任意概率多项式时间算法A存在一个可忽略函数negl,满足

则DDH是困难的。概率来源于实验中的输出,以及随机选择的。

注意到当z从中随机选择时,元素在G中是独立均匀分布的。