当作类似 AES 算法的对称密钥使用，可以只选择其中 128 个最重要位。另一种做法就是对 k_{AB} 使用哈希函数，并将得到的输出作为对称密钥使用。

在实际协议中，我们首先需要选择私钥 a 和 b。为了防止攻击者的准确猜测，这两个数必须来自于真随机数生成器。在计算公钥 A 和 B 以及会话密钥时，双方都可以使用平方-乘算法。这两个公钥通常通过预计算得到，因此，密钥交换中需要做的主要计算就是会话密钥的指数运算。由于 RSA 和 DHKE 的位长度和计算都非常类似，所以它们的计算开销也很接近。然而，第 7.5 节中介绍的使用短公开指数的技巧不适用于 DHKE。

到目前为止，我们讨论的都是群 $\mathbb{Z}_p^*$ (其中 p 为素数)内的古典 Diffie-Hellman 密钥交换协议。这个协议很容易就能推广到椭圆曲线群，进而产生了椭圆曲线密码学，而此密码学已经成为实际使用中非常主流的非对称方案。椭圆曲线和类似 Elgamal 加密的方案与 DHKE 有着紧密的关联，为了更好地理解这些概念，下面将首先介绍离散对数问题(这个问题是 DHKE 的数学基础)，然后重新审视 DHKE 并讨论其安全性。

8.2 一些代数知识

本章主要介绍了抽象代数的一些基础知识，尤其是群、子群、有限群和循环群的概念；这些概念对理解离散对数公钥算法非常重要。

8.2.1 群

为方便起见，这里将重述第 4 章给出的群的定义：

定义 8.2.1 群

群指的是一个元素集合 G 以及联合 G 内两个元素的操作 o 的集合。群具有以下属性：

1. 群操作 o 是封闭的，即对所有的 $a,b \in G$，$aob = c \in G$ 始终成立。
2. 群操作是可结合的，即对所有的 $a,b,c \in G$，都有 $ao(boc) = (aob)oc$。
3. 存在一个元素 $1 \in G$，对所有的 $a \in G$ 均满足 $ao1 = 1oa = a$，这个元素称为中性元或单位元。
4. 对每个元素 $a \in G$，存在一个元素 $a^{-1} \in G$，满足 $aoa^{-1} = a^{-1}oa = 1$，则 a^{-1} 称为 a 的逆元。
5. 如果所有 $a,b \in G$ 都额外满足 $aob = boa$，则称群 G 为阿贝尔群或可交换群。

请注意，密码学中经常使用乘法群(即操作符“ o ”表示乘法)和加法群(即“ o ”表示加法)。后一种表示方法常用于椭圆曲线中，这在下面的章节将会看到。

示例 8.2 为了说明群的定义，请考虑以下示例。

- $(\mathbb{Z},+)$ 是一个群，即整数集 $\mathbb{Z}=\{\ldots,-2,-1,0,1,2,\ldots\}$ 与普通加法形成了阿贝尔群，其中 $e=0$ 是单位元，$-a$ 是 $a\in\mathbb{Z}$ 的逆。
- (不包括0的$\mathbb{Z},\cdot$) 不是一个群，即整数集 $\mathbb{Z}$ (不包括元素 0)和普通乘法不能形成群，因为除元素 -1 和 1 外，对于元素 $a\in\mathbb{Z}$，不存在逆元 a^{-1}。
- $(\mathbb{C},\cdot)$ 是一个群，即复数 $u+iv$ 的集合(其中 $u,v\in\mathbb{R}$ 且 $i^2=-1$)及定义在复数上的乘法

$$(u_1+iv_1)\cdot(u_2+iv_2)=(u_1u_2-v_1v_2)+i(u_1v_2+v_1u_2)$$

形成了一个阿贝尔群。此群的单位元为 $e=1$，元素 $a=u+iv\ \in\mathbb{C}$ 的逆元为

$$a^{-1}=(u-i)/(u^2+v^2)。$$

◇

然而，所有这些群在密码学中都不是很重要，因为密码学中通常需要的是拥有有限个元素的群。下面来看一个在 DHKE、Elgamal 加密、数字签名算法和其他很多密码学方案中都非常重要群 $\mathbb{Z}_n^*$。

定理 8.2.1

集合 $\mathbb{Z}_n^*$ 由所有 $i=0,1,\ldots,n-1$ 整数组成，其中满足 $\gcd(i,n)=1$ 的元素与乘法模 n 操作形成了阿贝尔群，且单位元为 $e=1$。

下面验证此定理的正确性，请看下面这个例子。

示例 8.3 如果选择 $n=9$，$\mathbb{Z}_n^*$ 由元素 $\{1,2,4,5,7,8\}$ 组成。

计算表 8-1 所示的 $\mathbb{Z}_9^*$ 的乘法表能方便地检查定义 8.2.1 中给出的绝大多数条件。条件 1(封闭性)是满足的，因为此表中的元素都在 $\mathbb{Z}_9^*$ 内。对这个群而言，条件 3(单位元)和条件 4(逆元)也成立，因为表中的每行和每列都是 $\mathbb{Z}_9^*$ 内元素的置换。根据主对角线的对称性，即第 i 行 j 列的元素与第 j 行 i 列的元素相等，可以看出，条件 5(交换性)也是满足的。条件 2(可结合性)不能从表的形状中直接得到，但可以根据 $\mathbb{Z}_n$ 内普通乘法的可结合性立即得到。

◇

最后，读者应该记住第 6.3.1 节中的内容，即每个元素 $a \in \mathbb{Z}_n^*$ 的逆元 a^{-1} 都可以通过扩展的欧几里得算法计算得到。

表 8-1 $\mathbb{Z}_9^*$ 的乘法表

× Mod 9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

8.2.2 循环群

在密码学中，我们总是关注有限的结构，比如 AES 需要一个有限域。下面将给出有限群的简单定义：

定义 8.2.2 有限群

一个群 $(G,\circ)$ 是有限的，仅当它拥有有限个元素。群 G 的基或阶可以表示为 $|G|$。

示例 8.4 有限群的示例有：

- $(\mathbb{Z}_n,+)$：$\mathbb{Z}_n$ 的基为 $|\mathbb{Z}_n| = n$，因为 $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$。
- $(\mathbb{Z}_n^*,\cdot)$：请记住，$\mathbb{Z}_n^*$ 是由小于 n 且与 n 互素的正整数组成的集合。因此，$\mathbb{Z}_n^*$ 的基等于 n 的欧拉函数，即 $|\mathbb{Z}_n^*| = \Phi(n)$。例如，群 $\mathbb{Z}_9^*$ 的基为 $\Phi(9) = 3^2 - 3^1 = 6$。前面提到的由 6 个元素 $\{1,2,4,5,7,8\}$ 组成的群的例子可以很好地验证这个结论。

◇

本节剩余部分将介绍一种特殊的群，叫循环群，它是基于离散对数密码体制的基础。首先来看以下定义：

定义 8.2.3　元素的阶

群 $(G,\circ)$ 内某个元素 a 的阶 $ord(a)$指的是满足以下条件的最小正整数 k：

$$a^k = \underbrace{a \circ a \circ \ldots \circ a}_{k次} = 1,$$

其中 1 是 G 的单位元。

下面通过示例来解释这个定义。

示例 8.5　本例的目的是确定群 $\mathbb{Z}_{11}^*$ 中 $a=3$ 的序。为此，我们必须不停地计算 a 的幂值，直到得到单位元 1 为止。

$$\begin{aligned}
a^1 &= 3 \\
a^2 &= a \cdot a = 3 \cdot 3 = 9 \\
a^3 &= a^2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \bmod 11 \\
a^4 &= a^3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \bmod 11 \\
a^5 &= a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \bmod 11
\end{aligned}$$

从最后一行可以得到 ord(3) = 5。

◇

如果将得到的结果一直乘以 a，就会发现一个非常有趣的现象。

$$\begin{aligned}
a^6 &= a^5 \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11 \\
a^7 &= a^5 \cdot a^2 \equiv 1 \cdot a^2 \equiv 9 \bmod 11 \\
a^8 &= a^5 \cdot a^3 \equiv 1 \cdot a^3 \equiv 5 \bmod 11 \\
a^9 &= a^5 \cdot a^4 \equiv 1 \cdot a^4 \equiv 4 \bmod 11 \\
a^{10} &= a^5 \cdot a^5 \equiv 1 \cdot 1 \equiv 1 \bmod 11 \\
a^{11} &= a^{10} \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11 \\
&\vdots
\end{aligned}$$

从这一点可以看出，a 的幂值一直在{3，9，5，4，1}序列中无限循环。这个循环行为引发出如下定义：

定义 8.2.4　循环群

如果群 G 包含一个拥有最大阶 $ord(\alpha)=|G|$的元素 α，则称这个群是循环群。拥有最大阶的元素称为原根(本原元)或生成元。

群 G 中拥有最大阶的元素 α 称为生成元，因为 G 中每个元素 a 都可以写成是这个元素的幂值 $\alpha^i = a$(i 为任意值)，即 α 产生了整个群。可以使用下面这个示例来验证这些属性。

示例 8.6 本例的目的是验证 $a = 2$ 是否为 $\mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$ 的本原元。请注意，该群的基为$|\mathbb{Z}_{11}^*| = 10$。下面来看由元素 $a = 2$ 的幂值生成的所有元素：

$$
\begin{array}{ll}
a = 2 & a^6 \equiv 9 \bmod 11 \\
a^2 = 4 & a^7 \equiv 7 \bmod 11 \\
a^3 = 8 & a^8 \equiv 3 \bmod 11 \\
a^4 \equiv 5 \bmod 11 & a^9 \equiv 6 \bmod 11 \\
a^5 \equiv 10 \bmod 11 & a^{10} \equiv 1 \bmod 11
\end{array}
$$

从最后一个结论可知，

$$\mathrm{ord}(a) = 10 = |\mathbb{Z}_{11}^*|。$$

这意味着(i)$a = 2$ 是本原元；(ii)$|\mathbb{Z}_{11}^*|$是一个循环群。

下面将验证 $a = 2$ 的幂值是否真的生成了群 $\mathbb{Z}_{11}^*$ 内的所有元素。首先仍然来看一下 2 的幂值生成的所有元素。

i	1	2	3	4	5	6	7	8	9	10
a^i	2	4	8	5	10	9	7	3	6	1

从最后一行可以看出，幂值 2^i 的确生成了群 $\mathbb{Z}_{11}^*$ 内的所有元素。同时可以注意到，这些数字的生成顺序看上去是毫无章法的。指数 i 与群元素之间看上去随机的关系是很多密码体制的基础，比如 Diffie-Hellman 密钥交换。

◇

从上面的例子可以看出，元素 2 为群 $\mathbb{Z}_{11}^*$ 中的生成元。需要强调的一点，在其他循环群 $\mathbb{Z}_n^*$ 中，数值 2 并不是必要的生成元。比如在 $\mathbb{Z}_7^*$ 中 ord(2)= 3，因此，元素 2 并不是这个群的生成元。

循环群具有一些有趣属性，其中对加密应用最重要的一个在下面定理中给出。

> **定理 8.2.2** 对每个素数 p，$(\mathbb{Z}_p^*,\cdot)$ 都是一个阿贝尔有限循环群。

这个定理说明了每个素数域的乘法群都是循环群。这个结论对密码学产生了深远影响，因为这些群对于构建离散对数密码体制非常重要。为了理解这些看上去很奇怪的定理的实用性，请注意这样一个事实：几乎所有的 Web 浏览器都内嵌了一个基于 $\mathbb{Z}_p^*$ 的密码体制。

定理 8.2.3

假设 G 为一个有限群，则对每个 $a \in G$ 都有：

1. $a^{|G|} = 1$
2. $ord(a)$可以整除$|G|$

第一个属性是费马小定理对所有循环群的一个推广。第二个属性具有很强的实用性，它指的是，循环群内所有元素的阶都可以整除群的基。

示例 8.7　下面再来看一下基为$|\mathbb{Z}_{11}^*| = 10$ 的群 $\mathbb{Z}_{11}^*$。此群内仅有的元素阶为 1、2、5 和 10，因为只有这些整数可以整除 10。下面可以通过观察该群中所有元素的阶来验证这个属性：

ord(1)= 1	ord(6)= 10
ord(2)= 10	ord(7)= 10
ord(3)= 5	ord(8)= 10
ord(4)= 5	ord(9)= 5
ord(5)= 5	ord(10)= 2

的确只出现了可以整除 10 的阶。

◇

定理 8.2.4　假设 G 为一个有限循环群，则下面的结论成立：

1. G 中本原元的个数为 $\Phi(|G|)$。
2. 如果$|G|$是素数，则所有满足 $a \neq 1 \in G$ 的元素 a 都是本原元。

上面的例子验证了第一个属性，因为 $\Phi(10) = (5-1)(2-1) = 4$，即本原元的个数为 4，分别是元素 2、6、7 和 8。第二个属性可以从前一个定理得到。如果群的基是素数，则唯一可能的元素阶就是 1 和基本身。由于只有元素 1 的阶为 1，其他所有元素的阶都是 p。

8.2.3 子群

本节主要介绍了(循环)群的子集，当然它们本身也是群；这样的集合也称为子群。为了验证某个群 G 的子集 H 也是一个子群，我们需要验证 H 是否满足第 8.2.1 节中给出的群定义的所有属性。如果该群是个循环群，则有一种简单的方法生成子群，方法如以下定理：

> **定理 8.2.5　循环子群定理**
>
> 假设 $(G,\circ)$ 是一个循环群，则 G 内每个满足 $ord(a)=s$ 的元素 a 都是拥有 s 个元素的循环子群的本原元。

这个定理告诉我们，循环群的每个元素都是其子群的生成元，而且该子群也是循环群。

示例 8.8　下面将通过 $G=\mathbb{Z}_{11}^*$ 的一个子群验证上面的定理。从前面的例子可知 ord(3)=5，根据定理 8.2.5，3 的幂值生成了子集 $H=\{1,3,4,5,9\}$。现在需要做的是通过观察其对应的乘法表(如表 8-2 所示)，验证这个集合是否真的是一个群。

表 8-2　子群 $H=\{1,3,4,5,9\}$ 对应的乘法表

×Mod 11	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

H 对乘法模数 11(条件 1)运算是封闭的，因为这个表是仅由 H 内的整数元素构成。显而易见，群操作是可结合且可交换的，因为它遵循的是普通乘法规则(分别对应条件 2 和 5)。中性素是 1(条件 3)，并且每个元素 $a\in H$ 均存在一个逆元 $a^{-1}\in H$ (条件 4)。这一点可以从表中看出：表的每行和每列都包含一个单位元。因此，H 是 $\mathbb{Z}_{11}^*$ 的一个子群(如图 8-1 所示)。

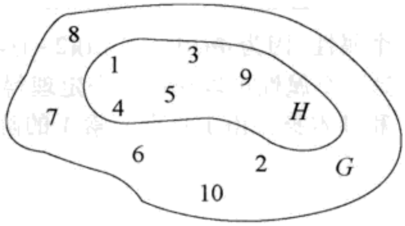

图 8-1　循环群 $G=\mathbb{Z}_{11}^*$ 的子群 H

更确切地讲，H 是一个阶为素数 5 的子群。需要注意的是，3 不是 H 唯一的生成元，它还有其他生成元 4，5 和 9，这个结论可以从定理 8.2.4 中得到。

◇

一种特殊情况就是阶为素数的子群。如果将该群的基数表示为 q，根据定理 8.2.4 可知，所有非 1 元素的阶都为 q。

根据循环子群定理可知，群 G 内的每个元素 $a \in G$ 都可生成某个子群 H。使用定理 8.2.3 可以得到下面定理。

定理 8.2.6　拉格朗日定理

假设 H 为 G 的一个子群，则$|H|$可以整除$|G|$。

下面来讨论拉格朗日定理的一个应用。

示例 8.9　循环群 $\mathbb{Z}_{11}^*$ 的基为$|\mathbb{Z}_{11}^*| = 10 = 1 \cdot 2 \cdot 5$。因此可以得到结论：$\mathbb{Z}_{11}^*$ 的子群对应的基为 1，2，5 和 10，因为这些数都是 10 可能的除数。$\mathbb{Z}_{11}^*$ 所有的子群 H 及这些子群的生成元 α 可以表示如下：

子　群	元　素	本原元
H_1	$\{1\}$	$\alpha = 1$
H_2	$\{1,10\}$	$\alpha = 10$
H_3	$\{1,3,4,5,9\}$	$\alpha = 3,4,5,9$

◇

本节最后一个定理全面描述了一个有限循环群对应的所有子群：

定理 8.2.7

假设 G 为一个阶为 n 的有限循环群，α 为对应的生成元，则对整除 n 的每个整数 k，G 都存在一个唯一的阶为 k 的循环子群 H。这个子群是由 $\alpha^{n/k}$ 生成的。H 是由 G 内满足条件 $a^k = 1$ 的元素组成的，且 G 不存在其他子群。

这个定理给出了从一个给定循环群构建子群的简单而直接的方法。我们只需一个本原元和群基数 n，然后计算 $\alpha^{n/k}$，即可得到拥有 k 个元素的子群的生成元。

示例 8.10 再次考虑循环群 $\mathbb{Z}_{11}^*$，从前面可知该群的本原元为 $\alpha = 8$。如果想要得到阶为 2 的子群的生成元 β，需要计算：

$$\beta = \alpha^{n/k} = 8^{10/2} = 8^5 = 32768 \equiv 10 \bmod 11 \text{。}$$

现在我们需要验证的确是元素 10 生成了拥有两个元素的子群：$\beta^1 = 10$，$\beta^2 = 100 \equiv 1 \bmod 11$，$\beta^3 \equiv 10 \bmod 11$，等等。

请注意：当然存在计算 $8^5 \bmod 11$ 的更简单方法，比如通过计算 $8^5 = 8^2 8^2 8 \equiv (-2)(-2)8 \equiv 32 \equiv 10 \bmod 11$。

◇

8.3 离散对数问题

在使用较大篇幅介绍了循环群后，读者也许想知道这与 DHKE 协议有什么关联。事实证明，DHKE 底层的单向函数，即离散对数问题(DLP)，可以直接使用循环群进行解释。

8.3.1 素数域内的离散对数问题

本节首先将介绍基于 $\mathbb{Z}_p^*$ 的 DLP，其中 p 为素数。

定义 8.3.1 基于 $\mathbb{Z}_p^*$ 的离散对数问题(DLP)

给定一个阶为 p-1 的有限循环群 $\mathbb{Z}_p^*$，一个本原元 $\alpha \in \mathbb{Z}_p^*$ 和另一个元素 $\beta \in \mathbb{Z}_p^*$。*DLP* 是确定满足以下条件的整数 x(其中 $1 \le x \le p-1$)的问题：

$$\alpha^x \equiv \beta \bmod p$$

从 8.2.2 节可知这样的整数 x 肯定存在，因为 α 是一个本原元，而每个群元素可以表示为任何本原元的幂值。这个整数 x 也称为以 α 为基的 β 的离散对数，可以正式地写作：

$$x = \log_\alpha \beta \bmod p$$

如果参数足够大的话，计算离散对数模一个素数是一个非常难的问题。因为指数运算

$\alpha^x \equiv \beta \bmod p$ 计算起来非常简单，这也形成了一个单向函数。

示例 8.11　考虑群 $\mathbb{Z}_{47}^*$ 内的离散对数，其中本原元为 $\alpha = 5$。对 $\beta = 41$ 的离散对数问题为：找到满足下面条件的正整数 x：

$$5^x \equiv 41 \bmod 47 。$$

即使使用这么小的数字，确定 x 也不是很容易。使用蛮力攻击，即系统地尝试所有可能的 x 值，可得到解 $x = 15$。

◇

在实际中，为了防止 Pohlig-Hellman 攻击(参考第 8.3.3 节)，群内 DLP 的基数最好是素数。由于群 $\mathbb{Z}_p^*$ 的基为 p-1，而这个数显然不是素数，所以人们常会选择 $\mathbb{Z}_p^*$ 子群中基为素数的子群内的 DLP，而非直接使用群 $\mathbb{Z}_p^*$ 本身。下面将用一个例子说明这个问题。

示例 8.12　群 $\mathbb{Z}_{47}^*$ 的阶为 46，因此，$\mathbb{Z}_{47}^*$ 中的子群对应的基有 23、2 和 1。$\alpha = 2$ 是拥有 23 个元素的子群的一个元素，因为 23 是一个素数，而 α 是子群内的本原元。$\beta = 36$(也在子群中)对应的一个可能的离散对数问题为：找到一个正整数 $x(1 \le x \le 23)$，使得

$$2^x \equiv 36 \bmod 47 。$$

利用蛮力攻击可以找到解 $x = 17$。

◇

8.3.2　推广的离散对数问题

使得 DLP 在密码学中尤其有用的一个特征就是，它并没有限制在乘法群 $\mathbb{Z}_p^*$(p 是一个素数)内，而是可以定义在任何循环群中。这也称为推广的离散对数(GDLP)问题，可以描述为：

定义 8.3.2　推广的离散对数问题

给定一个基为 n 的有限循环群 G，群操作为 $\circ$。考虑一个本原元 $\alpha \in G$ 和另一个元素 $\beta \in G$，则离散对数问题为：找到在 $1 \le x \le n$ 内的整数 x，满足：

$$\beta = \underbrace{\alpha \circ \alpha \circ \ldots \circ \alpha}_{x次} = \alpha^x$$

与 $\mathbb{Z}_p^*$ 内 DLP 的情况一样，这样的整数 x 一定存在，因为 α 是一个本原元，因此群 G 内的每个元素都可以通过 α 上重复使用群操作得到。

需要注意的一点是，有些循环群中的 DLP 并不是很困难的。这样的群就不能用于公钥密码体制，因为这样的群内的 DLP 并不是一个单向函数。请思考下面这个例子。

示例 8.13 这次将考虑整数模素数的加法群。例如，如果选择的素数为 $p = 11$，$G = (\mathbb{Z}_{11},+)$ 是本原元为 $\alpha = 2$ 的一个有限循环群。下面是 α 生成该群的过程：

i	1	2	3	4	5	6	7	8	9	10	11
$i\alpha$	2	4	6	8	10	1	3	5	7	9	0

现在我们将试图求解元素 $\beta = 3$ 的 DLP，即必须计算整数 $1 \le x \le 11$ 中，满足以下条件的 x：

$$x \cdot 2 = \underbrace{2+2+\ldots+2}_{x\text{次}} \equiv 3 \bmod 11$$

以下是针对此 DLP 的攻击方式。尽管群操作为加法，但是 α, β 及离散对数 x 之间的关系也可以用乘法来表示：

$$x \cdot 2 \equiv 3 \bmod 11\text{。}$$

为了求解 x，可以简单地将本原元 α 求逆：

$$x \equiv 2^{-1} 3 \bmod 11$$

根据扩展的欧几里得算法就可以计算 $2^{-1} \equiv 6 \bmod 11$，然后就可得到离散对数为：

$$x \equiv 2^{-1} 3 \equiv 7 \bmod 11\text{。}$$

这个离散对数可以从上面给出的小表中验证。

上面的技巧可以推广到 n 为任意值，且元素 $\alpha, \beta \in \mathbb{Z}_n$ 的任何群 $(\mathbb{Z}_n, +)$ 中。因此，我们可以得到这样一个结论：在 $\mathbb{Z}_n$ 上计算推广的 DLP 会非常简单。这里能非常容易求解 DLP 的原因在于，其中有些数学操作都不在加法群里，即乘法和逆元。

◇

介绍完这个反例后，现在我们列出了密码学中推荐使用的一些离散对数问题：

(1) 素数域 $\mathbb{Z}_p$ 的乘法群或其子群。例如古典 DHKE、Elgamal 加密或数字签名算法(DSA)都使用了这个群，它们也是最古老且使用最广泛的几种离散对数系统。

(2) 椭圆曲线构成的循环群。椭圆曲线密码体制将在第 9 章中介绍，它们在过去几十年