物联网网络层安全实验	文档编号	版本	页数
	AWS-WSN-01	1.0	10

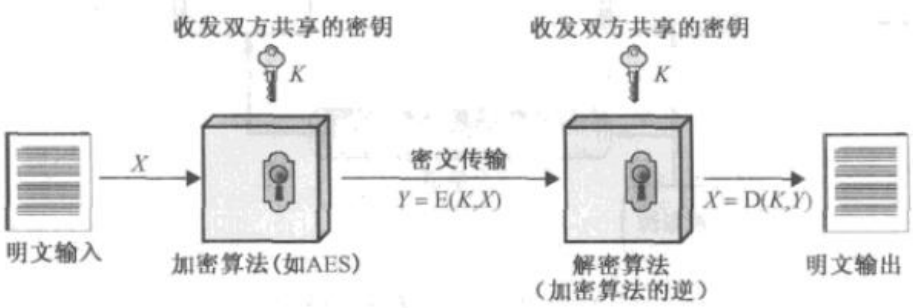
1 实验目的

帮助学生理解密钥概念，更直观直观认识对密钥与网络密钥在系统安全中所起的作用。

2 实验原理

3 对称密码和非对称密码机制

3.1 对称密码机制



对称密码算法，也称为传统加密或单钥加密算法，对称密码模型包括 5 个基本成分：

明文：原始可理解的消息或数据，是加密算法的输入。

加密算法：加密算法对输入的明文进行各种代替和变换，输出密文。

密钥：密钥也是加密算法的输入。密钥独立于明文和算法。算法根据所用的特定密钥而产生不同的输出密文。

密文：密文是加密算法的输出，是看起来完全随机而杂乱的消息或数据。一旦算法确定了，那么密文的取值取决于明文和密钥。如果明文也确定了，那么密文的取值也完全取决于密钥。

对称密码模型的安全使用要满足如下两个要求：

加密算法强度足够强。即攻击者拥有一定数量的密文和产生这些密文的明文，仍无法破译密文或发现密钥。

发送者和接收者必须在某种安全的形势下获得密钥并且必须保证密钥安全。如果有攻击者发现该密钥，而且知道相应的加解密算法，那么就能解读使用该密钥加密的所有通信。

3.1.1 分组密码

分组密码是将一个明文分组作为整体加密并且通常得到的是与明文等长的密文分组。即加密算法每次对一个明文分组（明文块）进行加密，典型的分组长度是 64 位（bit）或 128 位。发送者和接收者需要共享一个对称加密解密密钥。

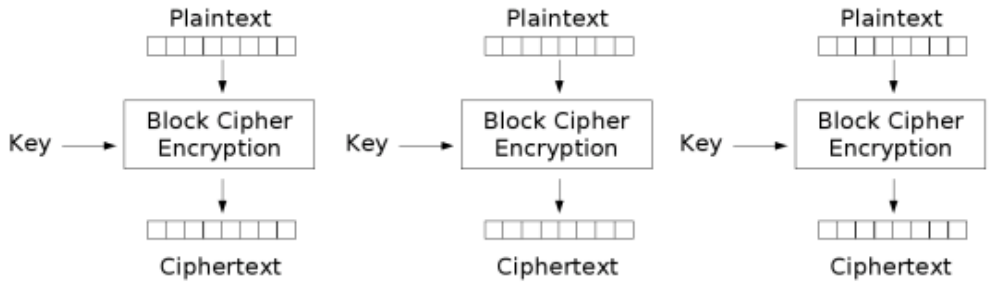
典型的分组密码有 DES、AES 等算法。DES 的明文分组长度为 64 位，密钥长度为 56 位。AES 的明文分组长度为 128 位，密钥长为 128 位、192 位或 256 位。

3.1.2 分组密码的工作模式

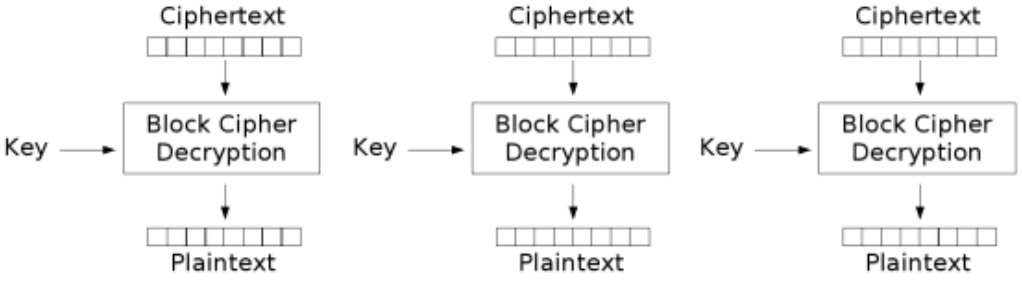
分组密码的工作模式是一种用来加强密码算法安全强度或使算法适应具体应用的技术。分组密码有 5 种标准的工作模式，即电码本模式（Electronic Code Book, ECB）、密文分组链接模式（Cipher Block Chaining，CBC）、密文反馈模式（Cipher Feedback，CFB）、输出反馈模式（Output Feedback，OFB）和计数器模式（Counter，CTR）。

模　式	描　述	典型应用
电码本(ECB)	用相同的密钥分别对明文分组独立加密	● 单个数据的安全传输(如一个加密密钥)
密文分组链接(CBC)	加密算法的输入是上一个密文组和下一个明文组的异或	● 面向分组的通用传输 ● 认证
密文反馈(CFB)	一次处理 s 位，上一块密文作为加密算法的输入，产生的伪随机数输出与明文异或作为下一单元的密文	● 面向数据流的通用传输 ● 认证
输出反馈(OFB)	与 CFB 类似，只是加密算法的输入是上一次加密的输出，且使用整个分组	● 噪声信道上的数据流的传输(如卫星通信)
计数器(CTR)	每个明文分组都与一个经过加密的计数器相异或。对每个后续分组计数器递增	● 面向分组的通用传输 ● 用于高速需求

3.1.2.1 ECB



Electronic Codebook (ECB) mode encryption

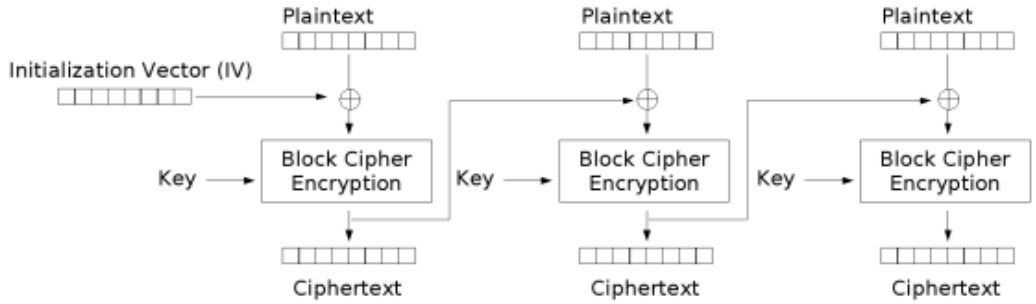


Electronic Codebook (ECB) mode decryption

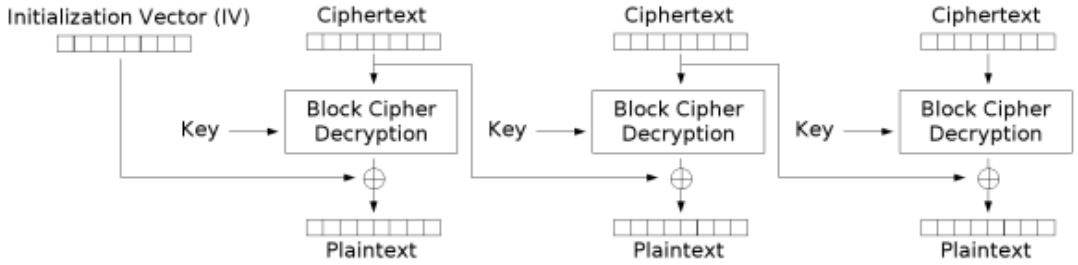
最简单的工作模式是电码本 ECB 模式，它一次处理一组明文分组，每次使用相同的密钥加密。ECB 模式特别适合于数据较少的情况，比如加密密钥。因此，若想安全传输一个 DES 或 AES 密钥，选择这种模式是合适的。ECB 要求，如果最后的明文分组长度不够一个分组长度的话，则需要填充至分组长度。ECB 模式最重要的特征是一段数据中若有几个相同的明文分组，那么密文也将出现几个相同的密文分组。

因此，当加密很长的数据时，ECB 模式可能不安全。如果数据是非结构化的，密码分析者可能利用数据的规律性特征来进行破译。例如，若已知这段数据总是以某些固定的字符开头，密码分析者就可以拥有大量已知明文密文对，依次来进行分析。若数据有重复的成分，且重复的周期正好是分组长度的倍数，则密码分析者就能辨认出这些成分，然后可以利用带环或重排这些分组的方式来进行分析。

3.1.2.2 CBC



Cipher Block Chaining (CBC) mode encryption



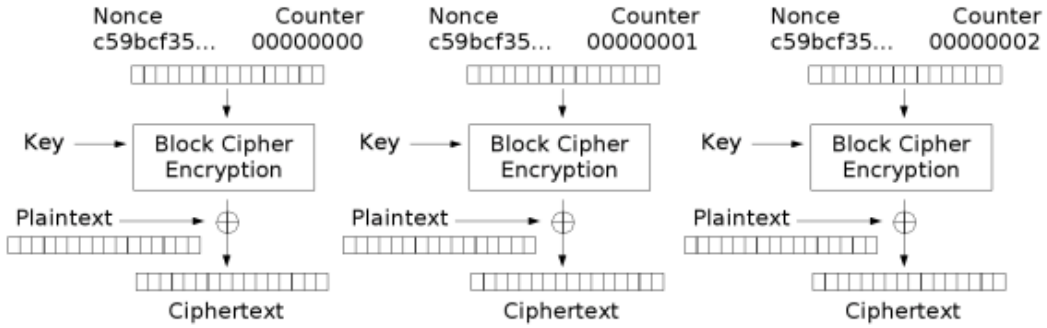
Cipher Block Chaining (CBC) mode decryption

为了克服 ECB 的弱点，就需要将重复的明文分组加密成不同的密文分组。为了实现这个效果，就需要用到 CBC 模式。CBC 模式下加密算法的输入使当前的明文分组和上一个密文分组的异或运算结果，而加密使用的密钥仍是相同的密钥。加密算法的每次输入与明文分组没有固定的关系。因此，若有重复的明文分组，加密后的密文分组也会不同。CBC 和 ECB 一样，如果最后的分组长度不够一个分组长度，也需要填充。

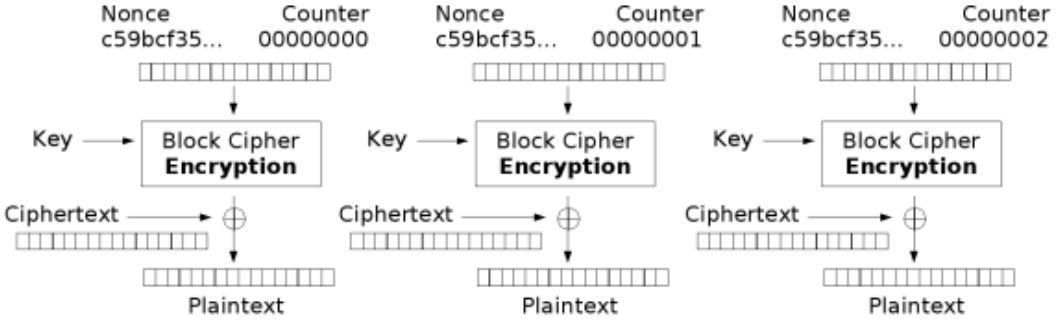
在第一个明文分组处理时，可以和一个初始向量 IV 异或后再加密，以此产生第一个明文分组。解密时将第一个明文分组解密的结果与 IV 异或恢复出第一个明文分组。IV 是和密文长度相同的一组数据。发送者和接收者必须共享 IV，并保证第三方无法预测。在 CBC 的解密过程中，每个密文分组分别进行解密，再与上一个密文分组异或就可以恢复出明文分组。

CBC 的链接机制使得它适合于加密长度大于一个分组长度的数据。

3.1.2.3 CTR



Counter (CTR) mode encryption

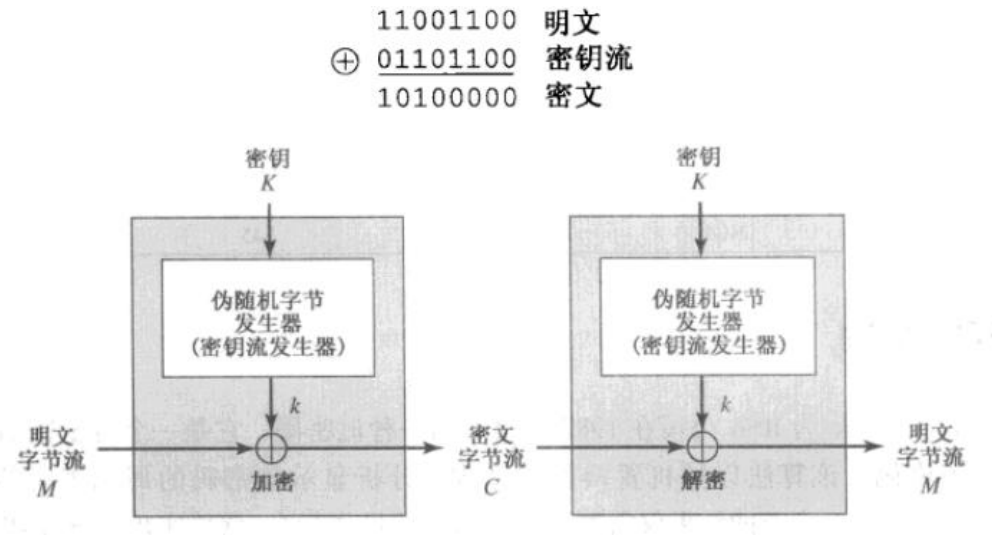


Counter (CTR) mode decryption

计数器模式中计数器的长度使用与明文分组长度相同。计数器首先被初始化位某一值，然后随着数据分组的增加，计数器的值加 1（模 2^b，b 是分组长度）。加密时，计数器加密后与明文分组异或得到密文分组，不同分组之间没有 CBC 那样的链接关系。解密过程中，使用相同值的计数器序列，用加密后的计数器的值与密文分组异或恢复明文分组。因此，解密过程也需要知道初始计数器的值。

3.2 流密码

与分组密码不同的是，流密码每次加解密是对一位（bit）或一个字节（byte）操作的，而不是一个分组。流密码的基本思想是，利用初始密钥生成一个密钥比特流，将这个密钥比特流与明文进行逐比特的异或操作得到密文。流密码的加密和解密也需要发送者和接收者共享一个初始密钥，利用这个初始密钥根据相同的计算方法得到相同的密钥流。



3.3 非对称密码机制

非对称密码与对称密码完全不同。首先，非对称密码是基于数学函数的，而对称密码是基于代替和置换的。更重要的是，对称密码机制中，发送者和接收者使用的是相同的密钥，而非对称密码机制中，发送者和接收者使用的是两个独立的密钥（公钥和私钥）。而且，非对称密码机制中的两个密钥在数据的机密性、密钥分配和身份认证等领域有着重要意义。

非对称密码算法依赖于一个加密密钥和一个解密密钥，算法具有以下两个重要特点：

仅根据密码算法和加密密钥来确定解密密钥在计算上是不可行的。

某些非对称算法中（如 RSA），两个密钥中的任何一个都可用来加密，另一个用来解密。

非对称密码模型有 6 个组成部分：

明文：算法的输入，是可读信息或数据；

加密算法：加密算法对明文进行各种变换；

公钥和私钥：算法的输入，这对密钥中的一个用于加密，另一个用于解密。加密算法执行的变换依赖于公钥或私钥；

密文：算法的输出，它依赖于明文和密钥，对给定的数据，不同的密钥生成的密文不同；

解密算法：该算法接收密文和相应的密钥，并还原得到原始明文数据。

对称密码（传统密码）与非对称密码（公钥密码）的对比如下图所示。

传统密码	公钥密码
一般要求	**一般要求**
(1) 加密和解密使用相同的密钥和相同的算法	(1) 同一算法用于加密和解密，但加密和解密使用不同密钥
(2) 收发双方必须共享密钥	(2) 发送方拥有加密或解密密钥，而接收方拥有另一密钥
安全性要求	**安全性要求**
(1) 密钥必须是保密的	(1) 两个密钥之一必须是保密的
(2) 若没有其他信息，则解密消息是不可能或至少是不可行的	(2) 若没有其他信息，则解密消息是不可能或至少是不可行的
(3) 知道算法和若干密文不足以确定密钥	(3) 知道算法和其中一个密钥以及若干密文不足以确定另一密钥

3.4 密钥定义及其重要性

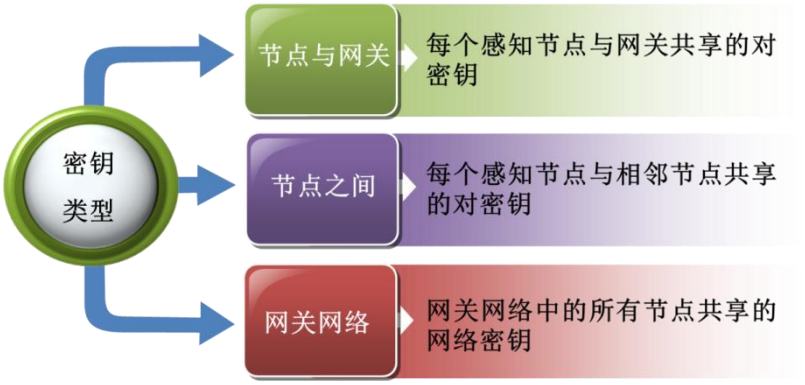
分析上述关于对称密码和非对称密码的描述发现，无论是对称密码还是非对称密码，由于加密算法都是公开的，所以加密机制的安全性就完全决定于密钥的安全性，即密钥都是必须保密的。

从理论上来将，密钥也是数据，但是由于密钥是用来加密其他数据的，因此，密钥的安全性要求最高。

3.5 密钥类型及密钥导出

从密钥用于来划分，密钥类型包括主密钥、密钥加密密钥、会话密钥三个主要类型。主密钥是指通信双方长期建立密钥关系的基础，也是安全等级最高的密钥。密钥加密密钥是由主密钥导出的，用来加密其他密钥的密钥。会话密钥是由密钥加密密钥来生成和加密的。例如，将主密钥作为密钥导出算法的输入，输出得到密钥加密密钥。将密钥加密密钥作为密钥导出算法的输入，输出得到会话密钥。

从密钥的作用范围来划分，密钥类型还可以分为网络密钥、对密钥、组密钥等。例如在一个无线传感器网络中，假设有一个网关，10 个传感器节点，则会存在如下图所示的三种密钥类型。



每个节点与网关之间都会存在一个对密钥，每个节点与相邻节点也会分别共享一个对密钥（或者节点中的某一部分节点、一簇节点共享一个组密钥），网络中的所有节点共享一个网络密钥（即网关与所有节点之间共享的一个密钥）。

3.6 密钥分配与密钥管理

就对称加密来说，通信双方必须使用相同的密钥并且该密钥要对其他人保密。如果攻击者在攻击破解密钥，那么为了减少攻击者破译密钥所带来的危害，通信双方需要定期的更新密钥。因此，这也就会涉及到密钥的更新、分配及其他管理工作。

对于通信双方 A 和 B 来说，密钥的分配可能以如下不同方式实现：

A 选择一个密钥后以人工或物理分发的方式传递给 B。

第三方选择密钥后以人工或物理分发的方式传递给 A 和 B。

如果 A 和 B 先前或最近使用过一个密钥，则一方可以将新密钥用旧密钥加密后发送给另一方。

如果 A 和 B 到第三方 C 有加密连接，则 C 可以在加密连接上传送密钥给 A、B。

4 实验内容

4.1 客户端与网关的对密钥预置

网关客户端用户与网关服务器之间的身份认证，可以采用基于随机数挑战响应认证方式来实现。学生通过操作界面来设置网关客户端用户的用户名(UserID)和口令(PIN)，以及网关客户端用户的 UKEY 与网关服务器之间的加解密算法的共享密钥。其中，网关客户端的用户输入用户名(UserID)和口令(PIN)代表了其知道什么，而 UKET 及 UKEY 的密钥称为身份认证的令牌，代表了网关客户端用户拥有什么。具体可参见实验二《身份认证实验》的实验原理内容。

4.2 节点与网关的对密钥预置

在节点与网关的通信过程中，对密钥用于传输数据的加解密，保证节点与网关之间的通信安全；网关也可以使用该密钥给某个特定节点发送敏感数据，节点也可以通过该密钥上报敏感数据给网关。

学生通过操作界面设置节点与网关之间的对密钥（即每个节点与网关之间共享的对密钥）。

节点和网关在部署网络前需要进行一些预置“密钥材料”的工作，具体如下：

- 网关生成所部署网络中的所有节点的 ID 号及与其 ID 号一一对应的随机数 N(8B)
- 网关与所部署的所有节点都预置一个散列函数 MD5
- 每个节点预置与自己的 ID 号相对应的随机数 Ni(i=1,2,3,...n)
- 新部署的合法新节点要预置当前的网络密钥

4.3 节点与网关的网络密钥预置

学生通过操作界面设置网关的网络密钥。