

RSA加密体制破译报告

2016全国高校密码数学挑战赛

◀ 双河安团队

2016 年全国高校密码数学挑战赛

答题卷

作品名称：RSA 加密体制破译报告——双河安团队答题卷

指导老师：程庆丰

参赛学员：韩旭 李钰汀 张兴隆

摘 要

RSA 密码算法是当今使用最广泛的公开密钥密码体制。它是利用大数分解的困难性而设计的一种公钥密码算法，凭借其安全性高、体制成熟完善、计算可行性高等优势在公钥密码体制中独树一帜，并在计算机通信、企业身份认证等商业领域得到了广泛的应用。

本文对 21 个片段的加密数据进行了细致的观察与分析，采用 **Fermat** 分解法和 $p-1$ 分解法成功分解了 **Frame2**、**Frame6**、**Frame10** 和 **Frame19** 的模数并由此得到了正确的明文消息；使用公共模数攻击法和低加密指数攻击法找到了存在某些安全缺陷的消息片段，成功破译了 **Frame0**、**Frame3**、**Frame4**、**Frame8**、**Frame12**、**Frame16** 和 **Frame20** 的明文消息；借鉴因数碰撞的思想，用欧几里德算法遍历所有模数，求出 **Frame1** 和 **Frame18** 的模数的公因数，进而成功分解了 **Frame1** 和 **Frame18** 的模数得到正确的加解密参数，破译了明文消息；利用已经得到的若干明文片段，通过查阅资料、语义分析等方法，采用猜测明文攻击，得到了其余分片的所有明文，并验证了其正确性；利用已得到的若干个素数参数，找到了随机数生成的规律，从而破解了所有分片的加解密参数（具体结果见附录），并对其正确性进行了验证。

目 录

| | |
|-------------------------------|-----------|
| 1. 理论分析报告 | 1 |
| 1.1 RSA 密码体制的发展历程..... | 1 |
| 1.2 常见攻击方法..... | 5 |
| 1.3 相关理论基础..... | 7 |
| 1.3.1 费马(Fermat)分解法..... | 8 |
| 1.3.2 Pollard $p-1$ 分解法 | 8 |
| 1.3.3 低加密指数攻击原理..... | 8 |
| 1.3.4 公共模数攻击..... | 10 |
| 1.3.5 欧几里德(Euclid)算法 | 10 |
| 1.3.6 扩展的欧几里德算法..... | 11 |
| 1.3.7 随机数发生器..... | 11 |
| 1.4 解题思路..... | 15 |
| 1.4.1 初步攻击尝试..... | 15 |
| 1.4.2 因数碰撞法求两个模数的最大公因数..... | 18 |
| 1.4.3 猜测明文攻击..... | 19 |
| 1.4.4 寻找随机数生成规律..... | 19 |
| 2. 实验数据报告 | 21 |
| 2.1 实验环境..... | 21 |
| 2.1.1 符号说明..... | 21 |
| 2.1.2 硬件设备..... | 21 |
| 2.1.3 软件工具..... | 22 |
| 2.2 常用攻击方法..... | 24 |

| | | |
|-----------|------------------------------|-----------|
| 2.2.1 | 费马分解法..... | 24 |
| 2.2.2 | Pollard $p-1$ 分解法 | 27 |
| 2.2.3 | 低加密指数攻击..... | 31 |
| 2.2.4 | 公共模数攻击..... | 35 |
| 2.3 | 因数碰撞法的意外发现..... | 36 |
| 2.4 | 猜测明文攻击还原全部明文..... | 40 |
| 2.5 | 还原随机数发生器..... | 42 |
| 2.6 | 结果检验..... | 66 |
| 3. | 小结 | 67 |
| 3.1 | 解题方法总结..... | 67 |
| 3.2 | 结果分析..... | 68 |
| | 参考文献 | 70 |
| | 附 录 | 72 |
| | 附录 1 明文信息..... | 72 |
| | 附录 2 通讯序号与接受序号对照表..... | 73 |
| | 附录 3 RSA 加解密参数表（16 进制） | 74 |
| | 附录 4 RSA 加解密参数表（10 进制） | 95 |

1. 理论分析报告

1.1 RSA 密码体制的发展历程

2014 年 2 月 27 日，习近平总书记主持召开中央网络安全和信息化领导小组第一次会议并发表了重要讲话，强调了网络安全和信息化的重要性。2016 年 4 月 19 日，习近平主持召开网络安全和信息化工作座谈会，提出推动网信事业发展，在核心技术有所突破。网络空间安全上升至国家战略层面，信息化时代的实力较量已迫在眉睫。

密码学作为网络空间安全的重要组成部分，其起源十分古老，目前正在蓬勃发展并得到有效应用。它综合了数学基础理论、计算机科学、网络技术、信息论等跨领域的专业知识。从公元前古希腊斯巴达出现的 Scytale，到古罗马帝国著名的凯撒密码；从一战时期的“齐默尔曼电报”，到二战时 Enigma 的破译，密码技术在人类社会中得到了越来越广泛的应用。在密码学的发展过程中，古今中外的专家学者们克服了重重困难，不断突破现有的理论，取得了众多丰硕的研究成果。

公钥密码体制作为当今应用最广泛的加密体制，在网络空间安全领域占有重要的一席之地，它与分组密码和杂凑函数一起，为电子商务应用提供了基础密码模块，与我们的日常生活、商业应用、数据保护等息息相关。而在公钥密码算法中，RSA 加密体制算法是目前最有影响力的加密算法，它能够抵御目前为止已知的绝大多数密码攻击。

1976 年，Whitfield Diffie 和 Martin Hellman^[1]发表了“密码学的新方向”一文，首次提出了公开密钥体制（简称为“公钥密码”）的思想，介绍了公钥加密和数字签名的新构想，自此，开启了密码学历史上一场伟大的变革。2016 年 3 月 2 日，美国计算机协会(ACM)宣布授予两位伟大的密码研究专家 Whitfield Diffie 和 Martin Hellman 2015 年的 ACM 图灵奖，他们对密码学的杰出贡献得到了世人的认可。

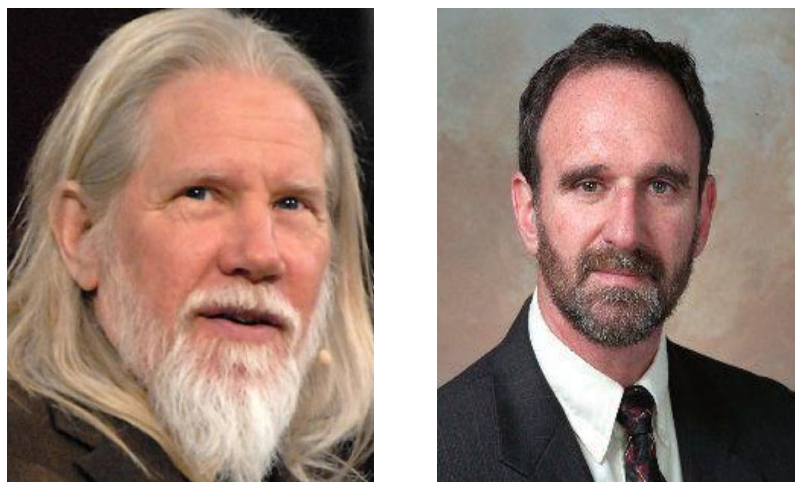


图 1.1 Whitfield Diffie 和 Martin Hellman

公钥密码体制（也称非对称加密体制）如今已成为大多数互联网安全应用的基础，是一种无需事先共享密钥就可以在两个用户之间安全地传送信息的方法，不同于通信双方必须提前商定密钥的对称加密算法。公钥密码的提出被视为是现代密码学的开端，具有划时代的意义。

公钥密码最大的优点是不需要通过安全渠道传递密钥，其公开一个密钥、隐藏另一个密钥的特点大大简化了密钥管理。两个用户采用公钥密码通信时，消息接收者可以完全公开加密规则与加密密钥，只保留解密密钥，任何想要向该用户发送消息的人只需用它公开的加密密钥，按照加密规则对信息进行加密，发送给该用户即可；只有该用户拥有的解密密钥才能恢复明文信息，无须担心消息被中

途截获。另外，该用户用解密密钥可以制作电子签名，由公开的加密密钥来验证，保证了签名来源的唯一性，有效防止了中间人的攻击，同时具备抗抵赖特性。

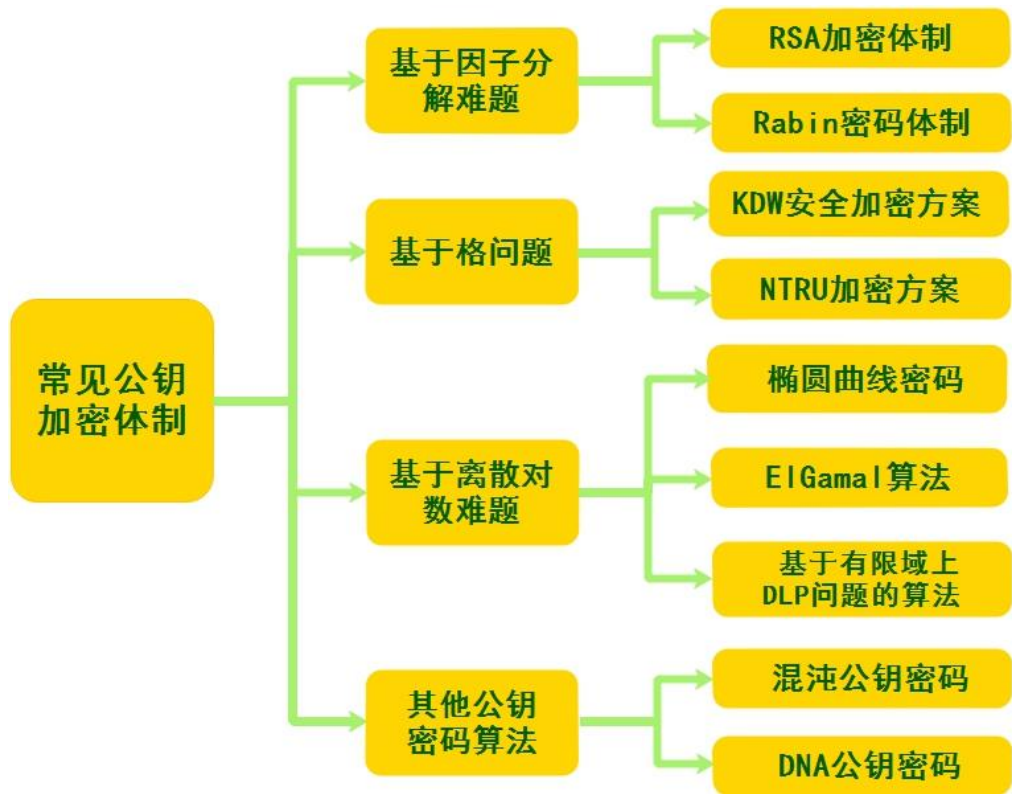


图 1.2 常见公钥加密体制

但是，由 Whitfield Diffie 和 Martin Hellman 最初所提出的 MH 背包算法于 1984 年被破译，因而失去了实际意义。真正有生命力的公开密钥加密系统算法是由 Ronald Rivest、Adi Shamir 和 Leonard Adleman^[2]共同设计的 RSA 算法。他们的研究成果在 1977 年 4 月以“数字签名和公开密钥密码体制”为题公开发表，引起了密码学界的广泛关注，并受到高度评价。

几十年来，RSA 密码体制经历了各种攻击和考验，不断成熟完善，逐渐为人们所接受，并以其利于理解与操作、安全性高的优点，迅速影响了全世界的加密算法发展与应用进程。

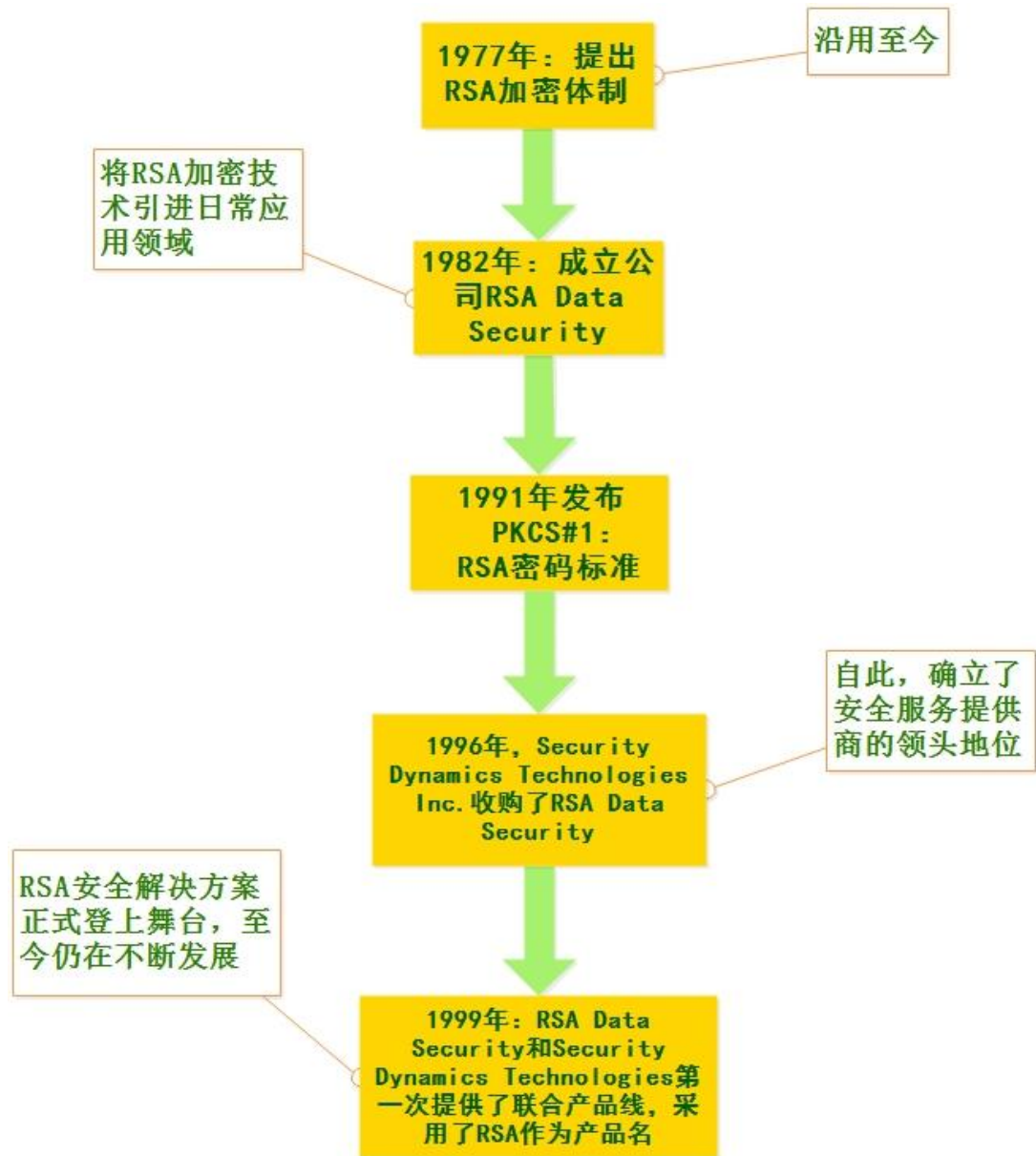


图 1.3 RSA 的起源与发展

RSA 加密算法的主要特点在它能够提供两种不同的密钥，所有使用者共用公钥，只有持有对应私钥的用户才能解密。这两个密钥之间存在着相互依存关系：即用其中任一个密钥加密的信息只能用另一个密钥进行解密。若以公钥作为加密密钥，以用户专用密钥（私钥）作为解密密钥，则可实现多个用户加密的信息只能由一个用户解读。依据此原理，RSA 算法可用于文件加密。

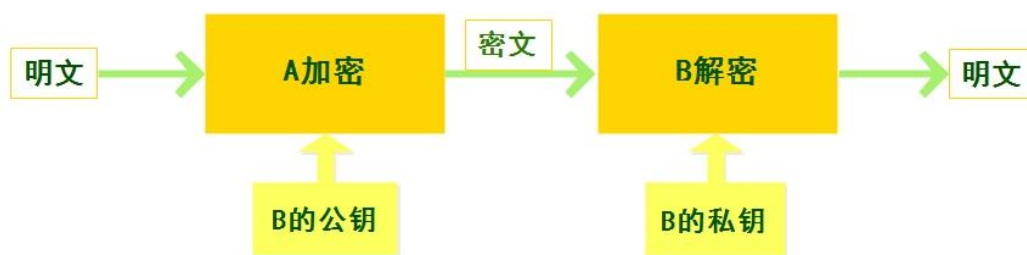


图 1.4 加解密过程

1.2 常见攻击方法

虽然 RSA 密码体制在理论上是安全的，但是在实际应用中，现实条件的制约和个人操作的失误往往会导致 RSA 密码系统产生不同的缺陷^[3]。这就给攻击者以可乘之机。

下面列举了几种常用的攻击方法：



图 1.5 常见攻击方法

从上图可以看出，针对 RSA 密码系统的攻击，尤其是分解因子的手段，国内外研究方法逐步从传统的纯数学方法演变成数学和物理技术相结合的方法（例如各种侧信道攻击技术），更加实用、高效^[4]。图 1.6 总结了近年来世界各国对 RSA 攻击技术的研究方向：

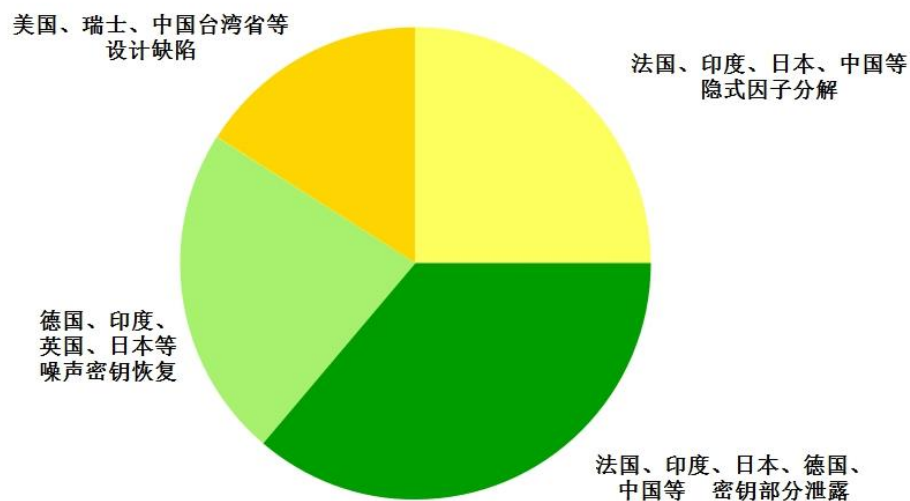


图 1.6 近年来各国针对 RSA 攻击技术的研究

RSA 加密算法理论基于简单的数论基础——两个大素数相乘是非常简单的，但是如果对两个素数的乘积做因式分解是非常困难的^[5]。以目前计算机的计算能力能成功分解的大数长度是有限的。刚开始的 RSA 密码算法采用的模数长度大多数为 512bit；直到 1999 年，使用 512bit 长度的模数的 RSA 密码算法被一台 Cray 超级电脑攻破，耗费近 8 个月时间；10 年之后，768bit 模数的 RSA 密码算法被攻破，所需时间是分解 512bit 的数千倍；而分解 1024bit 模数所需时间则是 768bit 的一千多倍，因此，在短时间内，1024bit 长度的模数仍然是安全的。

表 1.1 攻击进展

| 时间 | 被分解的模数 |
|----------------|---------|
| 1993.9-1994.4 | RSA-129 |
| 1999.1-1999.8 | RSA-155 |
| 2003.12 | RSA-160 |
| 2003.12-2005.5 | RSA-200 |
| 2005.11 | RSA-640 |
| 2009.12 | RSA-768 |
| 2013.9 | RSA-210 |

RSA 密钥长度随着保密级别提高，增加十分迅速。表 1.2 列出了对同一安全级别下不同算法所对应的密钥长度。

表 1.2 密钥长度与安全级别

| 对称密钥长度(bit) | RSA 密钥长度(bit) | ECC 密钥长度(bit) | 保密年限 |
|-------------|---------------|---------------|------|
| 80 | 1024 | 160 | 2010 |
| 112 | 2048 | 224 | 2030 |
| 128 | 3072 | 256 | 2040 |
| 192 | 7680 | 384 | 2080 |
| 256 | 15360 | 512 | 2120 |

1.3 相关理论基础

密码学是以数学学科为基础理论、以计算机科学为实现工具而形成的具有自己特色理论体系的一门科学。本节介绍了攻击 RSA 密码体制的方法所依赖的核心理论内容，并在之后的解题过程中有所应用与涉及。

1.3.1 费马(Fermat)分解法

为了降低模数 N 被试除法攻破的可能性, 算法设计者通常选择具有相同比特大小的参数 p 和 q , 然而, 如果 p 和 q 太过接近, 就可以利用费马分解法找到它们。

费马分解法基于如下思想: 设 $N = pq$, 其中 $p \leq q$ 都是奇数, 然后令 $x = \frac{1}{2}(p+q)$, $y = \frac{1}{2}(q-p)$, 可以找到 $N = x^2 - y^2 = (x+y)(x-y)$ 或 $y^2 = x^2 - N$ 。

定理 1 设 $N = pq$, 其中 $p > q$ 且 $\Delta = p - q$, 则当 $\Delta < N^{\frac{1}{4}}$ 时, 费马分解法可以有效地分解 N 。

1.3.2 Pollard $p-1$ 分解法

RSA 加密算法中, 素数 p 和 q 应该满足: $p \pm 1$ 和 $q \pm 1$ 至少有一个素因子大于 10^{20} , 否则, 要分解的整数 N 有一个素因数 p , 且 $(p-1)$ 有小的素因数时就可以利用 Pollard $p-1$ 分解法有效分解模数 N , 从而得到 p 。

设 $N = pq$, 其中 p, q 为两个不同素数。选取一个整数 k 使其满足 $(p-1) | k!$, 根据欧拉定理, 对任意与 p 互素的整数 g 可以得到 $g^{p-1} \equiv 1 \pmod{p}$, 因此, 有 $g^{k!} \equiv 1 \pmod{p}$, 即: $p | g^{k!} - 1$; 又由于 $p | n$, 因此 $p | ((g^{k!} \bmod n) - 1)$ 。但是, 如何选取 k 是该算法中的关键问题, 如果 k 选取太小, 则可能不满足关系 $p-1 | k!$; 如果 k 选取太大 (比如令 $k = p-1$), 算法执行的复杂度就会急剧加大。因此, 在执行算法前, 先对可能满足关系 $p-1 | k!$ 的 k 进行猜测, 并根据计算能力进行设定。

1.3.3 低加密指数攻击原理

在设计算法时为了加速计算, 常常使用较小的加密指数 e , 但是这种做法存

在很大的安全隐患。如果相同的消息使用同样的加密指数加密后发送给不同的接收者，则该明文消息可以被非常有效的恢复。该攻击方法基于著名的中国剩余定理。

定理 2（中国剩余定理） 设 m_0, \dots, m_{k-1} 是两两互素的正整数，对任意整数 a_0, \dots, a_{k-1} ，一次同余方程组

$$x \equiv a_i \pmod{m_i}, \quad 0 \leq i \leq k-1,$$

必有解，且解数唯一。这个唯一解是

$$x \equiv M_0 M'_0 a_0 + \dots + M_{k-1} M'_{k-1} a_{k-1} \pmod{m},$$

其中

$$m = m_0 \cdots m_{k-1} = m_i M_i \quad (0 \leq i \leq k-1),$$

以及

$$M_i M'_i \equiv 1 \pmod{m_i} \quad (0 \leq i \leq k-1)。$$

假设有三组密文是由同一明文、同一加密密钥加密得到，则根据该定理可以有效地还原其明文。设密钥 $e_1 = e_2 = e_3 = 3$ ，可列出同余方程组：

$$\begin{cases} c_1 \equiv m^3 \pmod{N_1} \\ c_2 \equiv m^3 \pmod{N_2} \\ c_3 \equiv m^3 \pmod{N_3} \end{cases}$$

对下面同余系统应用中国剩余定理：

$$\begin{cases} m^3 \equiv c_1 \pmod{N_1} \\ m^3 \equiv c_2 \pmod{N_2} \\ m^3 \equiv c_3 \pmod{N_3} \end{cases}$$

得到：

$$\begin{aligned}
m^3 &\equiv c_1 \cdot (N_2 \cdot N_3) \cdot ((N_2 N_3)^{-1} \bmod N_1) + \\
&c_2 \cdot (N_1 \cdot N_3) \cdot ((N_1 N_3)^{-1} \bmod N_2) + \\
&c_3 \cdot (N_1 \cdot N_2) \cdot ((N_1 N_2)^{-1} \bmod N_3) \pmod{N_1 \cdot N_2 \cdot N_3}
\end{aligned}$$

所以：

$$m = (m^3)^{\frac{1}{3}}。$$

1.3.4 公共模数攻击

RSA 加密中的四个参数 $\{d, p, q, \phi(N)\}$ 是同等重要的，任何一个参数泄露都会给其余三个的安全性带来威胁。但是，如果在 RSA 加密中使用相同的模数，那么有可能在不知道四个参数知识的情况下，攻击得到 RSA 加解密体制参数。

定理3 设 $N_1 = N_2$ 、 $m_1 = m_2$ 、 $e_1 \neq e_2$ ，且 $\gcd(e_1, e_2)$ 满足：

$$\begin{cases} c_1 \equiv m^{e_1} \pmod{N} \\ c_2 \equiv m^{e_2} \pmod{N} \end{cases}$$

则可以容易地恢复 m ；即

$$\{[c_1, e_1, N], [c_2, e_2, N]\} \xRightarrow{P} \{m\}。$$

证明 因为 $\gcd(e_1, e_2) = 1$ ，因此可用扩展欧几里德算法在多项式时间内找到

$x, y \in \mathbb{Z}$ 使得

$$e_1 x + e_2 y = 1。$$

因而，

$$\begin{aligned}
c_1^x c_2^y &\equiv (m_1^{e_1})^x (m_2^{e_2})^y \\
&\equiv m^{e_1 x + e_2 y} \\
&\equiv m \pmod{N}。
\end{aligned}$$

1.3.5 欧几里德(Euclid)算法

欧几里德算法又称辗转相除法，是数论和代数学中的重要方法。其思想方法

在数学的许多分支都有重要的应用。利用欧几里德算法可以求出若干个整数之间的最大公因数，可以直接用于求解一次不定方程^[6]。

定理 4 (Euclid 算法) 设 a 、 b 是给定的两个整数， $b \neq 0$ ，且 b 不能整除 a ，重复应用带余除法得到下面 $k+2$ 个等式：

$$a = q_0 b + r_0, \quad 0 < r_0 < |b|,$$

$$b = q_1 r_0 + r_1, \quad 0 < r_1 < r_0,$$

$$r_0 = q_2 r_1 + r_2, \quad 0 < r_2 < r_1,$$

.....

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}, \quad 0 < r_{k-1} < r_{k-2},$$

$$r_{k-2} = q_k r_{k-1} + r_k, \quad 0 < r_k < r_{k-1},$$

$$r_{k-1} = q_{k+1} r_k.$$

1.3.6 扩展的欧几里德算法

扩展的欧几里德算法是在已知整数 a 、 b 的情况下，可以在求得它们的最大公约数的同时，能够找到整数 x 、 y （其中一个很可能是负数），使它们满足等式：

$$ax + by = \gcd(a, b).$$

定理 5 已知两个非负整数 a 和 b ， $\gcd(a, b)$ 表示 a 和 b 的最大公约数，则必然存在整数对 (x, y) ，使得：

$$ax + by = \gcd(a, b).$$

1.3.7 随机数发生器

在 RSA 密码算法的设计中，素数的生成是一个关键的环节。一般来说，产生一个素数的过程是：先生成一个符合要求的随机数，通过素性检测判断其是否

为素数，若是素数，则输出该数；若不是素数，那么再生成一个随机数，直到通过素性检测为止。因此，素数发生器实质上是一个随机数发生器。

1927 年，剑桥大学出版社出版了一张列昂纳德·提珀特随机排列的 41600 个随机数字的表，这是世界上第一张公开发表的随机数表。在这张表出版仅十年之后，提珀特的四万个随机数表对于很大的抽样实验已不够用。1938 年，数学家费歇尔和雅特斯发表了 15000 个补充随机数字；1939 年肯德尔和巴秉顿发表了一张包含 100000 个随机数字的表；1949 年洲际贸易委员会(ICC)发表了一张由一个被称为复合随机化过程生成的 105000 个随机数字的表。随后人们开始寻求新的方法来大量产生符合要求的随机数以满足日益增长的需要。



图 1.7 随机数发生器的种类

以下为常见的一些随机数发生器。

1) 平方取中生成器

平方取中的方法是最早的伪随机数算法之一，由冯诺尼曼提出。其算法首先

给出一个 $2r$ 为数作为种子，取其中间的 r 位作为第一个伪随机数，然后将第一个随机数平方构成一个新的 $2r$ 位的数，再取中间的 r 为作为第二个伪随机数，以此类推。其递推公式表示为：

$$X_n = X_{n-1}^2 \bmod 2^r。$$

该方法生成的随机数存在均匀性不好，周期依赖于输入种子的值，容易通过大量的随机序列得到循环规律，从而分析得到全部序列。

2) 移位寄存器

移位寄存器由 Tausworthe 在 1965 年提出，它由串联的 n 个二元域上的寄存器及一个反馈函数构成。其通过反馈函数计算出寄存器下一比特信息，然后移寄存器进行移位输出，一个线性移位寄存器的基本结构如图 1.8 所示：

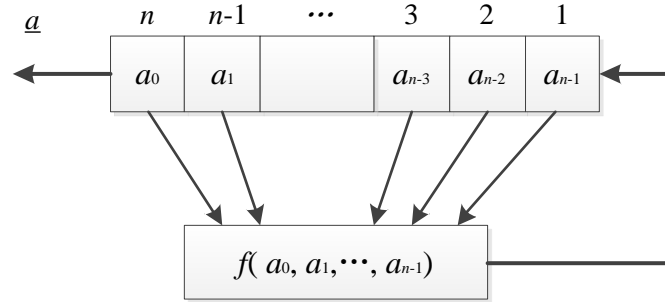


图 1.8 线性移位寄存器基本结构

推移公式为：

$$f(a_i, a_{i+1}, \dots, a_{i+n-1}) = a_{i+n}，$$

在选择合适的反馈函数时，线性移位寄存器生成的序列能够表现出非常好的特性。当 n 级线性移位寄存器的反馈函数为 n 次本原多项式时，所生成的序列称为 m 序列，其具有良好的 0-1 分布、游程分布特征，序列周期上也达到了最大的 $2^n - 1$ 。

线性移位寄存器是移位寄存器最基本的结构，使用非线性的反馈函数、添加

非线性前馈、使用多个线性反馈寄存器的组合等多种方式来实现复杂的移位寄存器结构，将使移位寄存器产生的伪随机序列的结构变得更加复杂，难以分析。

然而对于一般的线性移位寄存器而言，其线性的递推结构使得伪随机序列的分析并不困难，特别在获得连续 $2n$ bit 序列信息时，能够利用代数方法求解得到线性移位寄存器的结构信息。

3) 线性同余生成器

线性同余生成器由 Lehmer 在 1951 年提出此方法利用数论中的同余运算来产生随机数，故称为同余生成器，是使用最广的随机数发生器之一。其计算公式为：

$$X_n = aX_{n-1} + b \bmod m,$$

- ①当 $a=1$ 并且 $b \neq 0$ 时，此同余生成器称为乘法同余生成器；
- ②当 $a \neq 1$ 并且 $b=0$ 时，此同余生成器称为加法同余生成器；
- ③当 $a \neq 1$ 并且 $b \neq 0$ 时，此同余生成器称为混合同余生成器。

线性同余生成器可以在一维空间中产生较好的随机数，但在二维或更高维的空间中线性同余生成器的均匀性较差。在参数 a 、 b 、 m 的选取满足下述条件时，其可以获得满周期的随机数：

- ① b 与 m 互素；
- ②对于 m 的每一个质因数 p ， $a-1$ 为 p 的倍数；
- ③若 m 能够被 4 整除，则 $a-1$ 也可被 4 整除。

4) 非线性同余生成器

非线性同余生成器是从线性同余生成器发展而来，其递推关系式同样使用同余式，但不同的是使用了非线性的函数，其递推公式为：

$$X_n = f(X_{n-1}) \bmod m,$$

其中 f 为非线性函数，一般可以使用高次多项式构成二次或更高次的同余生成器，使用逆函数构成逆同余发生器，使用指数函数构成指数同余发生器，也可以使用各种组合方式构成结构更为复杂的非线性同余发生器。

1.4 解题思路

本问题是一个传统的 RSA 密码体制破译问题。题目中已知明文的加密规则，并截获了所有的加密指数 e 、模数 N 和密文 c ，要求据此求出解密指数 d 、素数 p 、 q 并最终恢复全部的明文 m 。

本题中，模数 N 的长度为 1024bit，对其准确快速地进行素数分解仍然是一个较大的难题。就目前的计算机水平来说，1024bit 长度的模数是基本安全的，2048bit 的模数是绝对安全的。直接对 1024bit 的模数进行因数分解在操作可行性上存在很大困难，然而对于某些存在不安全的 RSA 加解密体制参数，我们可以用特定的攻击方法，针对其中隐藏的安全缺陷进行破译。

根据题目中加密帧数据的格式分离出每个片段的模数 N 、加密指数 e 和密文 c 。其中，明文分成 8 个字符后进行加密，每一分片较短，符合猜测明文攻击的条件；有三组加密指数 e 同为 3，有五组加密指数 e 同为 5，存在明文片段相同的可能性，可以尝试公共模数攻击法对其进行破解；素数 p 、 q 中至少有一个是由随机数发生器生成的，若能找到随机数生成的规律，就可以破解全部加解密参数。

1.4.1 初步攻击尝试

关于 RSA 密码系统的攻击方法，人们首先想到的就是分解模数。然而，当模数超过 512bit 时，对其进行分解是一件非常困难的事情。通过查阅文献资料，

总结前人经验，我们考虑了一些 RSA 加密系统可能存在的一些隐藏缺陷：如模数生成时选择了不安全的素数，明文片段之间可能存在的联系等等。对此，我们可以用一些针对特定系统缺陷的攻击方法，尝试对模数进行分解，对明文消息进行破译。

1) 费马分解法

观察题目，可以发现一句提示“如果参数选取不当，同样存在被破译的可能”，由此，我们猜测，在 21 组模数中，必然有存在安全缺陷的参数，故可以尝试整数分解法进行攻击。

费马分解法在两个素数 p 、 q 十分相近的情况下，可以有效地对模数 N 进行分解。所以，可以考虑采用费马分解法对所有的模数进行攻击，若存在满足条件的模数，就可以成功破译。

2) Pollard $p-1$ 分解法

思路同上，若某个模数 N 的素因数为 p ， $p-1$ 存在小因数，则可以用 Pollard $p-1$ 分解法破解该模数 N 。根据算法原理，通过编程实现，对每个模数进行攻击尝试，若存在满足攻击条件的数，就能够有效破解。

3) 低加密指数攻击

查阅相关文献后我们了解到：相同的明文消息 m 采用同一公钥 e 和不同模数 N 加密后得到根据不同的密文 c ，应用中国剩余定理求解同余式组，可以有效地恢复明文消息。其中，对于不同的模数 N ，要求它们的最大公因数为 1，且模数 N 的个数与公钥 e 的值相同。

通过对所截获加密帧数据的观察，我们发现：在 21 个片段中，有些片段中的加密密钥是相同的，具体如下：Frame7、Frame11 和 Frame15 这 3 个分片均使

用“3”作为加密密钥；Frame3、Frame8、Frame12、Frame16 和 Frame20 这 5 个分片均使用“5”作为加密密钥，通过验证，这两组消息分片中的模数各自互素。如果这两组数据是由相同的明文片段加密得到的，那么它们就完全符合低加密指数攻击条件。所以，我们假设这两组数据均符合条件，尝试低加密指数攻击法进行破译。

下面，分别对两组消息片段进行破译并验证。

(1)对 Frame7、Frame11 和 Frame15 的攻击

①初次尝试

假设 Frame7、Frame11 和 Frame15 三个片段存在相同的明文，基于该攻击方法的原理，可以对其进行有效攻击，得到有意义的明文消息。

然而在攻击过程中，通过 C++语言进行编程实现，最终得到的结果并不符合题目中对明文消息格式的要求，且毫无语义。因此，本次攻击没有成功。说明这三组消息的明文可能并不完全相同，才导致攻击失败。

②算法改进

仔细研究该攻击方法的原理，我们发现：其所需的消息个数并非一定要等于公钥值的大小，即不要求模数 N 的个数与公钥 e 的值相同；起决定作用的是 m^e 与 $N_1 \cdots N_k$ 的大小关系（ N_1, \dots, N_k 为加密时所用消息的模数）。当 m^e 小于 $N_1 \cdots N_k$ 时，可以对其进行有效攻击。

观察题目中明文格式和模数格式的要求：明文长度固定为 512bit，模数长度固定为 1024bit，针对 $e=3$ 的攻击情形， $|m^3|=1536$ 远小于任意两个模数的乘积，因此针对 Frame7、Frame11 和 Frame15 的攻击，只要其中任意两个消息存在相同明文，即可进行有效攻击。

通过改进后的攻击算法，依然未能获得正确的明文消息，因此可得出结论：这三个消息的明文片段均不相同。

(2)对 Frame3、Frame8、Frame12、Frame16 和 Frame20 的攻击

借鉴上述改进后的算法思想，先对 m^e 与 $N_1 \cdots N_k$ 的大小关系做出判断。通过计算可得知：当 $e=5$ 时，只需存在 3 个消息拥有相同的加密明文即可实施有效攻击。

通过编程实现，对任意 3 个消息片段进行计算均可得到有效的明文消息，且得到的这些明文均相同。由此，破解得到 Frame3、Frame8、Frame12、Frame16 和 Frame20 这 5 个消息的明文片段，并证明这 5 个消息由同一明文片段加密所得。

4) 公共模数攻击

当系统中不同的消息共用一个模数 N ，只有 e 和 d 不同，系统将是危险的，此时，攻击者可能无需分解 N 就能够恢复明文。

通过观察加密帧数据，我们已经知道 Frame0 与 Frame4 中的模数 N 是相同的，若这两个消息存在相同的明文，则可以使用共模攻击的方法进行有效攻击。

根据共模攻击的原理，通过编程实现对 Frame0 和 Frame4 进行攻击测试，最终得到了符合明文格式要求，且具有语言意义的明文消息。

1.4.2 因数碰撞法求两个模数的最大公因数

通过阅读 Joppe W. Bos、Alex Halderman 和 Nadia Heninger 等人^[7]所著“Elliptic Curve Cryptography in Practice”一文，我们发现了一个巧妙的想法——从求任意两个模数的最大公因数入手，实现对大整数的因数分解。若某两个数的最大公因数为 1，则说明这两个数互素；若最大公因数大于 1，则说明该最大公因数同为这两个模数的一个因数，可以分别进行除法运算，进一步求出两个模数

的另一个因数，即间接实现了大数分解。与费马分解法和 $p-1$ 分解法相比，这种方法在运算效率方面有显著优势，计算可行性更强。

在实现过程中，我们采用欧几里得算法，对 21 个模数 N 两两求最大公因数，需要计算 C_{21}^2 次，即 210 次，其中，Frame0 与 Frame4 中的模数 N 是相同的，不予考虑，计算余下的 209 组模数 N ，可得到结果：Frame1 与 Frame18 中的两个模数 N 存在不为 1 的最大公因数，进而成功地对 Frame1 的模数与 Frame18 的模数进行分解，得到重要参数 p 和 q ，并依此计算出 $\varphi(N)$ ，再由公钥 e 计算得到私钥 d 。最终，使用私钥 d ，根据解密算法得到明文消息，即可最终实现对密文的完全破解。对得到的明文消息进行加密验证，与所截获密文消息完全相同。

至此，完成了对 Frame1 与 Frame18 的完全破解，得到了有意义的明文消息与 RSA 体制参数 p 和 q 。

1.4.3 猜测明文攻击

目前我们已经将现有条件下所能实现的全部常见攻击方法进行了试验，共得到了 13 个分片的明文，不考虑重复发送的消息，有 8 个片段的明文数据。根据已有的关键信息，通过查阅相关文献资料和互联网搜索，采用语义分析与加密验证相结合的方法，最终恢复了全部明文信息。

1.4.4 寻找随机数生成规律

仔细阅读题目，我们发现，题目中提到“素数 p 由某一随机数发生器生成”和“素数 q 可以随机选择，也可以由 2) 中的随机数发生器产生”这两条重要信息。这意味着，在我们现已分解得到的 Frame1、Frame2、Frame6、Frame10、Frame18 和 Frame19 这六个分片中的 12 个素数中，至少有 6 个素数是由同一个随机数发

生器生成的。于是我们考虑，能否通过已有的素数，找出随机数的生成规律，进而破解所有的素数参数呢？下面，我们将研究的重心转移到如何还原随机数发生器的问题上。

随机数发生器生成的随机数是伪随机的，也就是说，根据特定的数学函数、利用计算机强大的计算功能生成的数，其实是有内在规律可循的，并不是真正意义上的随机^[8]。伪随机与真随机的区别在于，对于给定的初值，一个伪随机生成器产生的随机数是能够完全确定的，而真随机数是完全无法预测的^[9]。从信息论的角度来说，在信息的传递过程中，信息量只能保持不变或减少。所以当有限的比特信息（在随机数发生器中，我们称输入的初值为“种子”）生成更多、更长的伪随机序列时，其信息量并没有增加。因此，随机数发生器生成的伪随机序列一定在某些方面呈现出相关特征^[10]。利用这些特征，我们可以进行利用已知的六组素数对随机数的生成规律进行探究，并还原随机数发生器。

分别检测这 12 个素数序列的 0-1 分布特征、游程分布特征、移位相加特征、采样特征，在获得的数字特征中观察分析其共性特点，去除非生成器产生的素数的干扰，然后再与已知的随机数发生器的特征特点进行比较，猜想得到可能使用的随机数发生器结构。

对于可能使用的移寄存器结构和同余式结构，通过不断的尝试，对猜想的随机数发生器结构进行实验验证。最终根据实验结果和数据特征，联想经典的 RC4 与 BBS 生成器的级联结构，确定了真实的随机数发生器的结构。利用获得的随机数发生器遍历初值，将产生的序列与模数 N 计算最大公因数，确定是否为模数 N 的因数，得到 RSA 重要加密参数，破解加密数据帧内容。

由于其分析过程需要依赖于实验数据，因此将具体的分析过程描述在实验数据报告部分，详见第 2 部分第 5 小节。

2. 实验数据报告

2.1 实验环境

2.1.1 符号说明

表 2.1 符号说明

| | |
|------------|--|
| N_i | Frame <i>i</i> 中的模数 N ($i=0,\dots,20$) |
| p_i, q_i | Frame <i>i</i> 中的 RSA 体制参数($i=0,\dots,20$) |
| d_i | Frame <i>i</i> 中的私钥 d ($i=0,\dots,20$) |
| e_i | Frame <i>i</i> 中的公钥 e ($i=0,\dots,20$) |
| c_i | Frame <i>i</i> 中的密文($i=0,\dots,20$) |
| m_i | Frame <i>i</i> 中消息解密得到的明文($i=0,\dots,20$) |
| $ x $ | x 在二进制表示形式下的位数 |

注：特别强调的是，在本部分第 2、3 小节中， p 和 q 的顺序是按照程序运行结果显示的，未区分是否由随机数发生器产生；在第 5 小节中，还原了随机数发生器后，对所有的素数进行检验，判别出了由随机数发生器产生的素数和随机选择的素数，具体结果见附录 3（16 进制）或附录 4（10 进制）。

2.1.2 硬件设备

在算法实现的过程中，我们共用了两台笔记本电脑，电脑系统信息如表 2.2：

表 2.2 硬件设备

| | | 电脑 1 | 电脑 2 |
|------------|-----|----------------------------|----------------------------|
| Windows 版本 | | Windows 8 | Windows 7 |
| 系统 | 处理器 | Intel(R) Core(TM) i5-4260U | Intel(R) Core(TM) i5-2415M |
| | 类型 | 64 位操作系统 | 64 位操作系统 |

由于设备所限，我们在算法实现过程中，优先考虑低耗时、低耗能的方法，所以在运行程序时，超过 5 小时仍未得到正确结果的，暂时不予考虑。

2.1.3 软件工具

计算机是我们在破译密码时得力的研究工具。许多数学软件都提供了对 RSA 加密体制运算上的支持功能，如 Magma、Matlab 和 Maple 等数学软件，它们拥有系统完整的封装函数，但是，在一定程度上限制了用户的底层权限，功能完整性有所欠缺。为了解决这一问题，本文选用了最基础的编程语言——C 语言开发平台^[11]，调用了 GMP 大数库^[12]和 Miracl 大数库^[13]，对 RSA 破译算法进行理论的实现与验证。

1) Microsoft Visual C++

Microsoft Visual C++（简称 Visual C++），是 Microsoft 公司推出的以 C++ 语言为基础的开发 Windows 环境程序，是面向对象的可视化集成编程系统。它不但具有程序框架自动生成、灵活方便的类管理、代码编写和界面设计集成交互操作、可开发多种程序等优点，而且通过设置就可使其生成的程序框架支持数据库接口、OLE2.0、WinSock 网络以及 3D 控制界面。

本小组在具体思路的实现方式上，均是基于 Microsoft Visual C++ 环境、用基

本 C++ 语言编程实现的，所用版本为 Microsoft Visual C++ 6.0。

2) GMP 数学函数库

GMP 大数库是 GNU 项目的一部分，诞生于 1991 年。作为一个大整数运算库，它包括了任意精度的整数、有理数和浮点数的各种基本运算操作，其目标是为所有需要不能由基本 C 语言类型直接支持的多精度类型的应用提供尽可能快的算法。它的主要应用方向是密码学、网络安全、代数系统、计算科学等。GMP 库的运行速度非常快，但是它所提供的只是数学运算功能，并没有密码学相关的高级功能。

本小组在编写基本 C 语言类型的代码时，由于题目对数据的格式规定，数字长度、精度范围等要求无法得到实现，经过适当调用 GMP 库中的集成函数，成功运行了程序并且得到了符合题目要求的数据。

3) Miracl 库

Miracl (Multiprecision Integer and Rational Arithmetic C/C++ Library) 是 Shamus Software 公司开发的一个大数运算函数库，是当今著名密码学 C 语言函数库，它的使用许可针对教育科学研究或者非商业目的的应用是免费的，是基于当前使用较为广泛的公钥加密算法保护实现的大数库之一。在功能上，它不但提供了高精度的大整数和分数的各种数学运算操作，而且提供了很多密码学算法中的功能模块，尤其是针对公钥密码学和椭圆曲线密码学的实现。最为特别的是，它还提供了很多椭圆曲线密码体制中的底层功能模块。由于 Miracl 库的内部实现采用了很多的汇编代码，故运算速度也非常快。Miracl 函数库自从开发至今，以其紧凑、快速、高效的优点得到了广泛的应用。

2.2 常用攻击方法

2.2.1 费马分解法

如果 21 个分片中，存在由两个比较接近的素数相乘得到的模数，那么，费马分解法将很快可以破解它。根据费马分解法的原理，我们用 C 语言开发平台编写程序，对所有 21 个分片的模数 N 进行攻击尝试。主要代码如下：

费马分解法代码：

```
输入  $N$  ;  
 $k \leftarrow \lfloor \sqrt{N} \rfloor + 1$ ;  
 $y \leftarrow k^2 - N$ ;  
 $d \leftarrow 1$ ;  
while( $\lfloor \sqrt{y} \rfloor \neq \sqrt{y}$  &&  $\lfloor \sqrt{y} \rfloor \geq N/2$ )  
{  
     $y \leftarrow y + 2k + d$  ;  
     $d \leftarrow d + 2$  ;  
};  
if( $\lfloor \sqrt{y} \rfloor < N/2$ )  
    输出 “没有找到因子” ;  
else  
{  
     $x \leftarrow \sqrt{N + y}$  ;  
     $y \leftarrow \sqrt{y}$  ;  
     $p \leftarrow x - y$  ;  
     $q \leftarrow \sqrt{x + y}$  ;  
    输出  $p, q$  ;  
}
```

根据该原理，对所有 21 个分片进行攻击后，Frame10 在较短时间内被成功破解。

程序运行结果如图 2.1:

```
*****Fermat分解算法*****
分解Frame10中模数N

分解成功!
结果:
Frame10:
n=
85A0AC7E685995D9F8012C3A0249491956697997BBB6E5DDC1B53DC6184A843C3E4EB9B2D97FEAFAD097AA0FF640846287953C88F5A0813FD81FF3EBBDD62D66F4403653DCEC64ACE99F9FAAED4FD35513214EF4B4B9AA910E5923CD87F9330E3599F2CF1AD90EFC6BDABBBD249D1AC8CF83836FE18399379E712010FC25A3DA3
p=
B8F4B3E37AA6DEAD7CA8BB875F7A20F1F79C096B6D8E33755DD0C18FF8E2DA39234447F39576193DFBFB84097174A3481DBEC8F7B925EB005F720589F5AB24FC9
q=
B8F4B3E37AA6DEAD7CA8BB875F7A20F1F79C096B6D8E33755DD0C18FF8E2DA39234447F39576193DFBFB84097174A3481DBEC8F7B925EB005F720589F5AB2500B

耗时0.01 s
```

图 2.1 破解 Frame10

运行结果显示，程序成功分解了 Frame10 的模数，得到了加解密参数，如表 2.3:

表 2.3 Frame10 模数分解结果

| Frame10 | |
|----------|---|
| N_{10} | 85A0AC7E685995D9F8012C3A0249491956697997BBB6E5DDC1B53DC6184A843C3E4EB9B2D97FEAFAD097AA0FF640846287953C88F5A0813FD81FF3EBBDD62D66F4403653DCEC64ACE99F9FAAED4FD35513214EF4B4B9AA910E5923CD87F9330E3599F2CF1AD90EFC6BDABBBD249D1AC8CF83836FE18399379E712010FC25A3DA3 |
| p_{10} | B8F4B3E37AA6DEAD7CA8BB875F7A20F1F79C096B6D8E33755DD0C18FF8E2DA39234447F39576193DFBFB84097174A3481DBEC8F7B925EB005F720589F5AB24FC9 |
| q_{10} | B8F4B3E37AA6DEAD7CA8BB875F7A20F1F79C096B6D8E33755DD0C18FF8E2DA39234447F39576193DFBFB84097174A3481DBEC8F7B925EB005F720589F5AB2500B |

根据得到的参数进行解密运算，运行结果如图 2.2:

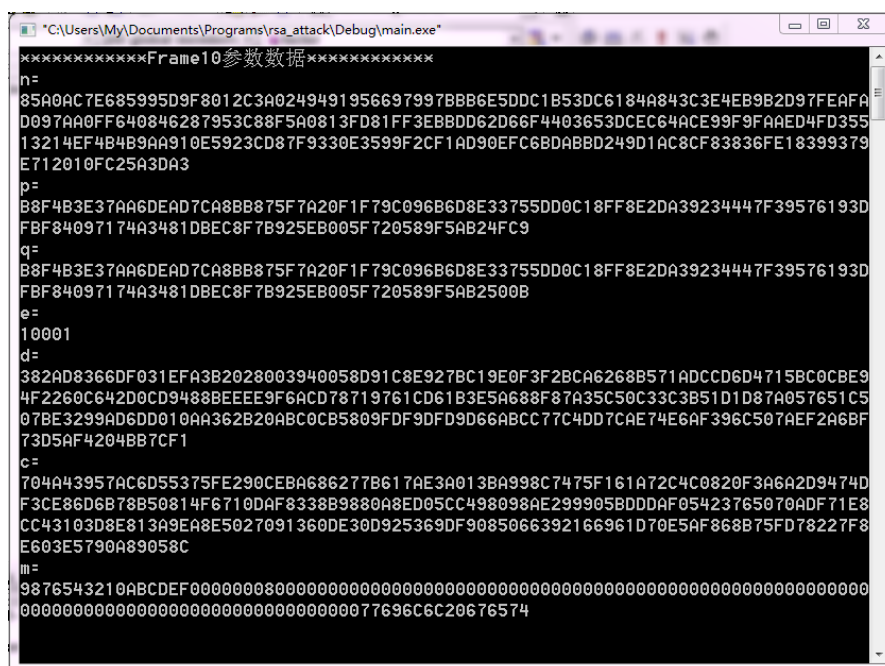


图 2.2 破译 Frame10

经过解密运算，我们恢复了明文片段为“77696C6C20676574”。通过查阅 16 进制 ASCII 码的对应规则，得到其相应的字符如表 2.4:

表 2.4 Frame10 明文还原

| ASCII 码 | 77 | 69 | 6C | 6C | 20 | 67 | 65 | 74 |
|---------|----|----|----|----|----|----|----|----|
| 对应字符 | w | i | l | l | 空格 | g | e | t |

最终，利用费马分解法成功破解了 Frame10 的加解密参数，并恢复了明文信息为“will get”。

分析本次攻击过程：分解模数所耗时长仅 0.01 秒，分解所得到的两个素数 p 和 q 在 16 进制表示下仅后四位不相同。这是因为，费马分解法能够针对由两个比较接近的素数 p 、 q 相乘得到的模数存在的缺陷实行十分有效的攻击，本次攻击结果也证实了这一点；除此之外，分解时长非常短，更进一步说明了由两个相近素数生成的模数存在极大的安全威胁。这说明，算法设计者在挑选素数时，考虑选择相同长度的两个素数的同时，还应该注意尽可能地令两个数值的差距大一

些，否则，参数将存在安全缺陷，很容易被费马分解法攻破。

2.2.2 Pollard $p-1$ 分解法

根据 Pollard $p-1$ 的原理，在 C 语言开发平台下编写程序，对剩余 20 个分片的模数 N 进行攻击尝试。主要代码如下：

Pollard $p-1$ 分解法代码：

```
输入  $N, B$ ;  
 $a \leftarrow 2$ ;  
 $k \leftarrow 1$ ;  
while( $k \leq B$ )  
{  
     $a \leftarrow a^k \bmod N$ ;  
     $p \leftarrow \gcd(a-1, N)$ ;  
    if( $1 < p < N$ )  
    {  
         $q \leftarrow N / p$ ;  
        输出  $p, q$ ;  
    }  
    输出 “没有找到因子”;  
}
```

对所有分片进行攻击后，成功破解了 Frame2、Frame6 和 Frame19。

1) 对 Frame2 中的模数的破解:

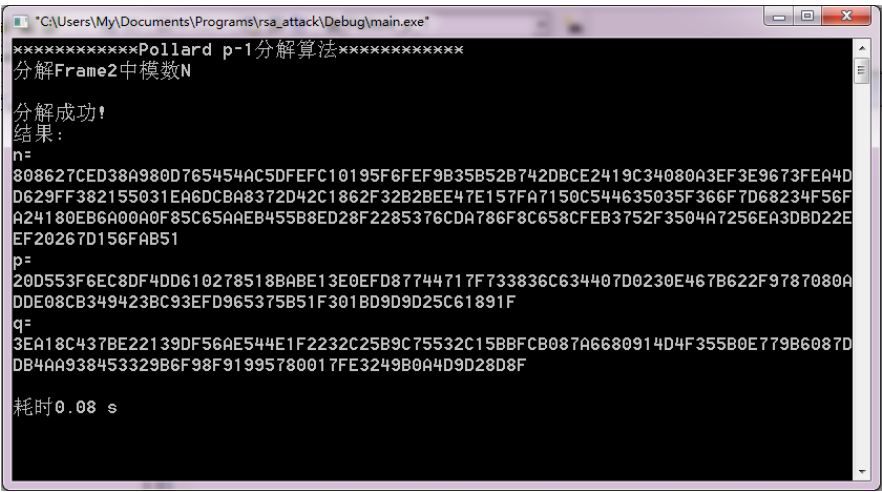


图 2.3 破解 Frame2

运行结果显示，成功分解了 Frame2 的模数，得到了加解密参数，如表 2.5:

表 2.5 Frame2 模数分解结果

| Frame2 | |
|--------|--|
| N_2 | 808627CED38A980D765454AC5DFEFC10195F6FEF9B35B52B742DBCE2419C34080A3EF3E9673FEA4DD629FF382155031EA6DCBA8372D42C1862F32B2BEE47E157FA7150C544635035F366F7D68234F56FA24180EB6A00A0F85C65AAEB455B8ED28F2285376CDA786F8C658CFEB3752F3504A7256EA3DBD22EEF20267D156FAB51 |
| p_2 | 3EA18C437BE22139DF56AE544E1F2232C25B9C75532C15BBFCB087A6680914D4F355B0E779B6087DDB4AA938453329B6F98F91995780017FE3249B0A4D9D28D8F |
| q_2 | 20D553F6EC8DF4DD610278518BABA13E0EFD87744717F733836C634407D0230E467B622F9787080ADDE08CB349423BC93EFD965375B51F301BD9D9D25C61891F |

表 2.6 Frame2 明文还原

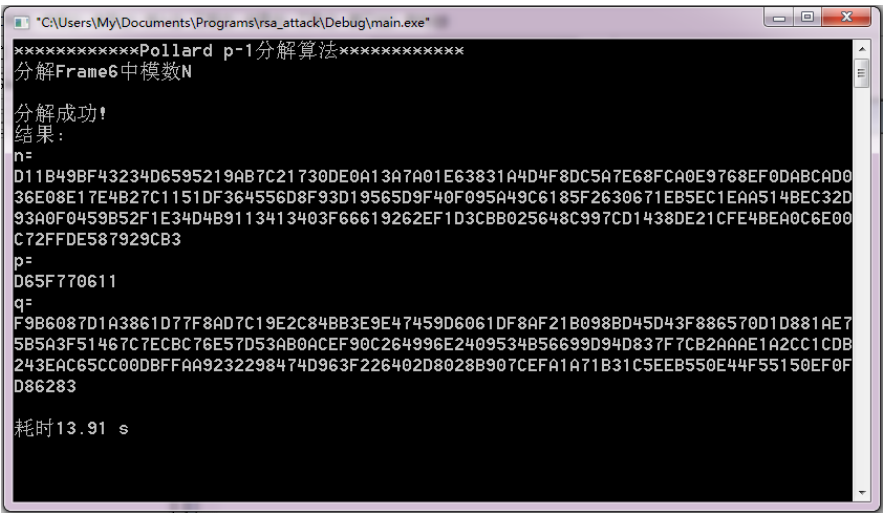
| | | | | | | | | |
|---------|----|----|----|----|----|----|----|----|
| ASCII 码 | 20 | 54 | 68 | 61 | 74 | 20 | 69 | 73 |
| 对应字符 | 空格 | T | h | a | t | 空格 | i | s |

经过解密运算，我们恢复了明文片段为“2054686174206973”。通过查阅 16

进制 ASCII 码的对应规则，得到其相应的字符见表 2.6。

最终，利用 Pollard $p-1$ 分解法成功破解了 Frame2 的加解密参数，并恢复了明文信息为 “ That is”。

2) 对 Frame6 中的模数的破解：



```
*****Pollard p-1分解算法*****
分解Frame6中模数N
分解成功!
结果:
n=
D11B49BF43234D6595219AB7C21730DE0A13A7A01E63831A4D4F8DC5A7E68FCA0E9768EF0DABCAD0
36E08E17E4B27C1151DF364556D8F93D19565D9F40F095A49C6185F2630671EB5EC1EAA514BEC32D
93A0F0459B52F1E34D4B9113413403F66619262EF1D3CBB025648C997CD1438DE21CFE4BEA0C6E00
C72FFDE587929CB3
p=
D65F770611
q=
F9B6087D1A3861D77F8AD7C19E2C84BB3E9E47459D6061DF8AF21B098BD45D43F886570D1D881AE7
5B5A3F51467C7ECBC76E57D53AB0ACEF90C264996E2409534B56699D94D837F7CB2AAAE1A2CC1CDB
243EAC65CC00DBFFAA9232298474D963F226402D8028B907CEFA1A71B31C5EEB550E44F55150EF0F
D86283
耗时 13.91 s
```

图 2.4 破解 Frame6

运行结果显示，成功分解了 Frame6 的模数，得到了加解密参数，如表 2.7：

表 2.7 Frame6 模数分解结果

| Frame6 | |
|--------|--|
| N_6 | D11B49BF43234D6595219AB7C21730DE0A13A7A01E63831A4D4F8DC5A7E68FCA0E9768EF0DABCAD036E08E17E4B27C1151DF364556D8F93D19565D9F40F095A49C6185F2630671EB5EC1EAA514BEC32D93A0F0459B52F1E34D4B9113413403F66619262EF1D3CBB025648C997CD1438DE21CFE4BEA0C6E00C72FFDE587929CB3 |
| p_6 | D65F770611 |
| q_6 | F9B6087D1A3861D77F8AD7C19E2C84BB3E9E47459D6061DF8AF21B098BD45D43F886570D1D881AE75B5A3F51467C7ECBC76E57D53AB0ACEF90C264996E2409534B56699D94D837F7CB2AAAE1A2CC1CDB243EAC65CC00DBFFAA9232298474D963F226402D8028B907CEFA1A71B31C5EEB550E44F55150EF0FD86283 |

经过解密运算，我们恢复了明文片段为 “20224C6F67696320”。通过查阅 16

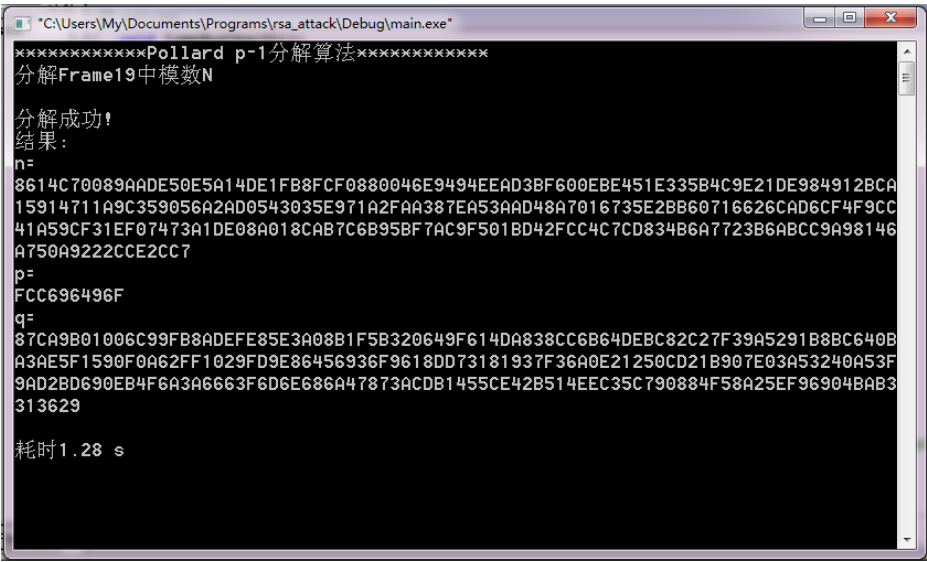
进制 ASCII 码的对应规则，得到其相应的字符如表 2.8:

表 2.8 Frame6 明文还原

| | | | | | | | | |
|---------|----|----|----|----|----|----|----|----|
| ASCII 码 | 20 | 22 | 4C | 6F | 67 | 69 | 63 | 20 |
| 对应字符 | 空格 | “ | L | o | g | i | c | 空格 |

最终，利用 Pollard $p-1$ 分解法成功破解了 Frame6 的加解密参数，并恢复了明文信息为 “ “Logic ”。

3) 对 Frame19 中的模数的破解:



```
*****Pollard p-1分解算法*****
分解Frame19中模数N
分解成功!
结果:
n=
8614C70089AADE50E5A14DE1FB8FCF0880046E9494EEAD3BF600EBE451E335B4C9E21DE984912BCA
15914711A9C359056A2AD0543035E971A2FAA387EA53AAD48A7016735E2BB60716626CAD6CF4F9CC
41A59CF31EF07473A1DE08A018CAB7C6B95BF7AC9F501BD42FCC4C7CD834B6A7723B6ABCC9A98146
A750A9222CCE2CC7
p=
FCC696496F
q=
87CA9B01006C99FB8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39A5291B8BC640B
A3AE5F1590F0A62FF1029FD9E86456936F9618DD73181937F36A0E21250CD21B907E03A53240A53F
9AD2BD690EB4F6A3A6663F6D6E686A47873ACDB1455CE42B514EEC35C790884F58A25EF96904BAB3
313629
耗时1.28 s
```

图 2.5 破解 Frame19

运行结果显示，成功分解了 Frame19 的模数，得到了加解密参数，如表 2.9:

表 2.9 Frame19 模数分解结果

| Frame19 | |
|----------|--|
| N_{19} | 8614C70089AADE50E5A14DE1FB8FCF0880046E9494EEAD3BF600EBE451E335B4C9E21DE984912BCA15914711A9C359056A2AD0543035E971A2FAA387EA53AAD48A7016735E2BB60716626CAD6CF4F9CC41A59CF31EF07473A1DE08A018CAB7C6B95BF7AC9F501BD42FCC4C7CD834B6A7723B6ABCC9A98146A750A9222CCE2CC7 |

| | |
|----------|--|
| p_{19} | 87CA9B01006C99FB8ADEFE85E3A08B1F5B320649F614DA838CC6B64 DEBC82C27F39A5291B8BC640BA3AE5F1590F0A62FF1029FD9E864569 36F9618DD73181937F36A0E21250CD21B907E03A53240A53F9AD2BD6 90EB4F6A3A6663F6D6E686A47873ACDB1455CE42B514EEC35C790884 F58A25EF96904BAB3313629 |
| q_{19} | FCC696496F |

经过解密运算，我们恢复了明文片段为“696E737465696E2E”。通过查阅 16 进制 ASCII 码的对应规则，得到其相应的字符如表 2.10：

表 2.10 Frame19 明文还原

| ASCII 码 | 69 | 6E | 73 | 74 | 65 | 69 | 6E | 2E |
|---------|----|----|----|----|----|----|----|----|
| 对应字符 | i | n | s | t | e | i | n | . |

最终，利用 Pollard $p-1$ 分解法成功破解了 Frame19 的加解密参数，并恢复了明文信息为“instein.”。

分析本次攻击过程，我们可以看到两组成功分解的模数 N 都得到了一个位数较短的素数参数和一个位数较长的素数参数，这是因为，Pollard $p-1$ 分解法是从素数 $p-1$ 的小因子开始尝试，知道能整除为止，若模数存在较小的因子，将很容易被分解。所以，我们在选取素数参数时应注意，尽量不选取位数相差过大的两个数，以降低被 Pollard $p-1$ 分解法破解的可能性。

2.2.3 低加密指数攻击

低加密指数攻击法适用于加密密钥相同且模数互素的数，通过对数据的观察，我们发现 Frame7、Frame11、Frame15 和 Frame3、Frame8、Frame12、Frame16、Frame20 这两组数分别符合低加密指数攻击的条件。

1) 对 Frame7、Frame11 和 Frame15 的攻击

假设 Frame7、Frame11 和 Frame15 三个分片是由相同的明文加密得到的，
即已知 $e_7 = e_{11} = e_{15} = 3$ ，设 $m_7 = m_{11} = m_{15} = m$ ，可列出如下同余式：

$$\begin{cases} c_7 \equiv m^3 \pmod{N_7} \\ c_{11} \equiv m^3 \pmod{N_{11}} \\ c_{15} \equiv m^3 \pmod{N_{15}} \end{cases}$$

对其应用中国剩余定理，可以求出 m 的值。根据该攻击法原理，编写 C 语言程序，主要代码如下：

低加密指数攻击代码：

输入 $c_7, c_{11}, c_{15}, N_7, N_{11}, N_{15}$ ；

$N'_7 \leftarrow (N_{11}N_{15})^{-1} \pmod{N_7}$ ；

$N'_{11} \leftarrow (N_7N_{15})^{-1} \pmod{N_{11}}$ ；

$N'_{15} \leftarrow (N_7N_{11})^{-1} \pmod{N_{15}}$ ；

$m' = c_7N'_7N_{11}N_{15} + c_{11}N_7N'_{11}N_{15} + c_{15}N_7N_{11}N'_{15} \pmod{N_7N_{11}N_{15}}$ ；

$m \leftarrow \sqrt[3]{m'}$ 。

但通过对此方法下程序运行结果的观察，可以发现，得到的明文数据与题中所给的加密规则不符，且不对应有明确语义的明文信息，该方法失败。

通过改进计算方法，假设有两组是由同一明文加密得到，不同时计算三组数据，而是在从任意两组数据入手，两两判断是否有相同的明文消息。

程序运行结果显示如图 2.6：

```
C:\Users\My\Documents\Programs\rsa_attack\Debug\main.exe
*****低加密指数攻击*****
Frame7 & Frame11 & Frame15 存在相同低加密指数e=3

假设Frame7与Frame11存在相同消息时,求解明文为:
m=
3BF9C6C4A109AC741813B2CD7D213C9CEDC0DEA5D7D6FEFEADA070B6AFBD57F0CE9EB8EFE17DCC12
FB3A7E9F046896489A15F56B300F28E7E8F4433F4298B46B13316BE6F40BD093733D4E7002492B1D
A7AD5303BBC

假设Frame7与Frame15存在相同消息时,求解明文为:
m=
4DC683CA1DACB9B98C1F71F4D9598010D95D113FF9AF376D2BC48BB34C9B3C7EC10777AAF5E2DADF
A02FF6D0AB0F4088BF0D470DD31EDA2A655C267F2020355516FEFB2921B25AF2E9E1D9F8CD40DA9D
ED802357E9E

假设Frame11与Frame15存在相同消息时,求解明文为:
m=
4F0784F6FC599A40B29CEB1DBEBBCF343B4D817B2D2D13FE20B4C64B4173E03AEF21F3D2CDE2BAA9
B2757ADB49D40230FCA9B0C26CC2573C8F8A6D31E7BD8A15BFEB456F5CF99FC60FE92B11E160BE5C
62FDE0812C4

耗时0.01 s
```

图 2.6 破译 Frame7、Frame11 和 Frame15

观察运行结果，我们可以看到：攻击任意两组数据得到的明文都不符合题目的加密规则，且无法还原成有意义的语句信息，说明本次攻击失败，Frame7、Frame11 和 Frame15 不是由同样的明文加密得到的。

2) 对 Frame3、Frame8、Frame12、Frame16、Frame20 的攻击

借鉴上一次对 Frame7、Frame11 和 Frame15 的攻击过程中积累的经验，先判断 m^e 与 $N_1 \cdots N_k$ 的大小关系：

$$|m^3| = 1536 < N_i \cdot N_j (i = 3, 8, 12, 16, 20, j = 3, 8, 12, 16, 20)。$$

由计算结果知：只要 5 个分片中有 3 个是由同一明文加密得到的，就符合低加密指数攻击的条件。

于是，假设这五组数据中有三组是由同一明文加密得到，利用改进后的算法进行判断。

程序运行结果如图 2.7：

通过程序实现，我们恢复了明文片段为“4D79207365637265”。通过查阅 16 进制 ASCII 码的对应规则，得到其相应的字符如表 2.12:

表 2.12 Frame0 和 Frame4 明文还原

| ASCII 码 | 4D | 79 | 20 | 73 | 65 | 63 | 72 | 65 |
|---------|----|----|----|----|----|----|----|----|
| 对应字符 | M | y | 空格 | s | e | c | r | e |

最终，利用公共模数攻击法恢复了明文信息为“My secre”。

2.3 因数碰撞法的意外发现

根据“Elliptic Curve Cryptography in Practice”一文中因数碰撞的思想，我们用 C 语言程序实现了欧几里德算法，对全部 21 组模数两两求最大公因数。程序运行结果如图 2.9:

```

*****求解公因子*****
[Frame0,Frame4]=
803F734ED9E3A3FBDEF8E3540B7B676FB66D15D2E5139840CB3CD06E62634C00A48EA2BF9BC3D7A7
09DBB47BE7E27DFB2C0E5B81254E6C326691471AE6DDC4A35539018BA6305DAFF1C480F195118B13
10C546C31FE62C7AEC2A947013AC2897D00FD60E7B792DD499315341895BD1D1C9AA923E9373E1E0
1E2856B4FC8C6893

[Frame1,Frame18]=
8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39A5291B8BC640BA3AE5F1590F0A62F
F1029FD9E86456936F9618DD73181937F36A0E21250CD21B

耗时0.01 s

```

图 2.9 对 21 个模数两两求最大公因数

观察结果，可以看到：Frame0 与 Frame4 有大于 1 的最大公因数；Frame1 与 Frame18 有大于 1 的最大公因数。然而 Frame0 与 Frame4 的模数相同，求出的最大公因数是它们共有的模数本身，仍是平凡因数，所以没有达到成功分解模数的目标；而 Frame1 与 Frame18 的最大公因数为非平凡因数，可以通过除法运算分别求得模数 N_1 和 N_{18} 的另一个因数(如下表)，即求出素数 p 和 q ，破译明文。

模数 N_1 分解的结果如表 2.14:

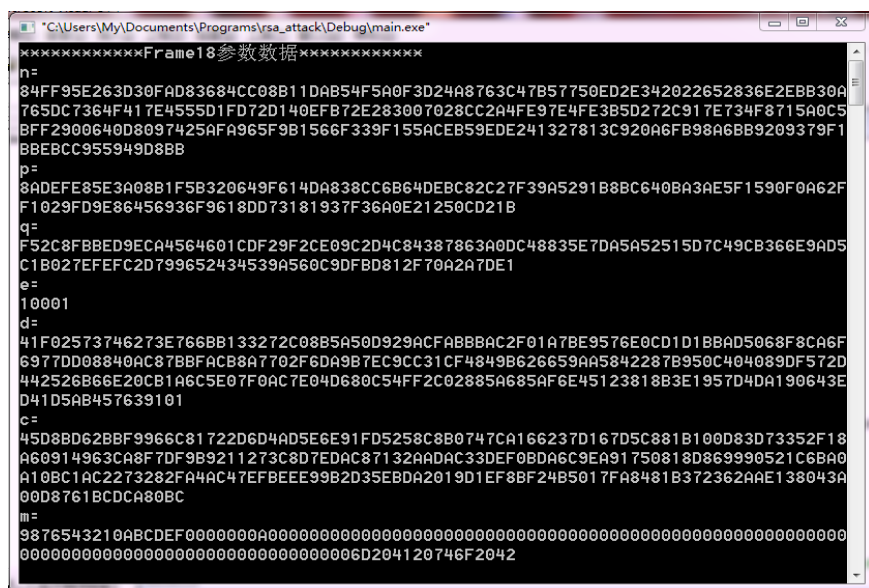
表 2.14 Frame1 模数分解结果

| Frame1 | |
|--------|--|
| N_1 | 845334AC0B3EB2239FDF0E3069750901E791CB774AD36941E30D85E5A0FED57749A30DC1F1F4CB191D9863F437C98293E8E8888B963BCF16B691F1D4EEF56C6807440E5FB5EC5B95DF3434DEDA30C60DCB4E77294BE027F984D5E675AEB1CBBE57E8CAF140226EAD6DCD9A9636A0CFF586FA434804CB09D7E8C48DE34EBE9049 |
| p_1 | 8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39A5291B8BC640BA3AE5F1590F0A62FF1029FD9E86456936F9618DD73181937F36A0E21250CD21B |
| q_1 | F3EECA557B30A36F05427F1936A4E7D387D6AC1D65587E774FAA9561FB4C4B5B70BEBEE52C80727F3F12ECA96CF457E34EA622AD70A89F87737AA4F12B9C2D6B |

经过解密运算，我们恢复了明文片段为“2E20496D6167696E”。通过查阅 16 进制 ASCII 码的对应规则，得到其相应的字符如表 2.15:

表 2.15 Frame1 明文还原

| ASCII 码 | 2E | 20 | 49 | 6D | 61 | 67 | 69 | 6E |
|---------|----|----|----|----|----|----|----|----|
| 对应字符 | . | 空格 | I | m | a | g | i | n |



最终，利用因数碰撞法成功破解了 Frame1 的加解密参数，并恢复了明文信息为 “. Imagin”。

模数 N_{18} 分解的结果如表 2.16:

表 2.16 Frame18 模数分解结果

| Frame18 | |
|----------|---|
| N_{18} | 84FF95E263D30FAD83684CC08B11DAB54F5A0F3D24A8763C47B57750 ED2E342022652836E2EBB30A765DC7364F417E4555D1FD72D140EFB7 2E283007028CC2A4FE97E4FE3B5D272C917E734F8715A0C5BFF290064 0D8097425AFA965F9B1566F339F155ACEB59EDE241327813C920A6FB 98A6BB9209379F1BBEBC955949D8BB |
| p_{18} | 8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39A529 1B8BC640BA3AE5F1590F0A62FF1029FD9E86456936F9618DD73181937 F36A0E21250CD21B |
| q_{18} | F52C8FBBED9ECA4564601CDF29F2CE09C2D4C84387863A0DC48835E 7DA5A52515D7C49CB366E9AD5C1B027EFEFC2D799652434539A560C 9DFBD812F70A2A7DE1 |

经过解密运算，我们恢复了明文片段为“6D204120746F2042”。通过查阅 16 进制 ASCII 码的对应规则，得到其相应的字符如表 2.17:

表 2.17 Frame18 明文还原

| | | | | | | | | |
|---------|----|----|----|----|----|----|----|----|
| ASCII 码 | 6D | 20 | 41 | 20 | 74 | 6F | 20 | 42 |
| 对应字符 | m | 空格 | A | 空格 | t | o | 空格 | B |

最终，利用因数碰撞法成功破解了 Frame18 的加解密参数，并恢复了明文信息为“m A to B”。

分析本次攻击过程：程序运行所耗时长仅 0.01 秒，且算法复杂度低，实现过程简单。如果我们用整数分解的方法去攻击所有的模数，所耗费的时间是无法估量的，并且，这种方法对设备的要求也非常严格。而实现欧几里德算法就简单得多，且仅用一台笔记本电脑就能够实现。这也给我们一个警示——在生成模数时，不要选择相同的素数去生成不同的模数，否则，将存在被因数碰撞法破解的安全威胁。

2.4 猜测明文攻击还原全部明文

通过以上攻击方法的尝试，目前已经得到了 13 个分片中的明文信息，不考虑重复发送的消息，共有 8 段明文消息。

表 2.18 明文信息

| | | | | | | | | |
|------|----------|----------|----------|----------|----|----------|---------|--------|
| 通信序号 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 明文 | My secre | t is a f | — | — | — | instein. | That is | "Logic |
| 通信序号 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 明文 | will get | — | m A to B | . Imagin | — | — | — | — |

观察通信序号为 10 的分片的明文消息“m A to B”，可以肯定的是，“m”一定是某个单词的尾字母，联想与“to”相关的介词结构，很容易想到“from……”

to……”；“from A to B”这句话并不常见，通过搜集资料，我们找到了爱因斯坦的一句名言“Logic will get you from A to B. Imagination will take you everywhere.”。这句话同时符合了序号为 7、8、10 和 11 四个分片的明文信息，于是，我们猜测，这句话就是序号为 7 的分片到序号为 15 的分片的明文信息。

用题目中所给的加密参数对这句话进行验证。其中通信序号为 7 的分片信息不完整，缺少第一个字符(1Byte)；通信序号为 15 的分片信息不完整，缺少最后两个字符(2Byte)，联系上下文和常用语言习惯，我们猜测最后两字符明文信息是“.”和“”。由于缺失部分较短，我们编写程序遍历了缺失部分所有可能的情况，经过极短时间的运行就得到了验证结果。最终，通过加密验证和暴力破解相结合的方式，证明了猜想是正确的。此时所得到的明文如表 2.19：

表 2.19 明文信息

| | | | | | | | | |
|------|----------|----------|----------|----------|----------|----------|----------|----------|
| 通信序号 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 明文 | My secre | t is a f | — | — | — | instein. | That is | "Logic |
| 通信序号 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 明文 | will get | you fro | m A to B | . Imagin | ation wi | ll take | you ever | ywhere." |

消息后半部分的这句话是爱因斯坦的一句名言，再观察通信序号为 5 的分片，很容易联想到爱因斯坦的英文表示“Einstein”，自然，通信序号为 4 的分片明文就是“Albert E”，通过加密验证，猜想正确。

再联系通信序号为 0 和 1 的分片，我们猜测整个明文消息可能是“我的秘诀是爱因斯坦的著名名言，逻辑会把你从 A 带到 B，想象力能带你去任何地方。”由此猜测，通信序号为 2 的分片最后一个字符“f”是“famous”的首字母，而后，我们列出了一些与“famous”相关且符合语境的短语：“famous quotes”、

“famous saying”、“famous notes”等，用加密密钥对这些可能的明文进行猜测明文攻击，最终验证“amous sa”为通讯序号为 3 的分片的明文。

因此猜测通讯序号为 4 的分片明文中，前 4 个字母为“ying”，第 5 个字母很可能为空格。再根据英语语法规则：名词之后常用介宾结构做后置定语；而人名之前的介词常用“of”。由此我们对“ying of ”做了加密验证，证明了猜想是完全正确的。

至此，我们确定了全部的明文信息，如表 2.20：

表 2.20 明文信息

| | | | | | | | | |
|------|----------|----------|----------|----------|----------|----------|----------|----------|
| 通信序号 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 明文 | My secre | t is a f | amous sa | ying of | Albert E | instein. | That is | "Logic |
| 通信序号 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 明文 | will get | you fro | m A to B | . Imagin | ation wi | ll take | you ever | ywhere." |

最终，全部明文信息破译成功，将所有分片的明文信息按照通信序号连接起来得到通关密语：My secret is a famous saying of Albert Einstein. That is "Logic will get you from A to B. Imagination will take you everywhere."

2.5 还原随机数发生器

通过之前的费马分解法、Pollard $p-1$ 分解法、因子碰撞法等大整数分解方法，已经成功分解得到了六组素数，共 12 个。在这 12 个素数中，至少有 6 个素数是由同一个随机数发生器产生的。因此，观察并分析这 12 个素数，发现其中的特点和潜在规律，是还原随机数发生器的关键。使用 16 进制表示已经获得的 12 个素数，如表 2.21：

表 2.21 已获得素数的 16 进制表示

| | |
|----------|--|
| p_1 | 8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39A 5291B8BC640BA3AE5F1590F0A62FF1029FD9E86456936F9618DD73 181937F36A0E21250CD21B |
| q_1 | F3EECA557B30A36F05427F1936A4E7D387D6AC1D65587E774FAA9 561FB4C4B5B70BEBEE52C80727F3F12ECA96CF457E34EA622AD70 A89F87737AA4F12B9C2D6B |
| p_2 | 20D553F6EC8DF4DD610278518BABE13E0EFD87744717F733836C63 4407D0230E467B622F9787080ADDE08CB349423BC93EFD965375B5 1F301BD9D9D25C61891F |
| q_2 | 3EA18C437BE22139DF56AE544E1F2232C25B9C75532C15BBFCB08 7A6680914D4F355B0E779B6087DDB4AA938453329B6F98F91995780 017FE3249B0A4D9D28D8F |
| p_6 | D65F770611 |
| q_6 | F9B6087D1A3861D77F8AD7C19E2C84BB3E9E47459D6061DF8AF21 B098BD45D43F886570D1D881AE75B5A3F51467C7ECBC76E57D53 AB0ACEF90C264996E2409534B56699D94D837F7CB2AAAE1A2CC1 CDB243EAC65CC00DBFFAA9232298474D963F226402D8028B907CE FA1A71B31C5EEB550E44F55150EF0FD86283 |
| p_{10} | B8F4B3E37AA6DEAD7CA8BB875F7A20F1F79C096B6D8E33755DD 0C18FF8E2DA39234447F39576193DFBF84097174A3481DBEC8F7B9 25EB005F720589F5AB24FC9 |
| q_{10} | B8F4B3E37AA6DEAD7CA8BB875F7A20F1F79C096B6D8E33755DD 0C18FF8E2DA39234447F39576193DFBF84097174A3481DBEC8F7B9 25EB005F720589F5AB2500B |
| p_{18} | 8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39A 5291B8BC640BA3AE5F1590F0A62FF1029FD9E86456936F9618DD73 181937F36A0E21250CD21B |
| q_{18} | F52C8FBBED9ECA4564601CDF29F2CE09C2D4C84387863A0DC488 35E7DA5A52515D7C49CB366E9AD5C1B027EFEFC2D799652434539 A560C9DFBD812F70A2A7DE1 |
| p_{19} | FCC696496F |

| | |
|----------|--|
| q_{19} | 87CA9B01006C99FB8ADEFE85E3A08B1F5B320649F614DA838CC6 B64DEBC82C27F39A5291B8BC640BA3AE5F1590F0A62FF1029FD9E 86456936F9618DD73181937F36A0E21250CD21B907E03A53240A53F 9AD2BD690EB4F6A3A6663F6D6E686A47873ACDB1455CE42B514E EC35C790884F58A25EF96904BAB3313629 |
|----------|--|

通过观察上述 12 个素数，可以发现以下显著特征：

- ① p_1 与 p_{18} 相同；
- ② 若把这 12 个数看作字符串， p_1 为 q_{19} 的子串；
- ③ p_{10} 与 q_{10} 只有最后 4 位不一致；
- ④ p_6 与 p_{19} 只有 40bit 长；
- ⑤ q_6 与 q_{19} 有 984bit 长；
- ⑥ 在 16 进制编码中，只有 p_6 与 q_2 的第 1 位小于 8，即首比特为 0。

在上述分析中， p_1 、 p_{18} 、 q_{19} 这 3 个素数分别在 3 组不同的加密帧中，却存在着数据上的紧密联系，因而这 3 个素数是同一随机数发生器生成的可能性较大。此外，“ p_1 为 q_{19} 的子串”这一特征非常符合移位寄存器产生序列的特点，因此，猜测该随机数发生器结构可能为某一移位寄存器。

下面，依据一般序列密码的分析方法，我们对上述 12 个素数分析了相关的数字特征。

1) 0-1 分布数字特征的检验

0-1 分布特征是伪随机序列数最基本的数字特征，一个好的随机数发生器产生的随机序列应当 0-1 分布均匀。由于 p_6 与 p_{19} 只有 40bit 长，其比特特征缺乏统计意义，因此，我们只对其余的 10 个素数进行特征统计。统计结果如下图：

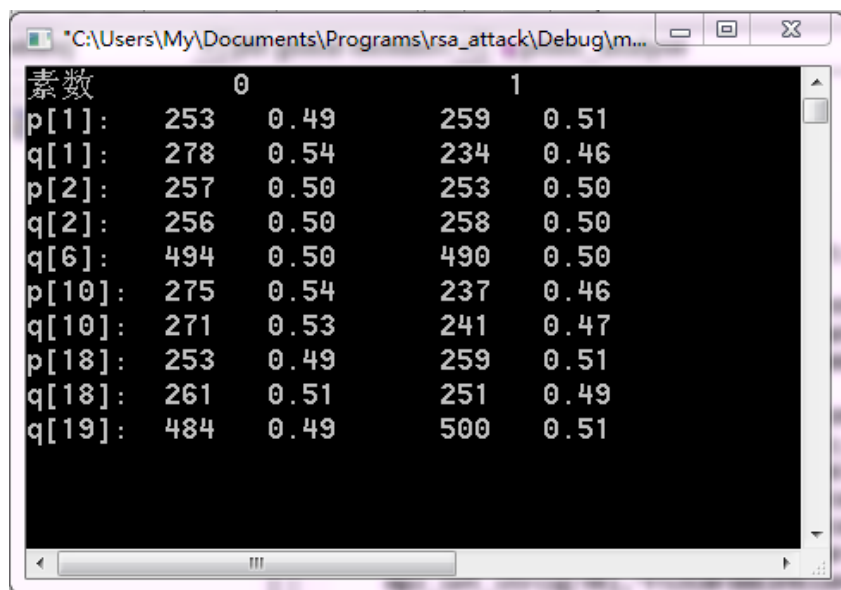


图 2.12 0-1 分布数字特征的检验

用表格表示统计规律:

表 2.22 0-1 分布的数字特征统计

| 素数 | 0 | | 1 | |
|----------|-----|------|-----|------|
| | 个数 | 占比 | 个数 | 占比 |
| p_1 | 253 | 0.49 | 259 | 0.51 |
| q_1 | 278 | 0.54 | 234 | 0.46 |
| p_2 | 257 | 0.50 | 253 | 0.50 |
| q_2 | 256 | 0.50 | 258 | 0.50 |
| q_6 | 494 | 0.50 | 490 | 0.50 |
| p_{10} | 275 | 0.54 | 237 | 0.46 |
| q_{10} | 271 | 0.53 | 241 | 0.47 |
| p_{18} | 253 | 0.49 | 259 | 0.51 |
| q_{18} | 261 | 0.51 | 251 | 0.49 |

| | | | | |
|----------|-----|------|-----|------|
| q_{19} | 484 | 0.49 | 500 | 0.51 |
|----------|-----|------|-----|------|

观察统计结果：0、1 分布相对均匀，并没有出现明显的优势，说明本题中的随机数序列并不符合 0-1 分布。

2) 游程分布数字特征的检验

定义 1 对于 n bit 序列 $a = \{0,1\}^n$ ，定义一组连续的相同符号称为一个游程，符号为 1 的称为 1-游程，符号为 0 的称为 0-游程，连续相同符号的个数称为这个游程的长度。即当连续比特的 k 个 0 的前一位和后一位均为 1 时，就称这 k 个 0 是长为 k 的 0-游程；反之，称为长 k 的 1-游程。

游程分布特征体现了伪随机序列在多比特字符串上的独立性质，一个好的统计特性的伪随机序列，应当满足以下要求：

- ① 0、1 个数接近；
- ② 相同长度的 0、1-游程的个数大致相等；
- ③ 长为 k 的游程的个数接近于长为 $k+1$ 的游程个数的两倍。

若某一伪随机序列在游程分布上出现不规律性，则意味着该序列的生成规律上存在一定的趋势或结构。

对已知的 12 个素数序列进行游程分布统计，如下图：

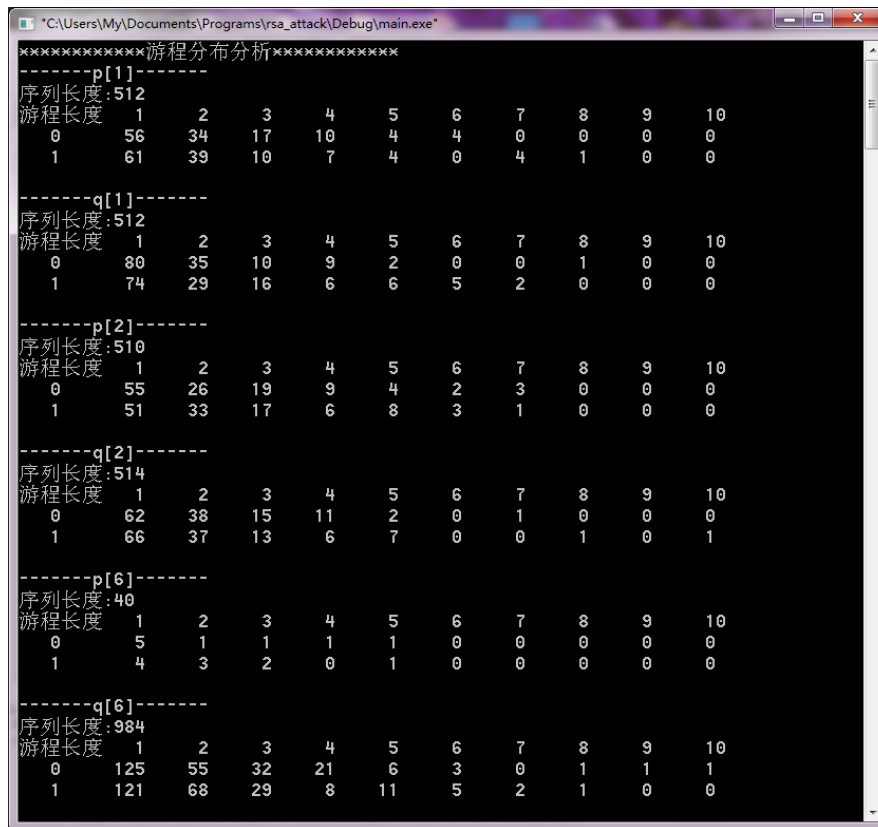


图 2.13 游程分布特征分析 1

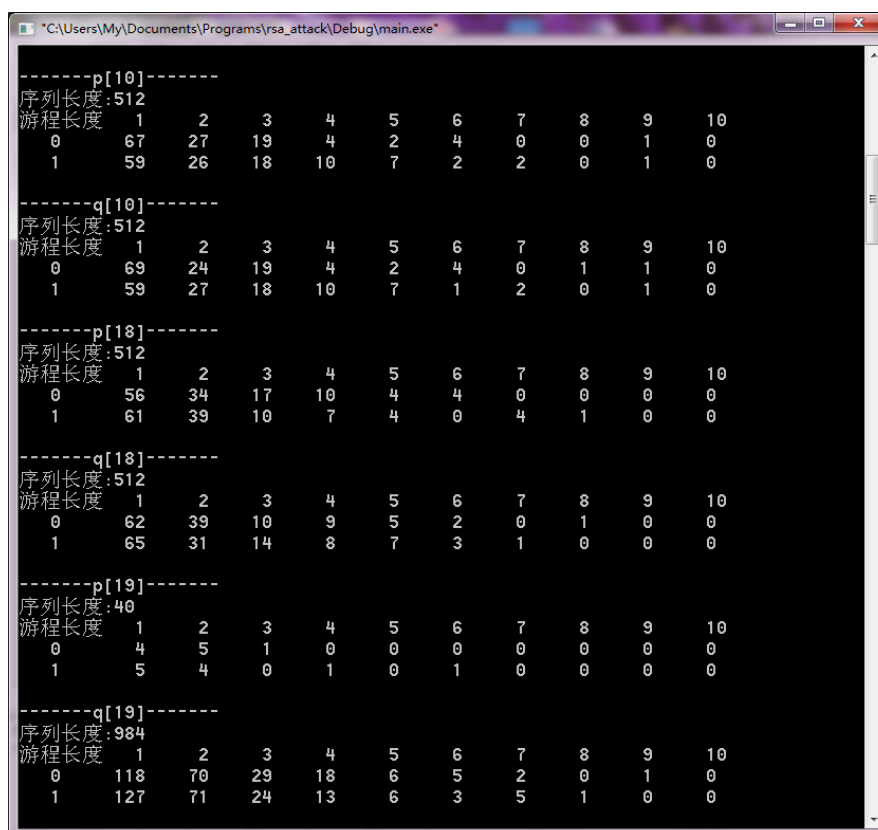


图 2.14 游程分布特征分析 2

从实验结果分析，整体的游程分布情况较好，但在个别较长游程上存在分布比例与真随机序列分布规律偏差较大的情况。例如 p_1 、 q_1 、 p_{10} 、 q_{10} 和 p_{18} 在较长的 0、1 游程上差异较大， q_2 在长为 7、8、9 的游程都存在的情况下未出现长为 6 的游程等。这可能由于统计的序列长度都不足 1000bit，难以满足游程分布统计分析的要求导致的，也可能是由于随机数发生器本身的结构特点导致的。

若这些游程统计的特征是由于随机数发生器导致的，则说明 p_1 、 q_1 、 p_{10} 、 q_{10} 和 p_{18} 这些素数序列存在结构上的内部联系，它们很可能是来自于同一随机数发生器。

3) 移加特性的检验

定理 6 序列 $a=\{0,1\}^n$ 是由一个周期为 T 反馈移位寄存器生成，则存在 k 个整数 s_0, s_1, \dots, s_k ，其中 $0 \leq k \leq T$ 使得序列 a 满足下列关系式：

$$L^{s_0}(a) + L^{s_1}(a) + \dots + L^{s_{k-1}}(a) = L^{s_k}(a),$$

其中 $L^s(a)$ 表示将序列 a 左移 s bit 后的序列。

移加特性反映的是反馈移位寄存器抽头位置的特征信息，若生成器是一个线性反馈移位寄存器，其反馈函数为 $g(a_0, a_1, \dots, a_{n-1}) = \sum_{i=0}^{n-1} b_{n-i-1} a_i$ ，其中 $b_{s_0} = b_{s_2} = \dots = b_{s_{k-1}} = 1$ ，除此之外，其余的系数均为 0，则显然可以得出 $L^{s_0}(a) + L^{s_1}(a) + \dots + L^{s_{k-1}}(a) = L^{s_k}(a)$ ，也就是意味着，抽头的位置即为移位相加的位置^[14]。

对于非线性反馈寄存器，依然可以找到满足这样条件的 s_0, s_1, \dots, s_k ，但 s_i 的值可能会很大 ($0 \leq s_i \leq T$)。因此在实际操作过程中，由于已知序列的长度限制或时间限制，往往无法有效地找到满足等式成立的 s_0, s_1, \dots, s_k 。通常情况下，选择

较少的移位序列 $L^0(a), L^1(a), \dots, L^{t_{j-1}}(a)$ ，当 t_0, t_1, \dots, t_{j-1} 的分布与 $b_{s_0}, b_{s_2}, \dots, b_{s_{k-1}}$ 的分布间距特征有明显的相关关系时，新序列 $a' = L^{s_0}(a) + L^{s_1}(a) + \dots + L^{s_{k-1}}(a)$ 往往会出现显著的优势特征。利用这种方法，可以有效地利用序列的移加特性分析寄存器抽头的分布情况。

因此我们对已知的 12 个素数序列分别进行移加特性检验。我们选取原序列，将其与移位 s bit 后的序列进行异或运算，然后观察新序列的 0-1 分布情况。

用程序对每一组素数进行移加特性检验，共检验了偏移 1 到 32 位的分布特征，结果显示如下：

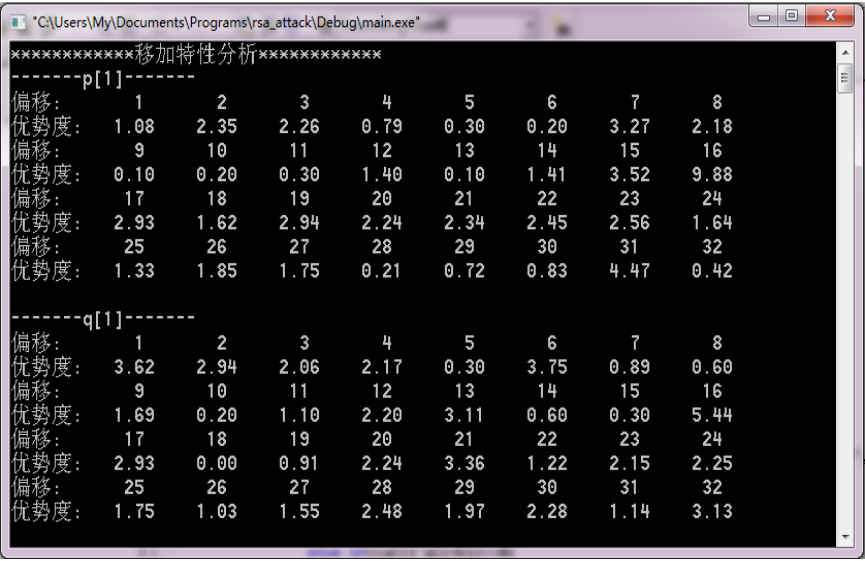


图 2.15 p[1]移加特性检验

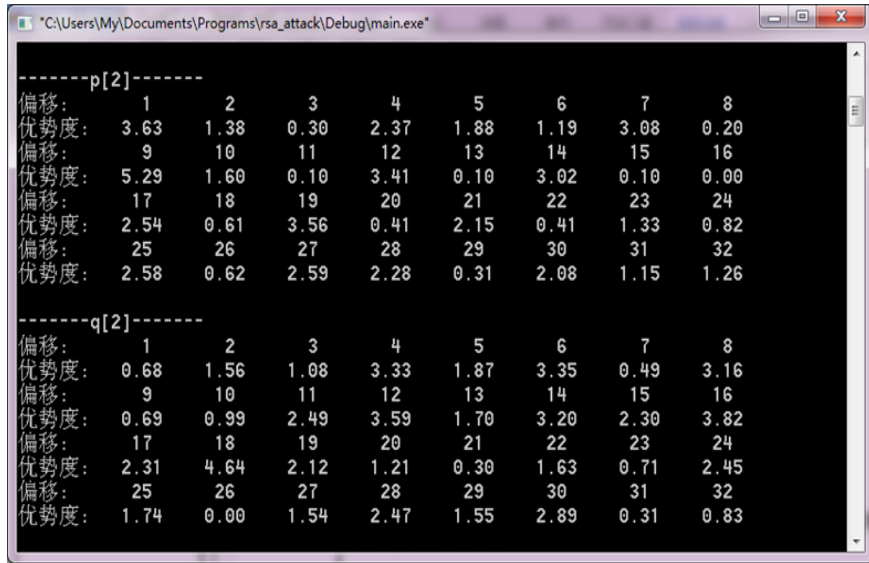


图 2.16 $p[2]$ 移加特性检验

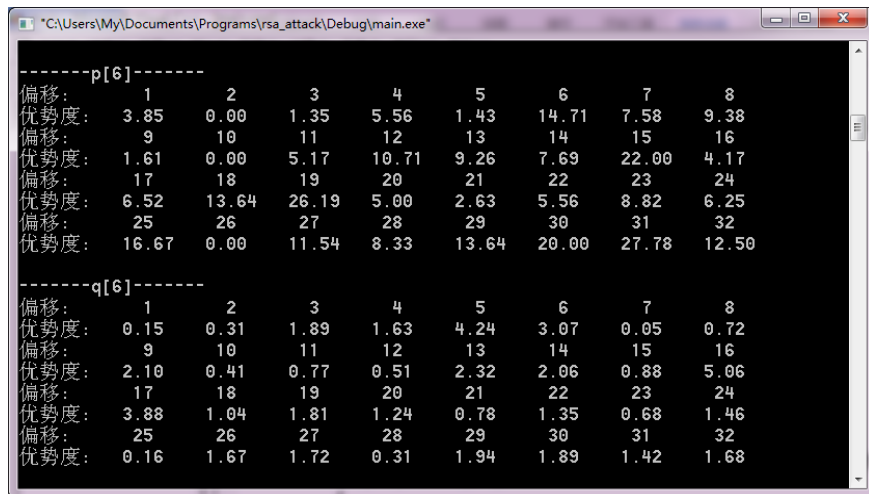


图 2.17 $p[6]$ 移加特性检验

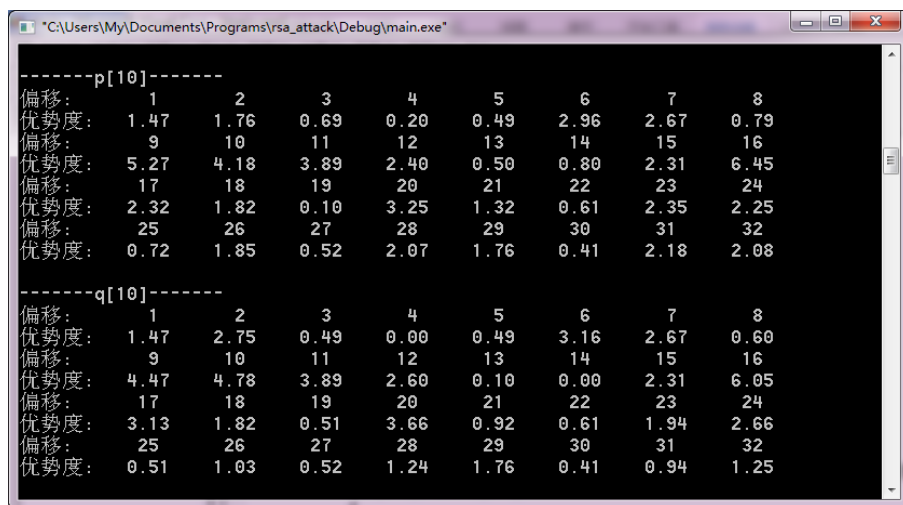


图 2.18 $p[10]$ 移加特性检验

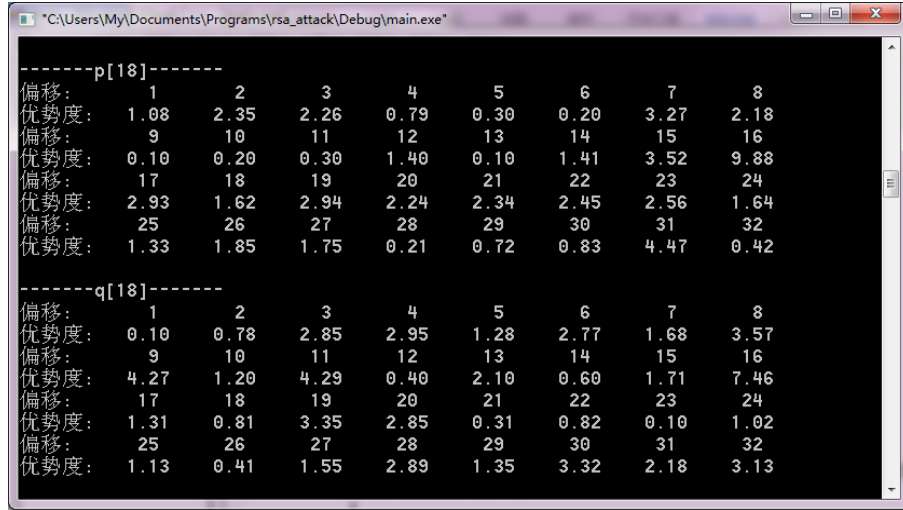


图 2.19 $p[18]$ 移加特性检验

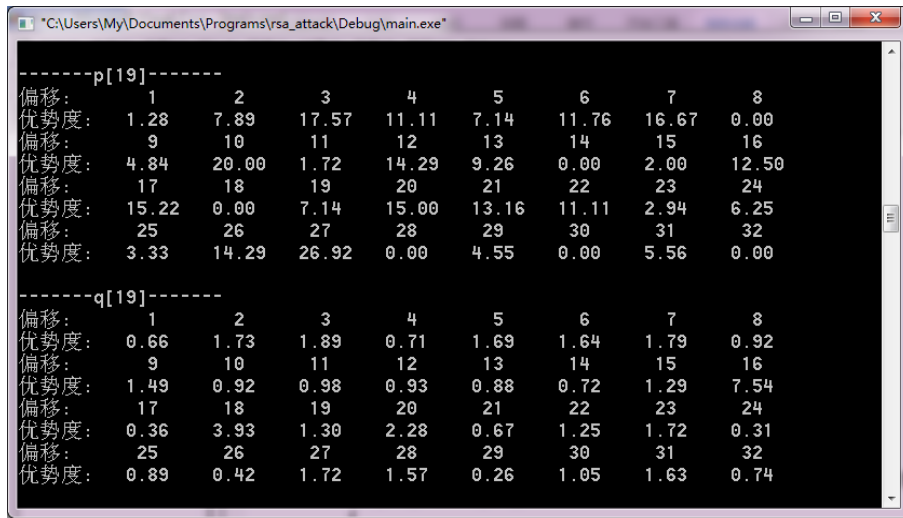


图 2.20 $p[19]$ 移加特性检验

其中优势 \mathcal{A} 定义为:

$$\begin{aligned}\mathcal{A} &= |(M(1)/M - 1/2) \times 100| \\ &= |(M(0)/M - 1/2) \times 100|,\end{aligned}$$

$M(1)$ 表示 1 的个数, $M(0)$ 表示 0 的个数, M 表示总比特数。

由于 p_6 与 p_{19} 较短, 其序列统计出的移加特性存在较大偏差, 不予考虑。将

其余 10 个素数的优势做成折线图进行比较分析, 如图 2.21:

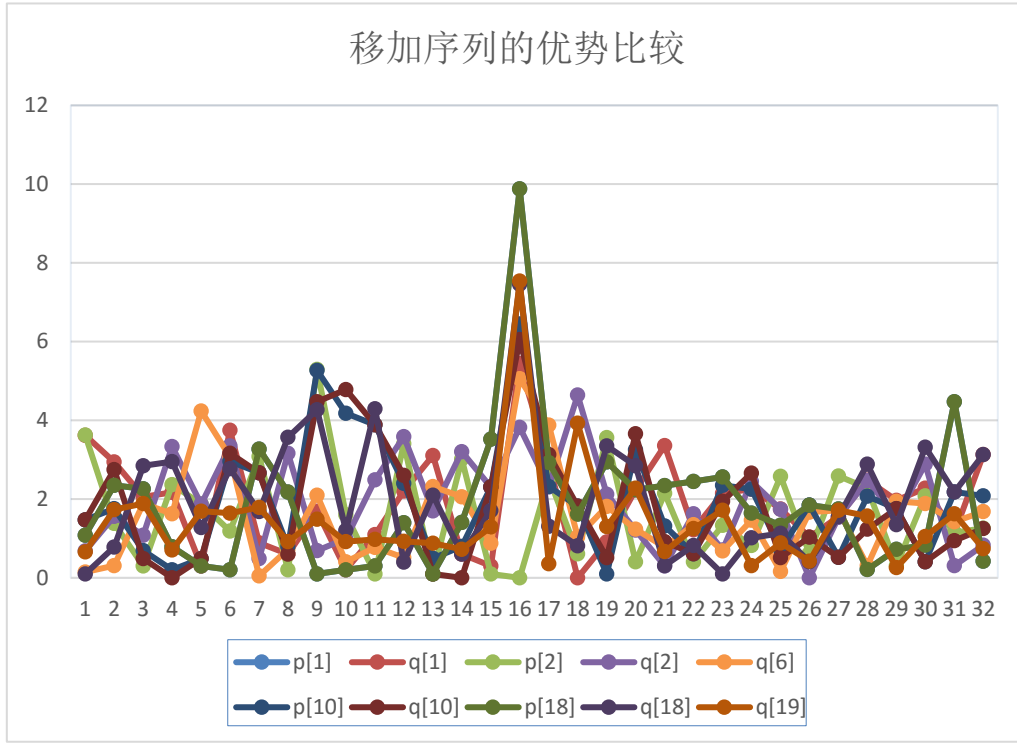


图 2.21 移加序列的优势比较

从上图的对比中可以发现，虽然 p_{10} 序列在偏移为 9 和 10 时优势比较高、 q_2 在多个位置都有较高优势，但从整体分析，在偏移为 16 时，除 p_2 以外其余 9 个素数序列的优势均明显增大。根据多个素数由同一随机数发生器产生的条件，可以认为，16（或其倍数）是该生成器递推关系中一个重要的周期参数。

4) 采样特征的检验

定义 2 对于序列 $a = \{a_i\}_{i=0}^{\infty}$ ， $a^{(k,j)} = \{a_{ik+j}\}_{i=0}^{\infty}$ 称为序列 a 的起点为 j 的 k -采样序列。称 $a = \{a_i\}_{i=0}^{\infty}$ 为被采序列， $a^{(k,j)} = \{a_{ik+j}\}_{i=0}^{\infty}$ 为采出序列。

鉴于上一环节中对移加特性分析得到的结论，可以选取 $k = 16$ ，即对序列进行 16-采样分析，采样序列如图 2.22：

```

"C:\Users\My\Documents\Programs\rsa_attack\Debug\main.exe"
*****采样特性分析*****
-----p[1]-----
起点为0: 1111001111010101111000001001
起点为1: 011010110010110101001011101001
起点为2: 011000100111101110011010101010
起点为3: 01001011010011100110110101111001
起点为4: 1101100110110010010001011010100
起点为5: 010001101101000101010110000110
起点为6: 111111101101100110101010101101
起点为7: 00111000001010001100110010111010
起点为8: 1110000110101110101001011100000
10000100111000000010011001001000
起点为9: 0010100000010010111001000011100
10011010000011100110010111110001
起点为10: 1001010001101011100101000110101
1001010001101011100101000110101
起点为11: 11010010110100101101001011010010
10011001100110011001100110011001
起点为12: 010101010101010101010101010101
10011001100110011001100110011001
起点为13: 010101010101010101010101010101
10011001100110011001100110011001
起点为14: 010101010101010101010101010101
10011001100110011001100110011001
起点为15: 010101010101010101010101010101
10011001100110011001100110011001
-----q[1]-----
起点为0: 11010001110001100100010000010100
起点为1: 11100101001110111001011110101000
起点为2: 101101101110010111111100110111
起点为3: 10100110000101101101100100111000
起点为4: 01100100010110110110111010010011
起点为5: 00001111111111000110111110010101
起点为6: 11110111100110110101100111011010
起点为7: 1011101101011110000100100011011
10000011100010001110011111110110
起点为8: 11011001101101110101001100001101
10110010000111001101011111101101
起点为9: 01100101111100011001101000001110
10010100011010111001010001101011
起点为10: 11010010110100101101001011010010
10011001100110011001100110011001
起点为11: 1111000111011010110000010100001
101101101110011001100110011001101
起点为12: 0100101100110001111011001000101
10110110101100001110010111101011
起点为13: 0110011010110000010110001000101
11111010011010011001100110011001
起点为14: 11111010011010011001100110011001
10011001100110011001100110011001
起点为15: 010101010101010101010101010101
10011001100110011001100110011001

```

图 2.22 对 $p[1]$ 进行 16-采样分析

观察结果可以发现：当 j 不同时， $p[1]$ 的采出序列的周期不同，当 $j = 15$ 时， $p[1]$ 的采出序列为“0101010101……”的循环序列。

对其余几个序列进行相同的检验，得到了相似的结果，程序显示如下：

```

"C:\Users\My\Documents\Programs\rsa_attack\Debug\main.exe"
-----p[2]-----
起点为0: 10111101000101010100000110100000
起点为1: 01010100000100000010100111111110
起点为2: 00100110100000000001111110011111
起点为3: 0011000011110010101010011110010
起点为4: 0100001011111111110000111011000
起点为5: 0100101101111110010101100111101
起点为6: 11110010100000100010110110101100
1101010011001110100010111001110
起点为7: 1101010111100101000010011111101
01000011110110001100110010110010
起点为8: 1101010111100101000010011111101
00110011100010011101000110001001
起点为9: 1111000111011010110000010100001
0100101100110001111011001000101
起点为10: 1011011010110000111001011101011
0110011010110000010110001000101
起点为11: 1111000111011010110000010100001
11111010011010011001100110011001
起点为12: 0100101100110001111011001000101
10110110101100001110010111101011
起点为13: 0110011010110000010110001000101
11111010011010011001100110011001
起点为14: 11111010011010011001100110011001
10011001100110011001100110011001
起点为15: 010101010101010101010101010101
10011001100110011001100110011001
-----q[2]-----
起点为0: 101101010000101011100101100010011
101010000111100111101000111001001
起点为1: 11101110010010100011110110000111
11001110010111010000001000100010
起点为2: 10101111101001001000100000101100
00111000001101001010111111111110
起点为3: 10100000000111010110000111100011
0110110011000001110110000010001
起点为4: 10110001011111000111011100011000
00011111110110011011011101010011
起点为5: 0001010101100100001110011010111
0001010101100100001110011010111
起点为6: 0001010101100100001110011010111
0001010101100100001110011010111
起点为7: 0001010101100100001110011010111
0001010101100100001110011010111
起点为8: 0001010101100100001110011010111
0001010101100100001110011010111
起点为9: 0001010101100100001110011010111
0001010101100100001110011010111
起点为10: 0001010101100100001110011010111
0001010101100100001110011010111
起点为11: 0001010101100100001110011010111
0001010101100100001110011010111
起点为12: 0001010101100100001110011010111
0001010101100100001110011010111
起点为13: 0001010101100100001110011010111
0001010101100100001110011010111
起点为14: 0001010101100100001110011010111
0001010101100100001110011010111
起点为15: 0001010101100100001110011010111
0001010101100100001110011010111

```

图 2.23 对 $p[2]$ 进行 16-采样分析

除去 p_6 和 p_{19} 由于长度过短，缺乏统计意义以外，通过观察，可以看出其余的 10 个素数序列中存在下述规律：

①当 $j=15$ 时， $p_1, q_1, q_2, q_6, p_{10}, q_{10}, p_{18}, q_{18}, q_{19}$ 这 9 个素数的采出序列均是 01 循环序列；

②当 $j=14$ 时， $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 这 8 个素数的采出序列的周期均为 4；

③当 $j=13$ 时， $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 这 8 个素数的采出序列的周期均为 8；

④当 $j=12$ 时， $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 这 8 个素数的采出序列的周期均为 16；

⑤当 $j=11$ 时， $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 这 8 个素数的采出序列的周期均为 32。

分析上述规律，可以得到以下三条结论：

①根据题目条件，每对素数中至少有一个由同一个素数生成器生成的素数。

经过 16-采样分析，在六对素数里，每一对中均至少有一个素数满足上述规律。

因此上述规律很可能是随机数发生器的特征，且 $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 则很可能就是该随机数发生器生成的素数。

②原素数在二进制表示下呈现出以 16 或 16 的倍数为周期的特征，因此，如果该规律是由于随机数发生器导致的，则该生成器的结构特征将可能与 16 有直接关系。

③将素数序列按每 16bit 为一组进行拆分，规定每组数最低比特位为第 0 位，最高位为第 15 位，纵向观察相同比特位的分布规律：第 0 位比特每 2 组为一循环周期，第 1 位比特每 4 组为一循环周期，第 2 位比特每 8 组为一循环周期，第 3 位比特每 16 组为一循环周期，第 4 位比特每 32 组为一循环周期，第 5 位比特至第 15 位比特因原序列长度有限，无法得出明显规律，但是可以推测：第 w 位比特可能每 2^{w+1} 组为一循环周期。这种根据比特位位置的不同而导致周期翻倍的

规律与带进位四则运算的二进制比特规律相同，其周期的翻倍是由于低位比特的进位而导致的。

在上述的分析中，我们在各种数字特征中，发现伪随机序列的结构即相似与移位寄存器序列的前后递推关系，即序列中可由前序列计算出后续序列（或由后向前），同时又符合同余发生器的四则运算特性。

我们先通过求解线性移位寄存器的方法，尝试计算出线性移位寄存器的反馈多项式，但在验证正确性时，发现其不能符合已知 12 个素数中任意一个素数序列，因此随机数发生器一定不是简单的线性移位寄存器。

通过翻阅文献，得知素数序列的前后递推关系的结构可以使用多个小整数级联的方式实现，如经典的 RC4 算法和 BBS 算法，将递推关系式中每次得到的随机序列串联得到更长的随机序列。因此该随机数可能也使用了该结构。

综合上述分析结果，现猜测该随机数发生器结构的基本雏形

$$X_n = f(X_{n-1}),$$

$$s = \overline{X_0 X_1 \cdots} \text{ 或 } s = \overline{\cdots X_1 X_0},$$

其中 X_i 长度为 16bit， f 为整数环上的某一多项式。

这一结构中的 f 函数的特征与同余生成器的结构十分相似，在当 f 为模某一整数下的一次线性多项式时，即为线性同余生成器。考虑到线性同余生成器是一种结构简单且普遍使用的随机数发生器，因此我们先尝试求解简单情况下的结果，即假设 f 为一次同余式：

$$X_n = aX_{n-1} + b \bmod m。$$

由于 $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 均符合生成器特征，但 q_{19} 包含有 p_1 序列，认为 q_{19} 和 p_1 是生成器产生的序列的可能性最大，因此将 q_{19} 序列每 16bit 作一划分，

将其分成 61 个子串（共计 984bit），并依次赋值于 X_0, X_1, \dots, X_{60} ，然后求解参数 a, b, m 。由于求解带未知模数的同余式是困难的（解不唯一），根据之前分析得到的 16bit 特征， X_i 的取值应当在 0 到 2^{16} 之间，于是先假设 $m = 2^{16}$ ，然后尝试求解同余式方程组，观察是否有满足方程组的解。解同余式方程过程如下：

$$\begin{cases} X_1 \equiv aX_0 + b \pmod{2^{16}} \\ X_2 \equiv aX_1 + b \pmod{2^{16}} \end{cases}$$

$$\Rightarrow X_2 - X_1 \equiv a(X_1 - X_0) \pmod{2^{16}},$$

$$\Rightarrow \begin{cases} a \equiv (X_2 - X_1)(X_1 - X_0)^{-1} \pmod{2^{16}} \\ b \equiv X_1 - aX_0 \pmod{2^{16}} \end{cases}$$

最终解得：

$$\begin{cases} a = 365 \\ b = 65535 \end{cases}$$

在模 2^{16} 下也可表示为：

$$\begin{cases} a = 365 \\ b = -1 \end{cases}$$

即随机数发生器的递推函数为：

$$X_n = 365X_{n-1} - 1 \pmod{2^{16}},$$

生成的序列为：

$$s = \overline{X_0 X_1 \dots}。$$

用其余已知的 11 个素数 $p_1, q_1, p_2, q_2, p_6, q_6, p_{10}, q_{10}, p_{18}, q_{18}, p_{19}$ 依次验证生成器的正确性，最终包括 q_{19} 在内的 8 个素数 $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 符合该生成器的生成规律，即可认为 $p_1, q_1, q_2, q_6, p_{10}, p_{18}, q_{18}, q_{19}$ 这 8 个素数由该随机数发生器生成的序列，同时也证明了该生成器的正确性。

使用上述分析得到的随机数发生器，遍历初值 X_0 ，然后截取所产生序列的

前 512bit 作为大整数 x ，依次与未分解的大整数 N 使用欧几里得算法求解最大公因子，若最大公因子不为 1，则其最大公因数即 x 为 N 的一个非平凡因子，成功分解大整数 N 。（由于 N 只有两个非平凡的素因子，若 $\gcd(x, N) \neq 1$ ，则必有 $\gcd(x, N) = x$ 。同样的，在求公因子之前不必先验证 x 是否为素数，若 x 不是素数，则必有 $\gcd(x, N) = 1$ ，同时一个素性检测算法并不比欧几里得算法更有效率。）

依据上述算法，成功分解出 $N_0, N_3, N_4, N_5, N_7, N_8, N_9, N_{11}, N_{12}, N_{14}, N_{15}, N_{16}, N_{20}$ 。

其分解结果如表 2.23:

表 2.23 分解模数结果

| Frame 0 | |
|---------|--|
| N_0 | 803F734ED9E3A3FBDEF8E3540B7B676FB66D15D2E5139840CB3C D06E62634C00A48EA2BF9BC3D7A709DBB47BE7E27DFB2C0E5B 81254E6C326691471AE6DDC4A35539018BA6305DAFF1C480F1951 18B1310C546C31FE62C7AEC2A947013AC2897D00FD60E7B792DD 499315341895BD1D1C9AA923E9373E1E01E2856B4FC8C6893 |
| p_0^* | 821273A9E7F4B6E3C1A619AD9BA8EE87167A0BF1069C6C6B948E CE755CD0548F8FE2253912440AF39C76143DDAF833978E4ADF81 AAECB27B795E0B05B620AB9F |
| q_0^* | FC68E047C53A33B1B35CBA2B6F4EB2351590BE4F56A284F997045 0B30F36AFFDEBB815576D0A774107ACF03B841E5EC51EE0055FA 8722A89A554B8C36E06DE8D |
| Frame 3 | |
| N_3 | 8365D1FF23709FAAEF6330AECA9C848B292E0872C5C41E8CBE9D 0780F32EBFC5FCC7947BD666F06AA619F952AFB8D7C08B921196 0D1916235D8AB3A60DEC45B1EF5CC21848E56D5235717186EAD5 1AE22A5661BDFDC42E31F9181F6AB1D070FDEBB078A9980D7A0 571B587130A1D3056CBA40CBBA287CD5031838BAB893B476B |
| p_3^* | 86B6117DEF3812D7DC8A70C1C32C45BB6B9E7045126032DF87F2 D40950D43E43C586A00D32880BE7F85A1851AB7C7FCB346EC0D5 EFB0BDEFCD25D9973242A53 |

| | |
|----------------|--|
| q_3^* | F9B405A30966666D096869471A3A64B1905CD32B144EF335C29067 4F4BA2D5F9140489B3543610FD38B8DE57020AE84124AC493B691 EDFC50BE0EE5FDD72BB89 |
| Frame 4 | |
| N_4 | 803F734ED9E3A3FBDEF8E3540B7B676FB66D15D2E5139840CB3C D06E62634C00A48EA2BF9BC3D7A709DBB47BE7E27DFB2C0E5B 81254E6C326691471AE6DDC4A35539018BA6305DAFF1C480F1951 18B1310C546C31FE62C7AEC2A947013AC2897D00FD60E7B792DD 499315341895BD1D1C9AA923E9373E1E01E2856B4FC8C6893 |
| p_4^* | 821273A9E7F4B6E3C1A619AD9BA8EE87167A0BF1069C6C6B948E CE755CD0548F8FE2253912440AF39C76143DDAF833978E4ADF81 AAECB27B795E0B05B620AB9F |
| q_4^* | FC68E047C53A33B1B35CBA2B6F4EB2351590BE4F56A284F997045 0B30F36AFFDEBB815576D0A774107ACF03B841E5EC51EE0055FA 8722A89A554B8C36E06DE8D |
| Frame 5 | |
| N_5 | 8D41AC379635A2C8FFA55F609BE3EB6219C7AD0D3C335AC1F7A E27C3C0510E9ACDE319A6E00B891BDDB05C6B53F62E9321340B C0F19727C0526AC811CC02C7229241045A3D125978C1181264FDE4 9D8A148AAD8A8796C12C2AB5E8D7B0F98EDAC907C092B70D8B 36E5BDC47C5801E4225BB508B1F081F5331C9B1324875EA25F |
| p_5^* | A2F2530963D4554390860F0D758892E7735A77511E7C76CB5F6E0F D592B024EFA8C29C9946240153E356219DECD8AFF7E32AE2E17A CC14DBBC3E6465240053FF |
| q_5^* | DDEC697B645E1A051920D29F4CB259C903941A031646C1CD5148 E3A7951A9611F63C138BDD2E5A952670CDAF4282D35955E476135 916045D3898B0B7F4EA31A1 |
| Frame 7 | |

| | |
|----------------|--|
| N_7 | DD1B58FF0DE86CD28DFFB60CC1EE0EFA3250D58264B3DA9CEA A5B5C17C728741F728C462C347DCB707BA7EE8672295F5A750C19 D48AE23A32FC21E76F3188B85008E4EC1A66371BBB0825E558E87 6D80FA59E7099AF25B0B298131277E634772F24EE0ED1BACD3BA 6F8D8E443D5AE16FAF6AA7DBAA59F91F763E4EAFD7D7F5CD |
| p_7^* | ECE0BB5F2672D0895354CEC3CC06E48DDD082467E6DA24D17DF CA04B8AEE15556A30666F0C427A1915A4DAD3FED6571D3458A1 7736AAF061BA4C9E5BC7BEC9E5 |
| q_7^* | EEF4B1E3A0A60CAD12A89987E57A2EF1ED9CC76B538E2175B3D 05F8F3EE2A839D944C5F33B76C73D11F89E971D4AC28151ECCD7 BF85E1E05CD20769F20B29DC9 |
| Frame 8 | |
| N_8 | 9288E1EEF599EA72113D950723A8FC0ADD096C7312D8E78911FE6 4A4322C4FEC96FD70B345AA5A345481FB91D8549998A90E2429D CAF1EEEC863F396479A0BBD121E36B0EFAC8D002FC95B58B587 9DD75251B5CEFCBE90BF50669742821BE2E89B3831FD6F0F3EAB 310E5BF3FC66D702D5FF1581EE1DEFF161EFCA359063C6AB |
| p_8^* | A526772DEB284807B1FAC171CE1CDDEB680E5BF51C505E0F1B62 0AB949C42C735FF6D1BD0A78ED1709CAF501526C83FB2CDEF88 555A0151F1D32A04988140483 |
| q_8^* | E324DA534856229D59D818F7982AF3E1B7CC0DDBC13E85653100 DCFF17929B293974EA632F26392D8528DA07DBFAA371081C8FEB 320E5DF5F650300F85622CB9 |
| Frame 9 | |
| N_9 | 8B39E72D3C13D48F7773118B19F0D1A0CC592FD8FF12469E1D51 ABA8869A23297CD62E28BCF885F744BD4A7C53CB5369F941F401 EC010DA8665B7EB0B17B1839B3F0E49B51A266DDB84899EB302E 050E43A284B5051C5B9002BA2B8BF1DD3A22C0BAB03A6E780F2 18852EE086F05E9ADF290189439AFF15986077D36D271C9A1 |
| p_9^* | B6E2C03911449DF333765F3DC9F8F697954ADA8189ECA57BF05E B6058520CE9F98B2B5C92F94D6032246DDCD3D485FA7611A7211 A23C4F8B692EF6959270C9AF |

| | |
|-----------------|--|
| q_9^* | C2E2DC39FD4419F3FF763B3D75F83297214A7681F5ECA17B3C5E1 205B1208A9FA4B2D1C91B945203EE46B9CDE9489BA7ED1A0E110 E3C4B8BB52E5295BE7085AF |
| Frame 11 | |
| N_{11} | 9FEDDC9C122AA836E9A04FE9358A118B358C7BC6F3ABDE4E035 E2BCB15B52950DB1D23449EA62F83406FB591ED39564FD0E2DA D0954156037BB32C9C23C49DA83E2E85BC09A9B6FD75E2F55129 044FA0F996895E8BF5E53D88938E4A3366649E97961BE5B7B40954 76D013D2E9F6FE75DC21295747BF371AE346355A5ADBD93F |
| p_{11}^* | C9C4AC73DFF651BD8A786D1789CA7501D26C03FBACDE7885D5 A0951F9D32204908148483EEC6704D1DC87627759AAC910ABC4E0 B45AE591502F0302FB30239D9 |
| q_{11}^* | CAEA4FA1888CAF9B5FFEDD254DC0DABFE252AEE962340423E5 E6C8ED79E8CFC73EBA6F3188DC21AB00CE25B5C3101DCF8022B 0799C84283350B6137DC938E4D7 |
| Frame 12 | |
| N_{12} | 808B8F96E7255B3F169EE854ABE0CD0AC7A4AE1B388CBC9A234 E225842208A435842C254A55855B867F3FCA78E3887C8D1663B501 A5D4D5E32F3EF84847F45651A5E2FC8A091E12E2B4DB7AB41113 D258E2200FFB2BBF8B7C38B0049B3E2E60C65EB8B6375F03A40D C9F9AB01FEC60E09DC8CA3644A83738BDA0CFDB2B5ABB3D |
| p_{12}^* | 85622CB9C3C41E7369F613BD2478FF17B3CA57010C6CB5FB76DE 7A85AFA0671F0732424982147683F8C6B24D37C888271F9A0E91C4 BC800B8FAEDB155CF0822F |
| q_{12}^* | F6B6C17DDF3842D74C8A20C1B32C75BBDB9E2045026062DFF7F2 840940D46E433586500D22883BE7685AC8519B7CAFCBA46E70D5 DFB0EDEF3DC20D9963245A53 |
| Frame 14 | |

| | |
|-----------------|---|
| N_{14} | AAE5F7D640FD102E49217A08E0A4AF72EC895D5ABA020BEAF6F73053F4053D47CB7EBF3D583532ABFFF50F69508A4DBF2421742DCC2C16AE00E88C237653EC4DCFCDD9A918763A9C9DE3CE3DA1FE2BC94FF93A9A7C261400A6E363C66816FDA0E44EE73662CFD2B8BFA926EF2B40F7D41F35B7E89516BC28330B5CF49976B8D7F |
| p_{14}^* | D12A38E118CC5ADB8A3E1A65A200F9FF70928029BA74D76318266E2D1628970754FA2871A91C1CEB3B0E32F5A7508D0F1E6251B984C44B7392F688BDF578FC17 |
| q_{14} | D12A38E118CC5ADB8A3E1A65A200F9FF70928029BA74D76318266E2D1628D708F61CF38BDB569321B9F5C0672E5BFE43A67EF230D650CC03A6A51784B065D2D9 |
| Frame 15 | |
| N_{15} | D2611805B6839FD983F2C574BDAD1C50A4FB9FAB35F3BB643F90A9FBB0B84AF1D042E35E821564FCA783F1A2AF41349BB3E1C159B20EA6A0DB9E70597CB5C0780EF6CD78481AEAC0DF65A8DE35A8B5021FCE55332C5B2ADAEDCF80963BD6FFF773CAB55D73637C9BD667148FB1359782D38C41CBB43FA5FD56F424F842D8683D |
| p_{15}^* | E79833B7BBEAECA1618C149B60FE4A25B6C08FBFF352EBE95B34092306E6D5ED02E824C76FBA4C31A1DCC6AB41CED2B56C1012CFD1222D79D5846D33B1B6607D |
| q_{15}^* | E88C8F9BBFFEBD25ADC0BABF42528EE9C234E42345E6A8EDD9E8AFC79EBA4F31E8DC01AB60CE05B52310FDCFE0229079FC840833B0B6F37D2938C4D7A68A72C1 |
| Frame 16 | |
| N_{16} | 811F75BEAD6F0C3EA1560CFA4BFD4762F1DA3A30E22644AB16B1BEA5A6A1AF14F0C3C2E63865FD29241246C1473892232DAB6224AF1600F73340BCA7BF5AF01EA1FA007E46064CE2F8DD92A9E7FA9F16CFEEE5A6CF67683BCD97F1E7E1BA73A9F86A8E4D7496393AC9727D10530A76B03B3A23321E8BDD756FCE265494F6D35 |
| p_{16}^* | 859E8245BC6094DF41F206099AD4C0431F86F20D1C88ADE7F25A8A51357C41CBCE6E52D519B09FEF07C20F993D242C533256C49D53D88AF7222AB5E151CC9FDB |

| | |
|-----------------|--|
| q_{16}^* | F762B6B985C4B873FBF63DBD0678391765CA21010E6C8FFB48DE E485D1A0E11FF9324C49C41490830AC65C4D99C84227519A589146 BCDA0BE1AEC515FEF07C2F |
| Frame 20 | |
| N_{20} | 8178408D7E1155B9F5B0665A3EDFE279189567AAC333CA33A7304 AE1BB9C9A921735888FB7BC9B41550817B1C0D42B2AB03045467 09648F45147180AD5FC839FB8F90B2D30772718A7B45E6204CE788 6122874759F93C198CE61D10555F03C13FD83E639A637D849C846D 5589029533E567E12FD992D690EC5EF38569327FC8D |
| p_{20}^* | 85C6BB4D0CC839277C9AA791E9BC410BBCAE0415D1F0532F9A0 294D93964D393A8965DDDD4186637BC6AA321960CEF1BE97EE8 A5B340923F83D2F2699FB4B3A3 |
| q_{20}^* | F7C23F99AD24DC532256F49DC3D83AF7122AE5E1C1CC4FDBDB 3E9765DB003EFFD192CD2983746C6389268B2D6F287C07D5FA157 1921C51EBCC0EEFF52050120F |

在上表中，用*号标记的 p 和 q 是由该随机数发生器生成得到的，即在 $N_0, N_3, N_4, N_5, N_7, N_8, N_9, N_{11}, N_{12}, N_{14}, N_{15}, N_{16}, N_{20}$ 这 13 个大整数的素因子 p, q 中，除了 N_{14} 的一个素因子外，其余的 25 个素因子均是由该随机数发生器生成的。

至此，一共有 19 个 RSA 模数被成功分解，但仍有 N_{13} 和 N_{17} 两个大数未能成功分解。再次分析观察已经得到的素数，可以发现问题在参数 p 和 q 的选取上——并非都是选取 512bit 长。在之前得到的 12 个素数中， q_6 和 q_{19} 是由该生成器产生，但长度为 984bit， q_2 同样由生成器产生，长度为 514bit。因此猜想 N_{13} 和 N_{17} 的素因子可能长度不为 512bit。调整算法参数，将初值遍历后产生的序列截取 40 至 984bit，然后再依次计算与 N_{13} 和 N_{17} 的最大公因数。（实际操作中为了节省时间，不会直接对 946 种截取情况进行遍历，因为这可能需要十几分钟，虽然可以忍受但并不高效。我们采取的做法是缩小范围依次尝试 500 至 520bit、470

至 500bit、520 至 550bit……实际在第一次截取 500 至 520bit 时已经计算出结果。)

最终成功计算出 N_{13} 和 N_{17} 的素因子。由表 2.24 列出:

表 2.24 分解模数结果

[illegible]

同样，带*的素数为该随机数发生器产生的，其长度为 514bit，符合我们猜想的结果。

至此，对题目中的 21 组 RSA 模数 N 全部分解成功。最后利用分解得到的 p

和 q 计算出解密私钥，解密得到明文信息，获得 21 组数据帧中的全部明文与加密参数信息。

2.6 结果检验

得到全部加解密参数及明文消息后，我们对所有的结果进行了检验。还原随机数发生器之前，无法判断破解出的参数究竟是不是由随机数发生器生成的。确定了随机数的生成规律后，我们对所有的素数进行了检测。

根据随机数的产生规律，逐个对第 2 节和第 3 节中破解出的模数进行了验证。最终发现，Frame1 与 Frame18 的两个素数参数都是由随机数发生器生成的素数，其余四个分片 Frame2、Frame6、Frame10 和 Frame19 中，均有一个素数参数是由随机数发生器生成的；在第 5 节中破解出来的素数，也都验证了它们是否是由随机数发生器产生的。具体结果见附录 3（16 进制）和附录 4（10 进制）。

最后，根据题目中的加密规则与加密参数，我们对每一个分片的明文序列进行了加密验证，将计算得到的密文序列与题目所给的密文序列一一比对，验证了所有明文消息与加解密参数的正确性。

3. 小结

3.1 解题方法总结

本文综合使用了费马分解法等常规攻击方法、因数碰撞法、猜测明文攻击和随机数发生器攻击方法完全破解了题目，得到了所有的明文和参数。其中，利用不同方法得到了各个分片的破译结果，具体见表 3.1：

表 3.1 解题方法总结

| 攻击方法 | 破解模数 | 破译明文 |
|-------------------|--|---|
| 费马分解法 | Frame 10 | Frame 10 |
| Pollard $p-1$ 分解法 | Frame 2、Frame6、Frame 19 | Frame 2、Frame6、Frame 19 |
| 低加密指数攻击 | 无 | Frame 3、Frame8、Frame12、 Frame16、Frame 20 |
| 公共模数攻击 | 无 | Frame0、Frame 4 |
| 因数碰撞法 | Frame1、Frame 18 | Frame1、Frame 18 |
| 猜测明文攻击 | 无 | Frame 5、Frame7、Frame9、 Frame11、Frame13、 Frame14、Frame15、 Frame17 |
| 随机数发生器攻击 | Frame 0、Frame 3、Frame 4、 Frame 5、Frame7、Frame 8、 Frame 9、Frame 11、Frame 12、 Frame 13、Frame 14、Frame 15、 Frame 16、Frame 17、Frame 20 | 验证了全部明文的正确性 |

3.2 结果分析

破解了全部 RSA 加解密体制参数并破译了全部的明文信息后，我们回顾了整个过程中所采用的攻击方法和程序运行的效率，对 RSA 加密算法的原理、应用与破译有了更深入的了解和认识。综合破译结果，对 RSA 加密算法设计过程中的一些经验进行总结。

1) 参数的选取

(1) 关于素数 p 、 q 的选取

首先我们采用了两种常见的整数分解法——费马分解法和 Pollard $p-1$ 分解法，成功地分解出了四组模数。这两种整数分解法都是确定性的算法，通过寻找特定的条件，使得素因数在某区间分布的概率大大提高，这样一来，算法的实现过程就变得简单可行。只要选取的素数符合某些规律，其生成的模数就存在用该类方法破解的安全威胁。

此外，如果用同一个素数生成两个不同的模数，也存在通过求两个模数最大公因数进而成功分解的可能性。总结了这些方法的攻击特点，RSA 算法设计者在选择素数时应当注意以下几点：

表 3.2 RSA 密码体制中素数的选择

| RSA 密码体制中素数 p 、 q 的选择 | | |
|---------------------------|--------------------------------|---------------------------|
| 1 | p 、 q 的长度不宜相差过大 | 防止被试除法轻易破解 |
| 2 | p 、 q 的在数值上的差距应当尽可能大 | 防止被费马分解法轻易破解 |
| 3 | $p-1$ 和 $q-1$ 有大的素因数 | 防止被 Pollard $p-1$ 分解法轻易破解 |
| 4 | 选择 p 使得 p 和 $(p-1)/2$ 均为素数 | 防止消息加密后没有被隐藏 |
| 5 | 不要用同一个素数 p 生成不同的模数 | 防止被因数碰撞法轻易破解 |

然后，我们利用已知的六组素数参数，分析它们之间的关系，找到了随机数产生的规律，最终还原了随机数发生器，进而求出了所有的素数参数。这也向我们证明：如果采用数学方法生成伪随机数，就存在随机数发生器被还原的风险。所以，我们在选择随机数时，应尽量减弱随机数之间的相关关系，可以采用增大随机函数的复杂性的方法，例如增加代数次数、线性复杂度等^[15]。

(2) 关于模数 N 的选取

根据公共模数攻击的原理，我们成功破译 Frame0 和 Frame4 的过程，耗时仅 0.03 秒，由此可知，将同一个明文信息发送给不同的人时，尽量不要选取相同的模数 N 。否则，当窃听者截获加密后的不同明文后，仅根据已知的公钥，就能够恢复明文消息。

此外，不同的用户应该选用不同的模数 N ，用户之间不能共享。这是因为，当某中心选择公用的模数 N ，然后把 (e, d) 分发给众多用户，任何一对 (e, d) 都能分解模数 N ，从而，本质上来讲，任何用户都可以求出共享该模数的每个用户的解密密钥 d ^[16]。

(3) 关于加密指数 e 的选取

为了提高运算效率，RSA 算法设计者常常选取较小的加密指数 e 。然而，利用很小的 e ，不同的模数，去加密同样一段明文信息时，系统将是非常危险的。若密文不慎被攻击者截获，仅根据加密指数 e ，就可以有效地恢复明文信息。

所以，在选择加密指数 e 时，应尽量选择 16bit 以上的数，即不影响计算效率，又保证了算法的安全性；另外，当明文信息很短时，可以使用独立随机值填充的方法，降低明文信息的相关性，使得攻击者无法用低加密指数攻击法破译算法系统。

2) 对明文的要求

在本题的破译过程中，我们用到了猜测明文攻击的方法，根据已知的 8 个明文片段，通过互联网搜索，结合语义、语境的判断，最终恢复了全部明文信息。这也证实了，当明文空间较小时，猜测明文攻击是一种有效的攻击方法。

要想避免以这种方式破译出明文，我们在与特定对象进行通信交流时，可以提前商定某种语法规则，使得语言表达的意思不是其本身的意思，这样，即使消息被中途截获并破译，攻击者也无法理解明文所表达的意义；或尽可能地增大明文空间，并提前商定哪些字符不具有语义，也能有效防止攻击者对明文消息的恢复；还可以将明文分片加密后打乱顺序随机发送，采用只有合法接收者才能还原的发送顺序，即使消息全部被破译也难以恢复成完整的具有明确语义的语句，降低猜测明文攻击的可行性。

参考文献

- [1] Whitfield Diffie, Martin Hellman. New Directions in Cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644-654.
- [2] Ronald Rivest, Adi Shamir, Leonard Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. *Communications of the ACM*, 1978, 21(4): 120-126.
- [3] 谢健全, 杨春华. RSA 中几种可能泄密的参数选择[J]. *计算机工程*, 2006, 32(16): 118-119.
- [4] 王小云, 胡磊, 王明强. 公钥密码发展研究[A]. 2014-2015 密码学学科发展报告[M]. 中国科学技术出版社, 2016.

- [5] 张乐友, 胡予濮. 公钥广播加密的发展现状[A]. 中国密码学发展报告 2011[M]. 电子工业出版社, 2012.
- [6] 王小云, 王明强, 孟宪萌. 公钥密码学的数学基础[M]. 科学出版社, 2013.
- [7] Joppe W. Bos, Alex Halderman, Nadia Heninger. Elliptic Curve Cryptography in Practice[A]. In: Proc. *Financial Cryptography and Data Security*[C], LNCS 8437, Springer-Verlag, 2014: 157-175.
- [8] 龙建超. 公钥算法中大素数生成方法的研究改进[D]. 昆明: 云南大学, 2014.
- [9] 谭阳, 关于随机数生成算法的研究[D]. 长沙: 湖南师范大学, 2008.
- [10] 杨雪, 关于随机数发生器的综述[D]. 长春: 吉林大学, 2006.
- [11] Microsoft Visual C++, <https://www.visualstudio.com/>.
- [12] GMP package, GNU Multiple Precision Arithmetic Library, <https://gmplib.org/>.
- [13] Miracl package, <http://www.shamus.ie/>.
- [14] 张广强, 张小彩. 混合线性同余发生器的周期分析[J]. 商丘师范学院学报, 2007, 23(6): 40-12.
- [15] 吴飞. 产生随机数的几种方法及其应用[J]. 数值计算与计算机应用, 2006, 27(1): 48-51.
- [16] 孙淑玲. 应用密码学[M]. 清华大学出版社, 2003.

附录

附录1 明文信息

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|--|--|--|--|
| 通讯序号 | 0 | | | | | | | | | | 1 | | | | | | | | | | 2 | | | | | | | | | |
| 明文 | M | y | | s | e | c | r | e | t | | i | s | | a | | f | a | m | o | u | s | | s | a | | | | | | |
| 通讯序号 | 3 | | | | | | | | | | 4 | | | | | | | | | | 5 | | | | | | | | | |
| 明文 | y | i | n | g | | o | f | | | A | l | b | e | r | t | | E | i | n | s | t | e | i | n | . | | | | | |
| 通讯序号 | 6 | | | | | | | | | | 7 | | | | | | | | | | 8 | | | | | | | | | |
| 明文 | | T | h | a | t | | i | s | | " | L | o | g | i | c | | w | i | l | l | | g | e | t | | | | | | |
| 通讯序号 | 9 | | | | | | | | | | A | | | | | | | | | | B | | | | | | | | | |
| 明文 | | y | o | u | | f | r | o | m | | A | | t | o | | B | . | | I | m | a | g | i | n | | | | | | |
| 通讯序号 | C | | | | | | | | | | D | | | | | | | | | | E | | | | | | | | | |
| 明文 | a | t | i | o | n | | w | i | l | l | | t | a | k | e | | y | o | u | | e | v | e | r | | | | | | |
| 通讯序号 | F | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 明文 | y | w | h | e | r | e | . | " | | | | | | | | | | | | | | | | | | | | | | |

将所有分片的明文信息按照通信序号连接起来，得到通关密语：My secret is
a famous saying of Albert Einstein. That is "Logic will get you from A to B.
Imagination will take you everywhere."

附录 2 通讯序号与接受序号对照表

由于存在重复发送的分片，所以不同的分片对应的明文消息可能是相同的，
通讯序号与分片的对应关系如下：

| | | | | |
|------|----------------|---|---------|---------|
| 通讯序号 | 0 | 1 | 2 | 3 |
| 分片 | Frame0, Frame4 | Frame3, Frame8, Frame12, Frame16, Frame20 | Frame7 | Frame11 |
| 通讯序号 | 4 | 5 | 6 | 7 |
| 分片 | Frame15 | Frame19 | Frame2 | Frame6 |
| 通讯序号 | 8 | 9 | A | B |
| 分片 | Frame10 | Frame14 | Frame18 | Frame1 |
| 通信序号 | C | D | E | F |
| 分片 | Frame5 | Frame9 | Frame13 | Frame17 |

附录3 RSA 加解密参数表（16 进制）

| Frame 0 | | | | | | | | | | |
|---------|--|------|---|---|--|---|---|---|---|---|
| N | 803F734ED9E3A3FBDEF8E3540B7B676FB66D15D2E5139840CB3C D06E62634C00A48EA2BF9BC3D7A709DBB47BE7E27DFB2C0E5B 81254E6C326691471AE6DDC4A35539018BA6305DAFF1C480F1951 18B1310C546C31FE62C7AEC2A947013AC2897D00FD60E7B792DD 499315341895BD1D1C9AA923E9373E1E01E2856B4FC8C6893 | | | | | | | | | |
| p^* | 821273A9E7F4B6E3C1A619AD9BA8EE87167A0BF1069C6C6B948E CE755CD0548F8FE2253912440AF39C76143DDAF833978E4ADF81 AAECB27B795E0B05B620AB9F | | | | | | | | | |
| q^* | FC68E047C53A33B1B35CBA2B6F4EB2351590BE4F56A284F997045 0B30F36AFFDEBB815576D0A774107ACF03B841E5EC51EE0055FA 8722A89A554B8C36E06DE8D | | | | | | | | | |
| e | 42A04A989C5800528EF687C978355E9C4AFD410A9DD4B08CCA76 69C747CCE5446D5E85022CA2A2C383C28E85AD038C37CED2E18 BD88529BD2480E20191958497C61823378CA06DE01C8B6FB148C9 BC935E433EFCD960A1BF841FD60599811941A122CB1A323A76367 EE78D71870B7134881CA077518C809013AE8EC6BAECD519 | | | | | | | | | |
| d | 5B3B2DA24B37CED4E91817CA8A52A0AC2D870C23C65D1E71723 68544192A6D48C301F947394AE86093905F7949E82247B52F043E78 01EA7A3562D6E27687A5F4DB1DC4959F5BED65A7B12595DC4775 257E03AFC86DF4311DD150249CB6A74384771CA87C62114130B0D 79F4815B39057C452BBDF438B69537FE874C5A1A542F9 | | | | | | | | | |
| c | 45446FC78AC9AA9F2E38197D44B76F0C2A7DED354615D9066080 16E9F884FA51E20893FA0AEAF5975E28A68FBCD9BA469EA00263 F812523EEC79E0CF967190317BEF53EE8FF29AF4411A238E7FCE1 48AE7603C9A1DEC4EEAC1E41AD5FB8725FD3DCE4C058DB10F2 79B3EC1FA3EBC6584547D29501CCA52851148344316073E6B | | | | | | | | | |
| m | 9876543210ABCDEF000000000000000000000000000000000000 0004D 79207365637265 | | | | | | | | | |
| 通讯序号 | 0 | 明文分片 | M | y | | s | e | c | r | e |

①本附录中带*的 p 和 q 是由随机数发生器生成的。

| Frame 1 | | | | | | | | | | |
|---------|--|------|---|--|---|---|---|---|---|---|
| N | 845334AC0B3EB2239FDF0E3069750901E791CB774AD36941E30D8 5E5A0FED57749A30DC1F1F4CB191D9863F437C98293E8E8888B96 3BCF16B691F1D4EEF56C6807440E5FB5EC5B95DF3434DEDA30C6 0DCB4E77294BE027F984D5E675AEB1CBBE57E8CAF140226EAD6 DCD9A9636A0CFF586FA434804CB09D7E8C48DE34EBE9049 | | | | | | | | | |
| p^* | 8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39 A5291B8BC640BA3AE5F1590F0A62FF1029FD9E86456936F9618DD 73181937F36A0E21250CD21B | | | | | | | | | |
| q^* | F3EECA557B30A36F05427F1936A4E7D387D6AC1D65587E774FAA 9561FB4C4B5B70BEBEE52C80727F3F12ECA96CF457E34EA622AD 70A89F87737AA4F12B9C2D6B | | | | | | | | | |
| e | 10001 | | | | | | | | | |
| d | 4CCA3C76DACFB7711505CCA62B8CCF7D5B75302E3A2E159736B C5247BFF622CAE6E0C8CB142E8AEE384E8732E26CFE69F76F7A4 E07110E4C900681E0A00BACAC93E48ED30DF9A75802261B201AB A465D7207B191CE41F1ECBEBFF5F258146B6DF8AB7CE45153B82 3A28D7D1D57BF14310F2DB82FF94C9363357B42F0A582BE5 | | | | | | | | | |
| c | 0251025DC5FB84476581D0F67C640D8927DA6D083627C9C29F317 4C17CFE316A6218194DD4BE03D30EF9ECCBB4C609673D853590D D122B151DCFD6D75FD202DC2C758E897BABE0A4CD842FF35D0 86CF4E34EFBD09E8FF9FBFB4B5254CA2323A463139ABD16E301C 37F683579BA624EFBB297B9E6D5A1C68F75EB4BADF9AA198C | | | | | | | | | |
| m | 9876543210ABCDEF0000000B0000000000000000000000000000 002E 20496D6167696E | | | | | | | | | |
| 通讯序号 | B | 明文分片 | . | | I | m | a | g | i | n |

| Frame 2 | | | | | | | | | |
|---------|--|------|--|---|---|---|---|--|-----|
| N | 808627CED38A980D765454AC5DFEFC10195F6FEF9B35B52B742D BCE2419C34080A3EF3E9673FEA4DD629FF382155031EA6DCBA83 72D42C1862F32B2BEE47E157FA7150C544635035F366F7D68234F5 6FA24180EB6A00A0F85C65AAEB455B8ED28F2285376CDA786F8C 658CFEB3752F3504A7256EA3DBD22EEF20267D156FAB51 | | | | | | | | |
| p^* | 3EA18C437BE22139DF56AE544E1F2232C25B9C75532C15BBFCB0 87A6680914D4F355B0E779B6087DDB4AA938453329B6F98F919957 80017FE3249B0A4D9D28D8F | | | | | | | | |
| q | 20D553F6EC8DF4DD610278518BABE13E0EFD87744717F733836C6 34407D0230E467B622F9787080ADDE08CB349423BC93EFD965375 B51F301BD9D9D25C61891F | | | | | | | | |
| e | 10001 | | | | | | | | |
| d | 759C4E6951E38DE923D35FF8ABBB5E664D11AC9912EB3EF298C A1202EA0F4AFDE0826329BF3619EF487FFDF11B6F73FF64AAB07 3016D6F3C91AFFC5DA31B5BF33746594E57305BFF450E943CF79A 78CC82C4E7C36EC448FD0F18C07AF173E0D339E97117DA2F92E1 915A74186BD000B3DF214B2A24D98716383B717B5E206391 | | | | | | | | |
| c | 38702EF6FD51CA1CA834EF495618DA956C8F8AD222B99E256ED5 E3DD9089E194DE67FD427F6132715709830A73B1A1CB582E56D06 AF8F31BBA2851DBA1A1C2985B7FC233018E42554C2AABD69A22 5F9283A164C3AA5479363F89260219F9964738B7C78C5D08618009F 3904EB55A6A570E8D4B1701F4BF1B2C99C7887CCFF2C9 | | | | | | | | |
| m | 9876543210ABCDEF00000000600000000000000000000000000000 000 54686174206973 | | | | | | | | |
| 通讯序号 | 6 | 明文分片 | | T | h | a | t | | i s |

| Frame 3 | | | | | | | | | |
|---------|--|------|---|---|---|---|---|--|--|
| N | 8365D1FF23709FAAEF6330AECA9C848B292E0872C5C41E8CBE9D 0780F32EBFC5FCC7947BD666F06AA619F952AFB8D7C08B921196 0D1916235D8AB3A60DEC45B1EF5CC21848E56D5235717186EAD5 1AE22A5661BDFDC42E31F9181F6AB1D070FDEBB078A9980D7A0 571B587130A1D3056CBA40CBBA287CD5031838BAB893B476B | | | | | | | | |
| p^* | 86B6117DEF3812D7DC8A70C1C32C45BB6B9E7045126032DF87F2 D40950D43E43C586A00D32880BE7F85A1851AB7C7FCB346EC0D5 EFB0BDEFCD C25D9973242A53 | | | | | | | | |
| q^* | F9B405A30966666D096869471A3A64B1905CD32B144EF335C29067 4F4BA2D5F9140489B3543610FD38B8DE57020AE84124AC493B691 EDFC50BE0EE5FDD72BB89 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 4ED6B132AEDD2C99C2D51D35ACC44F86B24ED1DE76A8DF213F 2B048091E8D976CADE25E3E70A903FFD42C8CB363BB4A6BA247 0F3A17573AED1B99EFD3B8DC369DC2B3361302A926E62E58E186 E7576ACB569DEFB810C9E779BF2EF3E0CCF37A70AE32F58A3FC 6B1359FB23730459DE93118567FFC5D4E95D34B9BFD1552F6DBD | | | | | | | | |
| c | 76CBCAF659936784799208C3EE2420B7BBFDBB9AA8D7C89874C1 1314DF5DECD3AA97F3DA89851A043AF16E6570E7D03A4F3225D 49E552FAA2FB9F6A19AE95BA73ECD6E7CC05CD9C03E03E06F82 9042DBA4C1A91F39AC0CAD516C8DE7FB45939A2038C24C13F7F 62A20040473D8F3D8339A4B30A65715F98A43CC3293E51190D5 | | | | | | | | |
| m | 9876543210ABCDEF00000000100000000000000000000000000000 000 20697320612066 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | i | s | a | f | | |

| Frame 4 | | | | | | | | | | |
|---------|--|------|---|---|--|---|---|---|---|---|
| N | 803F734ED9E3A3FBDEF8E3540B7B676FB66D15D2E5139840CB3C D06E62634C00A48EA2BF9BC3D7A709DBB47BE7E27DFB2C0E5B 81254E6C326691471AE6DDC4A35539018BA6305DAFF1C480F1951 18B1310C546C31FE62C7AEC2A947013AC2897D00FD60E7B792DD 499315341895BD1D1C9AA923E9373E1E01E2856B4FC8C6893 | | | | | | | | | |
| p^* | 821273A9E7F4B6E3C1A619AD9BA8EE87167A0BF1069C6C6B948E CE755CD0548F8FE2253912440AF39C76143DDAF833978E4ADF81 AAECB27B795E0B05B620AB9F | | | | | | | | | |
| q^* | FC68E047C53A33B1B35CBA2B6F4EB2351590BE4F56A284F997045 0B30F36AFFDEBB815576D0A774107ACF03B841E5EC51EE0055FA 8722A89A554B8C36E06DE8D | | | | | | | | | |
| e | D8BFFCDD82504C05A241E26742F0A867B162E5ECBF185E66F0A5 FCA1801A2C3A2A562549D433C600E3A4085C123535AA7AD14D55 C0B3765C55C5B78B946517C14438AD876EC0F7AC22792988BB6C D7837AA64334EB5F7C668D570CBF8134B7F7E87EEFA95179CA11 BEDCDF420EB6DF9178C0A3B489A07B86EBCA6ADF96982D0D | | | | | | | | | |
| d | 7D71AF7541F1B1BA8A810DEF794F3662EE73B7E81EAD2B89313E 969FF5CD12B40CFED55EA2B5F1572EBF14532B17062A206371BE5 6C78799FD20CF61113CD677537090516953F0AA64AFDA84C60D8 A863D1639446BD3F21D24C60B406308F458640FE0BB8F3FE9CE0B F13060219B9C5DA80DF8594F32349831863DCEAF98293D | | | | | | | | | |
| c | 1BDAF2DBCEC34D6602C949E9B53876A4D8B62FA69DD960063B3 42E5101F92A0F5D88A445D7BDF36F3816AEBD5A98A8F06AB2CD 708E363A657665CF05CB1F289EB758E09D11351816DF1EDF4575F0 1F95EFCE164D62EEE92BCE562B94B451FD9B566E4F8625E0428A D93BC6F8342C089AF2842EA6DEB9ED22D450F062CC7B18A8 | | | | | | | | | |
| m | 9876543210ABCDEF000000000000000000000000000000000000 000 79207365637265 | | | | | | | | | |
| 通讯序号 | 0 | 明文分片 | M | y | | s | e | c | r | e |

[illegible]

[illegible]

| Frame 7 | | | | | | | | | |
|---------|--|------|---|---|---|---|---|---|---|
| N | DD1B58FF0DE86CD28DFFB60CC1EE0EFA3250D58264B3DA9CEA A5B5C17C728741F728C462C347DCB707BA7EE8672295F5A750C19 D48AE23A32FC21E76F3188B85008E4EC1A66371BBB0825E558E87 6D80FA59E7099AF25B0B298131277E634772F24EE0ED1BACD3BA 6F8D8E443D5AE16FAF6AA7DBAA59F91F763E4EAFD7D7F5CD | | | | | | | | |
| p^* | ECE0BB5F2672D0895354CEC3CC06E48DDD082467E6DA24D17DF CA04B8AEE15556A30666F0C427A1915A4DAD3FED6571D3458A1 7736AAF061BA4C9E5BC7BEC9E5 | | | | | | | | |
| q^* | EEF4B1E3A0A60CAD12A89987E57A2EF1ED9CC76B538E2175B3D 05F8F3EE2A839D944C5F33B76C73D11F89E971D4AC28151ECCD7 BF85E1E05CD20769F20B29DC9 | | | | | | | | |
| e | 3 | | | | | | | | |
| d | 936790AA09459DE1B3FFCEB32BF409FC218B39019877E713471923 D652F704D6A4C5D841D7853DCF5A7C549AEF6C63F91A35D668D B1EC26CCA8169A4A2105D02187B40FF3F870DAE31ADF95BE8AE E6AB75235224405C0DD7FA7820DDCDB70697C9E6785C8D4D0C4 2DAA00DE6162685361B6E25F05235F1CFF48B7BCDF4EF096B | | | | | | | | |
| c | B1E7F916884F9D17DFFCB8EF1A93D61E3DA73E066CE8B71F09B B8EF61C833300CB472854FF642F540DB232DED17095F4FDDCA6C CCC27628EA781F546863FA431B9057FA7DC1AA41C127FB22B113 E512B14926CA0C361DD6DAAEBC3F2E9CE51D012F40173CF88F0 7752CAAABA06AE53C4DBD559F50EED636A0A2E65D6BD835BD 0 | | | | | | | | |
| m | 9876543210ABCDEF000000002000000000000000000000000000 000 6D6F7573207361 | | | | | | | | |
| 通讯序号 | 2 | 明文分片 | a | m | o | u | s | s | a |

| Frame 8 | | | | | | | | | |
|---------|--|------|---|--|---|---|--|---|---|
| N | 9288E1EEF599EA72113D950723A8FC0ADD096C7312D8E78911FE6 4A4322C4FEC96FD70B345AA5A345481FB91D8549998A90E2429D CAF1EEEC863F396479A0BBD121E36B0EFAC8D002FC95B58B587 9DD75251B5CEFCBE90BF50669742821BE2E89B3831FD6F0F3EAB 310E5BF3FC66D702D5FF1581EE1DEFF161EFCA359063C6AB | | | | | | | | |
| p^* | A526772DEB284807B1FAC171CE1CDDEB680E5BF51C505E0F1B62 0AB949C42C735FF6D1BD0A78ED1709CAF501526C83FB2CDEF88 555A0151F1D32A04988140483 | | | | | | | | |
| q^* | E324DA534856229D59D818F7982AF3E1B7CC0DDBC13E85653100 DCFF17929B293974EA632F26392D8528DA07DBFAA371081C8FEB 320E5DF5F650300F85622CB9 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 753A4E58C47B21F4DA97AA6C1C873008B0D456C2757A52D40E65 1D5028237323ABFDF3C29E21E1C376CE62DB1376E146EDA4E9BB 16F27F256D1CC2DE9FAE6FC93B0F1DBFC9BE81E2832B9A590C3 309A1C1F9099818F2F108D002F2D4E70415D667D6C4B0F78CE0521 B4870BBD7FFBFABB402D7411EBF9716A523FB16CF24778D | | | | | | | | |
| c | 246F3344F2C341FDA293ECB4214C14D57164CB37FB364ED14B2F E3D10C94D2365155959B481085379A9C85B9FCB86C7E3676B2BFD 98DF7055D7E474CFEE6CE3529980A3FA0C537AF9C375E606E89B1 9D34FC801200DB462538E2E9FE80803A8EF02F662D0E5AC9C35D CE7A758B9EFD6D5FEA73BD9649C9B651E5AA5F1D96A773 | | | | | | | | |
| m | 9876543210ABCDEF000000001000000000000000000000000000 00074 20697320612066 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 9 | | | | | | | | | | |
|---------|--|------|---|---|--|---|---|---|---|--|
| N | 8B39E72D3C13D48F7773118B19F0D1A0CC592FD8FF12469E1D51 ABA8869A23297CD62E28BCF885F744BD4A7C53CB5369F941F401 EC010DA8665B7EB0B17B1839B3F0E49B51A266DDB84899EB302E 050E43A284B5051C5B9002BA2B8BF1DD3A22C0BAB03A6E780F2 18852EE086F05E9ADF290189439AFF15986077D36D271C9A1 | | | | | | | | | |
| p^* | B6E2C03911449DF333765F3DC9F8F697954ADA8189ECA57BF05E B6058520CE9F98B2B5C92F94D6032246DDCD3D485FA7611A7211 A23C4F8B692EF6959270C9AF | | | | | | | | | |
| q^* | C2E2DC39FD4419F3FF763B3D75F83297214A7681F5ECA17B3C5E1 205B1208A9FA4B2D1C91B945203EE46B9CDE9489BA7ED1A0E110 E3C4B8BB52E5295BE7085AF | | | | | | | | | |
| e | 10001 | | | | | | | | | |
| d | 4D82B10767F90A4FCD0A8CEBCA475E0D8D76E1C2874F1F6D8B9 91A5E3A81B9ADB148746E4DB676AED0E02985CA08DAA9971176 CD531CCB03C3E89041C2AD6B307282022C181F465F0CA3C93402 A57F2B98158F7FF756FF328F8000537D1F2D36BCB93E674D30F24 CB3FD733E68266146E36DF312D277B25849EA620B3DD8B799 | | | | | | | | | |
| c | 1478D729930A4BAC9A114ABCF11B6E5267818C936EDC70C87CC EEAE6114CEEFD83F0ECE19D1DD120470F7D7C22882A57A3DF23 D467DDDEAA86BBB2C1FEA07CE8F660440F7A269F2D5C9090C6 E8775A553063F8240CC3CED605AE71699AFFB5740C522EAC8C86 4B207AC691DEEFE08A66D216FEC93961131F786EF9F949F092C8 | | | | | | | | | |
| m | 9876543210ABCDEF0000000D0000000000000000000000000000 006C 6C2074616B6520 | | | | | | | | | |
| 通讯序号 | D | 明文分片 | l | l | | t | a | k | e | |

[illegible]

| Frame 11 | | | | | | | | | | |
|----------|---|------|---|---|---|---|--|---|---|--|
| N | 9FEDDC9C122AA836E9A04FE9358A118B358C7BC6F3ABDE4E035 E2BCB15B52950DB1D23449EA62F83406FB591ED39564FD0E2DA D0954156037BB32C9C23C49DA83E2E85BC09A9B6FD75E2F55129 044FA0F996895E8BF5E53D88938E4A3366649E97961BE5B7B40954 76D013D2E9F6FE75DC21295747BF371AE346355A5ADBD93F | | | | | | | | | |
| p^* | C9C4AC73DFF651BD8A786D1789CA7501D26C03FBACDE7885D5 A0951F9D32204908148483EEC6704D1DC87627759AAC910ABC4E0 B45AE591502F0302FB30239D9 | | | | | | | | | |
| q^* | CAEA4FA1888CAF9B5FFEDD254DC0DABFE252AEE962340423E5 E6C8ED79E8CFC73EBA6F3188DC21AB00CE25B5C3101DCF8022B 0799C84283350B6137DC938E4D7 | | | | | | | | | |
| e | 3 | | | | | | | | | |
| d | 6A9E9312B6C71ACF466ADFF0CE5C0BB223B2FD2F4D1D3EDEAC E9728763CE1B8B3CBE1783146ECA57804A790BF37B8EDFE0973C 8B0E2B8EACFD221DBD6D2DBE6F1BAA5BC46B6F23C3079D1CB 83650AA94D88FE450FDECFC06288B2CAD368324DB435DA1ACAD 560FA3D90264FF920DD780E362C1C8C43B323E1B5154BC8946B27 0B | | | | | | | | | |
| c | 9A597210DA69760A66B063FA125DC17DC2038EC720CAE6D0B159 9EC25B9A19F328BC55882EE9ED05FC9BD90276B0F7F1D227946F FD77081DF6E08976EBF57A3BB21AC13FE25A742A0C137E007BD8 787A42683D81ADC28450051B44617C2081D5ACA3141DC2C848F1 401CEA94DA7D11142BB2406306B299953D1C28259521EA11 | | | | | | | | | |
| m | 9876543210ABCDEF000000003000000000000000000000000000 0079 696E67206F6620 | | | | | | | | | |
| 通讯序号 | 3 | 明文分片 | y | i | n | g | | o | f | |

| Frame 12 | | | | | | | | | |
|----------|--|------|---|--|---|---|--|---|---|
| N | 808B8F96E7255B3F169EE854ABE0CD0AC7A4AE1B388CBC9A234 E225842208A435842C254A55855B867F3FCA78E3887C8D1663B501 A5D4D5E32F3EF84847F45651A5E2FC8A091E12E2B4DB7AB41113 D258E2200FFB2BBF8B7C38B0049B3E2E60C65EB8B6375F03A40D C9F9AB01FEC60E09DC8CA3644A83738BDA0CFDB2B5ABB3D | | | | | | | | |
| p^* | 85622CB9C3C41E7369F613BD2478FF17B3CA57010C6CB5FB76DE 7A85AFA0671F0732424982147683F8C6B24D37C888271F9A0E91C4 BC800B8FAEDB155CF0822F | | | | | | | | |
| q^* | F6B6C17DDF3842D74C8A20C1B32C75BBDB9E2045026062DFF7F2 840940D46E433586500D22883BE7685AC8519B7CAFCBA46E70D5 DFB0EDEF3DC20D9963245A53 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 336B063C5C7557B2D5D929BB77F38537830EAC0AE36B7EA40E1F 40F01A736A8156811A884223557CF661984305B0365053C27E200A8 BB88C14619301CE994EF4A5B54D6D323BCCC161EBCE11C3C4B6 8732B09D7D74C5F324EEB0CD7DE7C5A044107ACA052087CFEEF E32733A1EA943925719B785D9B11D4BF9ACC2DE914F25E5 | | | | | | | | |
| c | 3F312B5FDA3A9AA43DE2697FA001EE909DFE677AA6A48BEAF84 991FF7D423596B5CC230DB4E5BE42E7C886E1FA6B39002B148F67 0C3B162816EFCC6341A96D3CDCF849A35B866EFB9E5F5C48DF9 BBD3F065FFA3E0961EB2393C6F2689B72603B21A2E1C674EE2A1 A6534CA01F5606B062FB53CA9C3EB1BEC80AC6849B090A7EF | | | | | | | | |
| m | 9876543210ABCDEF000000001000000000000000000000000000 000 20697320612066 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 13 | | | | | | | | | | |
|----------|--|------|---|---|---|--|---|---|---|---|
| N | 866AA521700CC11B537E0AA52D40843F8DD23469B9B4C5A3C966 266DC9682947DA3A24B1505C932BD44EB3358290274F0BA295F9D 40449B314531725BDB1DF55D57D088A5D188994C77362BFE54777 D666B8C4D59C0C9C2B4D4E63780FD8D7C637444E0A9EC83A9ED 3FA856D5155F6FCB5861F0CB66994EE0CCB615B99D22E73 | | | | | | | | | |
| p^* | 219AA9485C033046D4DF82A94B50210FE3748D1A6E6D3168F2598 99B725A0A51F68E892C541724CAF513ACCD60A409D3C2E8A57E7 501126CC50DB43F7E2E2795F | | | | | | | | | |
| q | 400 000 7650C08E1F6D | | | | | | | | | |
| e | 10001 | | | | | | | | | |
| d | 411BED4AEA1CB3794A131692F5FD7751D59F8995E0C768A8B288 917AC2817AE57C1687E97FB4A7F12610CD0BD1678432ECBEDF88 B9232E93D8F77A91E47601684DE51E1F91E437806C7EBC31675B66 BAB717B222E0D3B11D77BABDB47D7FA5415959E3B770C38BD26 571FAB7044E9A4000E27A8F6A28D187F39B91344535F5A9 | | | | | | | | | |
| c | 3B54C09AC3380DD2CD82D1244D9B774A1E9D4B5809E79280E525 4D4A41B8F803A7151D6FEEA62B04B90854A96F1B5284F209FB8D C0BFDA39C885C1401F821872F17610CDF5BC8B7D236966B3A749 CDD0907716FCE3AF5E39678EFE9B344E2C05EDE973F4DA393B27 F505030E3AA56C6C1022FC0B9ED6454884E41784A3EFEF5C | | | | | | | | | |
| m | 9876543210ABCDEF0000000E0000000000000000000000000000 000 6F752065766572 | | | | | | | | | |
| 通讯序号 | E | 明文分片 | y | o | u | | e | v | e | r |

[illegible]

| Frame 15 | | | | | | | | | |
|----------|--|------|---|---|---|---|---|---|---|
| N | D2611805B6839FD983F2C574BDAD1C50A4FB9FAB35F3BB643F90 A9FBB0B84AF1D042E35E821564FCA783F1A2AF41349BB3E1C159 B20EA6A0DB9E70597CB5C0780EF6CD78481AEAC0DF65A8DE35 A8B5021FCE55332C5B2ADAEDCF80963BD6FFF773CAB55D73637 C9BD667148FB1359782D38C41CBB43FA5FD56F424F842D8683D | | | | | | | | |
| p^* | E79833B7BBEAECA1618C149B60FE4A25B6C08FBFF352EBE95B3 4092306E6D5ED02E824C76FBA4C31A1DCC6AB41CED2B56C1012 CFD1222D79D5846D33B1B6607D | | | | | | | | |
| q^* | E88C8F9BBFFEBD25ADC0BABF42528EE9C234E42345E6A8EDD9 E8AFC79EBA4F31E8DC01AB60CE05B52310FDCFE0229079FC8408 33B0B6F37D2938C4D7A68A72C1 | | | | | | | | |
| e | 3 | | | | | | | | |
| d | 8C40BAAE79AD153BAD4C83A3291E12E06DFD151CCEA27CED7F B5C6A7CB25874BE02C979456B8EDFDC502A1171F80CDBD22968 0E676B46F15E7BEF590FDCE804ED48C06C332CB80A68ABB3BAD 0C3A92A1C49096354CC10EAD25CC851D0ECE91E5B0045F47173C C72360FB8AB85F82CD8CF1FAC48576EF03599024A1F3470FB8AB | | | | | | | | |
| c | 4A6972B03F96CC30DE3F60DA66C71842E600320964A69EC818047 B219506A12F3E4D522B40B10EB3F630A068C908186F29BF782360E 35262A4CECCAD554F57D1721DB61B260AC6C5FBCB020AC32656 2048B0FC9270AFE51C63F5F27A9A3CFD78B5971D5CBF7FBF20E2 3CA7B429121BD0BB9AE0552D6907C659E2B450B01675D7 | | | | | | | | |
| m | 9876543210ABCDEF00000000400000000000000000000000000000 000 6C626572742045 | | | | | | | | |
| 通讯序号 | 4 | 明文分片 | A | l | b | e | r | t | E |

| Frame 16 | | | | | | | | | |
|----------|--|------|---|--|---|---|--|---|---|
| N | 811F75BEAD6F0C3EA1560CFA4BFD4762F1DA3A30E22644AB16B 1BEA5A6A1AF14F0C3C2E63865FD29241246C1473892232DAB6224 AF1600F73340CBCA7BF5AF01EA1FA007E46064CE2F8DD92A9E7 FA9F16CFEEE5A6CF67683BCD97F1E7E1BA73A9F86A8E4D74963 93AC9727D10530A76B03B3A23321E8BDD756FCE265494F6D35 | | | | | | | | |
| p^* | 859E8245BC6094DF41F206099AD4C0431F86F20D1C88ADE7F25A8 A51357C41CBCE6E52D519B09FEF07C20F993D242C533256C49D53 D88AF7222AB5E151CC9FDB | | | | | | | | |
| q^* | F762B6B985C4B873FBF63DBD0678391765CA21010E6C8FFB48DE E485D1A0E11FF9324C49C41490830AC65C4D99C84227519A589146 BCDA0BE1AEC515FEF07C2F | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 674C5E322458D6988111A3FB6FFDD2B58E482E8D81B836EF455AF EEAE8B48C10C09C9BEB605197541CDB6BCDD293A81C24891B50 8C119A5F5C33D63B965E2599F0E51F3A1B62792F27B7AAB664288 D458624AF7034CDC6E6CE19A69F926536A57984D49E61368F4E14 D89654F1D02D8D330204039F75E0A9DC1C52BE60750DBD | | | | | | | | |
| c | 224CD570EAF4D650AA24D51127E1657D201C8483AA690D48D58C A56AE86EA517DF43F9F130CC7CA75C8868623BA145189E2D1632 6A82A437516530D130161552D016ADB2D8746DC92D30F2A4D90A 50A63AF038B0449CF2A3442BA6696B6485A46D47545591AADB1C 68E901745D4F9231627C9E0C0A52CC7439CC45B21AE51AEE | | | | | | | | |
| m | 9876543210ABCDEF000000001000000000000000000000000000 000 20697320612066 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 17 | | | | | | | | | | |
|----------|--|------|---|---|---|---|---|---|---|---|
| N | 9E52BAE97E34F02361E694ED55E87BC77ABAFB3124DC8DABFC CE71B51F1049CF3C22BC79B8841433CCB6DF840F2BD5A6E75A1 CE52F54048FF4930E7B103C6A3433A2663BD9CBA0E38A35695F92 7EB2FF7A51939869A113D8A6CB03228C0E5D1466B1FF491129A98 8EFDBC636AB2610CAA50925554BE758321178F9EB94072C1D | | | | | | | | | |
| p^* | 2794AEBA5F8D3C08D879A53B557A1EF1DEAEBECC4937236AFF3 39C6D47C41273CF08AF1E6E21050CF32DB7DF694E2435E0A287B0 764B28EEDC67BF9162181C37F | | | | | | | | | |
| q | 400 000 2B21342F286E63 | | | | | | | | | |
| e | 10001 | | | | | | | | | |
| d | 6F02930C24F1F96ED5B657B6120670C3EDCA2D56C801DD543A6E 864BF8FBF2C4DBE57F41D99EC28B8F7EAA3A6E68CDE5B951F5F 0BCBEAC744388D91E70C3EBB1C59690DD8660476C0767B64925F CA55C02AFC3C9C4E4172DF2BA630E59060A3A891DD8C47F41C6 7475913D15E12203150C1811A66B490DE734F6F3569F65121 | | | | | | | | | |
| c | 1FCA302BE54FD4B4F8DA498EDE013BF551C714E321B17465CF55 B9980EC12FDF92F4F408C15239FE5EED408248D598510C0E77618E BA67321938D487D7286BD9EF539CB2B068FE02617BE2954109B3B 3DA0C76ECF00957894D556ACBCE10E1FF68A536B82EF0BEFA92 E9FD96264786FAB50A3162D2564D8634338E5A6EEF5E0 | | | | | | | | | |
| m | 9876543210ABCDEF0000000F0000000000000000000000000000 000 77686572652E22 | | | | | | | | | |
| 通讯序号 | F | 明文分片 | y | w | h | e | r | e | . | " |

| Frame 18 | | | | | | | | | |
|----------|--|------|---|--|---|--|---|---|---|
| N | 84FF95E263D30FAD83684CC08B11DAB54F5A0F3D24A8763C47B5 7750ED2E342022652836E2EBB30A765DC7364F417E4555D1FD72D 140EFB72E283007028CC2A4FE97E4FE3B5D272C917E734F8715A0 C5BFF2900640D8097425AFA965F9B1566F339F155ACEB59EDE241 327813C920A6FB98A6BB9209379F1BBEBCC955949D8BB | | | | | | | | |
| p^* | 8ADEFE85E3A08B1F5B320649F614DA838CC6B64DEBC82C27F39 A5291B8BC640BA3AE5F1590F0A62FF1029FD9E86456936F9618DD 73181937F36A0E21250CD21B | | | | | | | | |
| q^* | F52C8FBBED9ECA4564601CDF29F2CE09C2D4C84387863A0DC48 835E7DA5A52515D7C49CB366E9AD5C1B027EFEFC2D7996524345 39A560C9DFBD812F70A2A7DE1 | | | | | | | | |
| e | 10001 | | | | | | | | |
| d | 41F02573746273E766BB133272C08B5A50D929ACFABBBAC2F01A 7BE9576E0CD1D1BBAD5068F8CA6F6977DD08840AC87BBFACB8 A7702F6DA9B7EC9CC31CF4849B626659AA5842287B950C404089 DF572D442526B66E20CB1A6C5E07F0AC7E04D680C54FF2C02885 A685AF6E45123818B3E1957D4DA190643ED41D5AB457639101 | | | | | | | | |
| c | 45D8BD62BBF9966C81722D6D4AD5E6E91FD5258C8B0747CA1662 37D167D5C881B100D83D73352F18A60914963CA8F7DF9B9211273 C8D7EDAC87132AADAC33DEF0BDA6C9EA91750818D869990521 C6BA0A10BC1AC2273282FA4AC47EFBEEE99B2D35EBDA2019D1 EF8BF24B5017FA8481B372362AAE138043A00D8761BCDCA80BC | | | | | | | | |
| m | 9876543210ABCDEF00000000A00000000000000000000000000000 006D 204120746F2042 | | | | | | | | |
| 通讯序号 | A | 明文分片 | m | | A | | t | o | B |

| Frame 19 | | | | | | | | | |
|----------|--|------|---|---|---|---|---|---|---|
| N | 8614C70089AADE50E5A14DE1FB8FCF0880046E9494EEAD3BF600 EBE451E335B4C9E21DE984912BCA15914711A9C359056A2AD054 3035E971A2FAA387EA53AAD48A7016735E2BB60716626CAD6CF4 F9CC41A59CF31EF07473A1DE08A018CAB7C6B95BF7AC9F501BD 42FCC4C7CD834B6A7723B6ABCC9A98146A750A9222CCE2CC7 | | | | | | | | |
| p^* | 87CA9B01006C99FB8ADEFE85E3A08B1F5B320649F614DA838CC6 B64DEBC82C27F39A5291B8BC640BA3AE5F1590F0A62FF1029FD9 E86456936F9618DD73181937F36A0E21250CD21B907E03A53240A5 3F9AD2BD690EB4F6A3A6663F6D6E686A47873ACDB1455CE42B5 14EEC35C790884F58A25EF96904BAB3313629 | | | | | | | | |
| q | FCC696496F | | | | | | | | |
| e | 10001 | | | | | | | | |
| d | 444AA8E158F808BE0868F8D5974CEC85E864750CD459FDD364815 0EDA9AED471C1E9C1D9E5264C45375E3FA41679C28D5D61D24F E9CB2E5583B84B7F71E651B9156EF68E2C115880C148355E9BA23 67A0355AE99EB3ACE56E5B093C827E60BB081B7C9D3DCAA7012 C2B72FA9EFC513BC8619EBF5F6A6E221D6ADB8CA4BCD06C1 | | | | | | | | |
| c | 4B6A6A6CE0CD9D8E0DF4FBD2A23AF3FB45FA587406A3E052231 519C4B6B0B606D64DC531A29C0A7510928D4487E7BC3D45CDBA DB595AE7D53FBDEE70371DEBCB9A938B94DC0F266326A9DF619 1E04F82A9CDC067D366926B58A9092F55DB22F8D4BCD9777A99F 14ED95083D091DA69F80F448EFF48A21F998BBDC97DAEA135C1 | | | | | | | | |
| m | 9876543210ABCDEF00000000500000000000000000000000000000 00069 6E737465696E2E | | | | | | | | |
| 通讯序号 | 5 | 明文分片 | i | n | s | t | e | i | n |

[illegible]

附录 4 RSA 加解密参数表（10 进制）

| Frame 0 | | | | | | | | | | |
|---------|--|------|---|---|--|---|---|---|---|---|
| N | 900587051865585699352619484961329143800773125702819800200337600443 8251093307045093124134867865210377276811442056711984814236086711106 575330140208867670166821203517575485095189710333807997895981067329 7215370534716084813732883918187890434411552463739669878295417744080 700424913250020348487161014643951785502867 | | | | | | | | | |
| p^* | 6812427463539231600349464320632373878259506266011361351387035583576 1320419892511765086368785690374083772984025305208564111371556348302 56279629494046731167 | | | | | | | | | |
| q^* | 132197672075866407955715263775417328904651575170284233858122563051 6985743152190617208920569818877914453454888159181531140860040349288 9107894773842719465101 | | | | | | | | | |
| e | 467864653626863349172659968437798432336069925854249764817450553354 686786979487749884503056121279679265339232682604125570001251535696 223403532460960406042848835055873378293229496336376091807974477545 1399203901890478653711508788800552854790064033927005262891544078735 7271345416818313808448127098885767015748889 | | | | | | | | | |
| d | 640647027851500239246022590556679136772188365373833426853395393361 014449083596355793777413683517814178574454861732756713465060021978 278164449754077676168029871354522070503447020482337025636250575703 693998229521240027223068355883663582322432988617351394774261660926 12182422007673854917722168010527798129410809 | | | | | | | | | |
| c | 4864117372047570227869031765267692479634099669756708770511934446199 193077338615319822337257932846263580365356151667438020927666632837 5805315553713680858906705068657158073776194628700821011001144559278 7847959780977101451922363476297511165344002072887367765452474098956 72030976932673010818369814246455196991083 | | | | | | | | | |
| m | 798509450050819761921609517894014426345653719151394358624603896803 2293358555096757707390195545717847658989113846815132728257700850422 867276861362837615205 | | | | | | | | | |
| 通讯序号 | 0 | 明文分片 | M | y | | s | e | c | r | e |

①本附录中带*的 p 和 q 是由随机数发生器生成的。

| Frame 1 | | | | | | | | | | |
|---------|--|------|---|--|---|---|---|---|---|---|
| N | 9292179080070582697749775583293859289106228790333284489604 6168726101016067456726822505517352409138948392871113192427 2105292971919086388883881363912406831579946542073384636780 6544089987043488709421677231235873114231777425994219980853 5233769089985063860828267808621928898445383706310204223006 136919334252875849 | | | | | | | | | |
| p^* | 7273268163465293471933643674908027120929096536045429682300 3471302263984423914189568624761737988340573922478722744413 20512158525416407044516675402521694747 | | | | | | | | | |
| q^* | 1277579606750453488930879383770509385644718627643460718129 1462366302734214583227473619414509043813033676998357747882 057607288385639737162184366176530607467 | | | | | | | | | |
| e | 65537 | | | | | | | | | |
| d | 3370235084506122506759726042005203706334666804190337859802 8860500471812135487532181377788843962421728234410277562048 8394995406297460723923430428921035604038782164844024362036 8467873895824269701077696911995194762768484614281005894626 7556557924949475841898976300838543407378257647526095943254 38440597282630629 | | | | | | | | | |
| c | 1626661141529320283833484152716550848856697186049377493478 3687998320433794207275092233186943476259776945007614600486 7010182076965661241973405787156202346315969852234851015712 5720014700549254630959391701883372400982386084212421115166 7917287048672537343548749342109873011375123410701907602272 27749365878233484 | | | | | | | | | |
| m | 7985094500508197619216095180801677871569877246162537093666 3222161890809457825126712129612030384445557804418636905479 49326495942981239718080535505859471726 | | | | | | | | | |
| 通讯序号 | 11 | 明文分片 | . | | I | m | a | g | i | n |

| Frame 2 | | | | | | | | | |
|---------|--|------|--|---|---|---|---|--|-----|
| N | 9025265360096445352455966929661813527291128977594919492254 3520872164147768650421038176330053599968601135821750672685 6643607865954300286844194118933160742863127937308229635642 2056461670857376476438683012381819718323344347250610682891 9670406785228124876225200632055727680225997407097843708009 916059133498338129 | | | | | | | | |
| p^* | 5248406512257276755729353447736168645667928088030412529110 6733197354892893647364164212186415880889674435558369420400 890814461263958618375991691022752189839 | | | | | | | | |
| q | 1719620105458406433483340568317543019584575635895742560438 7711050583216552385626130839796514795557880099945578220245 65226932906295208262756822275663694111 | | | | | | | | |
| e | 65537 | | | | | | | | |
| d | 8258895191658208655835470783003162806639052551143972287249 6147729457074171559623579070004210972386849372377466642389 8662289255489437978586447498369768467254840388655176343790 3115722345807460930396270788481544972436779296592510052271 4951639990422347138894120078817973323451848604716319336643 295543873255793553 | | | | | | | | |
| c | 3963226350487047857486169505125185080745429478797470921486 6410237055871793939895562441267574482198916367858789237648 4349838153691234792087263447165942277853088366019321817276 1085989895119020634505642625325107992982242425227195726963 0987623886812686545521745791771387808772030614435314730783 528512800343192265 | | | | | | | | |
| m | 7985094500508197619216095179955526231518359039504085499384 3752852087229515882327105286107450872051429979633410343057 59963660378376322965694370023122954611 | | | | | | | | |
| 通讯序号 | 6 | 明文分片 | | T | h | a | t | | i s |

| Frame 3 | | | | | | | | | |
|---------|--|------|---|--|---|---|--|---|---|
| N | 9227062778302034190376987727263516375761173725230232940187 6135487358785338853904185572496782685853218459404423868889 3608086461928580603321108309624639861640143315403360377186 8460622389350632712611273940802301490000360002865492948848 7584130630596342720833061628867179840913592694993869009133 576053124769728363 | | | | | | | | |
| p^* | 7055398260479522499340383681532186847092995337600547504968 0110293347858492481988272615921087380309003501468009697150 64939422943632175860165796992047655507 | | | | | | | | |
| q^* | 1307801833099484562155274785542999674112962876886767678871 0615773048246855802311926334525991481279783903078961691672 741494174797757666145632542141818518409 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 5536237666981220514226192636358109825456704235138139764112 5681292415271203312342511343498069611511931075642654321333 6164851877157148361992664985774783916863285489693170017586 7488481215879364334209317976387923273282607858737333466278 6098320707497674046089285041862711071864295458351487500276 666628394542132669 | | | | | | | | |
| c | 8342143428660254649336420413918294989779512316049868067096 4040331447569764445309937195566103281638928183742488663157 1385720208179245619909797234447970453751018013548624727615 0742189645490481887443923199056773817305981564753973780052 3632262742398190575822391771655932895657208471832891505814 792263361394479317 | | | | | | | | |
| m | 7985094500508197619216095179109374591466840832845633905102 4283542283649573939527498442602871359657302154848183780635 70600824813771406220340542500306493542 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 4 | | | | | | | | | | |
|---------|---|------|---|---|--|---|---|---|---|---|
| N | 9005870518655856993526194849613291438007731257028198002003 3760044382510933070450931241348678652103772768114420567119 8481423608671110657533014020886767016682120351757548509518 9710333807997895981067329721537053471608481373288391818789 0434411552463739669878295417744080700424913250020348487161 014643951785502867 | | | | | | | | | |
| p^* | 6812427463539231600349464320632373878259506266011361351387 0355835761320419892511765086368785690374083772984025305208 56411137155634830256279629494046731167 | | | | | | | | | |
| q^* | 1321976720758664079557152637754173289046515751702842338581 2256305169857431521906172089205698188779144534548881591815 311408600403492889107894773842719465101 | | | | | | | | | |
| e | 1522069925757068934848359844725445295093254409441316626317 4140341403795669566553318665007147614638973702055421595618 1827422540843366433981607643940546405002217220286072880967 3311183448063157563046502486345465977845979638866564227061 9775726531698188911802697886529559713547073557603228269434 8773714479076093197 | | | | | | | | | |
| d | 8808983115855943267394917370227855385662768621048537726144 7653737689967883346026994105419051551162437756710912061574 1061454295081091244820829682602826025919935409136316634613 4712349091366249935240952309188837913591552469429394370618 5914919458120628631732165371691607982212461058847727942387 916343380712892733 | | | | | | | | | |
| c | 1956063455630575555092754061098953776671590224407231281835 0844104485773927537226443429404190213856361759564153804627 4508058805126003398691695133489291946438098594685497189229 6599764768920302951713539600863105029254402265194800939247 5583045438153697076529266662217519588521116539517972522591 294232192817502376 | | | | | | | | | |
| m | 7985094500508197619216095178940144263456537191513943586246 0389680322933585550967577073901955457178476589891138468151 32728257700850422867276861362837615205 | | | | | | | | | |
| 通讯序号 | 0 | 明文分片 | M | y | | s | e | c | r | e |

| Frame 5 | | | | | | | | | |
|---------|--|------|---|---|---|---|---|---|---|
| N | 9919371154725706316081685054421492434057435875267064461529 3764532335872088470223740970673347993652626497557387222167 7841828763954360888452818401697016546298492142222977845113 4905969896321294729914232049775925888942518270504212321747 6724761095690092179821753840224757786599021225709340258545 979566824267620959 | | | | | | | | |
| p^* | 8534204848837515931975393694743604482233978795239717717444 2496455007444984812121861705603969807398793017952764599150 05215431744867752453542213016868639743 | | | | | | | | |
| q^* | 1162307599878724540234655975033145507916506011733793003488 9727146620333293916811257160778523014841986594526205881807 563317848049715664071879977965137310113 | | | | | | | | |
| e | 65537 | | | | | | | | |
| d | 3664765457213078521007764167153021900694763184885506382761 0478365220386512628431686530096186504879854820717411795021 8740317681029448100952257380720659499681778351587798939558 6244905511991482571370681929245555805464198668247750647926 2436535982737603932531320904242033052449306569333872582142 053431516070034369 | | | | | | | | |
| c | 2605467779358177292486627373700967328577506280273478653240 4396138990264566536537921648515854012553861999940229349708 9895191565638309165537547622084667453212268353129749717397 6176932456931552587209698736700154375838007185942961958018 2411498650200401467760546057912183435480924905200466941116 258838789328064564 | | | | | | | | |
| m | 7985094500508197619216095180970908199580180887494227412522 7116023851525446213686633498312946286924383369375682217963 87199063055902223072057557872738858857 | | | | | | | | |
| 通讯序号 | 12 | 明文分片 | a | t | i | o | n | w | i |

| Frame 6 | | | | | | | | | |
|---------|---|------|--|---|---|---|---|---|---|
| N | 1468396439700164648131974095690042755958287918257226170666 0799300168290102378426755481594618937465153028889432228685 9792246413142980277245909181062525398546369553995023529451 3968205493086904939285933240076891356487533231613947351209 0896045886080174347635322897008136943951319710503914393000 8573928693059198131 | | | | | | | | |
| p^* | 1594826922590108161395231954947243507956540075898893987573 8355402718392411641342753318422091403710654325353510345232 4841452565420868944985464229649420240708554088156331324206 7337276907853734645755256982745520583865601061630939650658 3007127746594383430808370806542949509274602868196867003672 1164931 | | | | | | | | |
| q | 920724637201 | | | | | | | | |
| e | 65537 | | | | | | | | |
| d | 7072330686342883623979462832650527045053244487611684375174 1862462827776049146014385813063637754641128224016479468802 8366681044024681020040528796250995319698379697263370645183 7414044570766536958201333535092209130852590765317992957169 9242807523052334299065827781416356624702821072187589449553 295008322392493473 | | | | | | | | |
| c | 4719077580747250617358799308202375990960135722980866704404 4468676457696140445235738005020994278091230440755033222450 2193780478076468177223769183642117279718043123272042945551 7899648094418862497263237167482239725812722702999019695690 0925820980263353418653201918881814896866168764140848945600 419602253279143149 | | | | | | | | |
| m | 7985094500508197619216095180124756559528662680835775818240 7646714047945504270887026654808366774530255544590455655541 97836227491297306315958671527603954464 | | | | | | | | |
| 通讯序号 | 7 | 明文分片 | | " | L | o | g | i | c |

| Frame 7 | | | | | | | | | |
|---------|---|------|---|---|---|---|---|---|---|
| N | 1552664939360431038498551999878968137168319864167070806450 3602290915337311036700714030163514495063487998328972016411 7794783088845393686109145443728632527874768524615377182297 1257162761538007659060142067975482306617642749975626709001 1538332460584393303531411075256029054084815223731675257347 1110899212429555149 | | | | | | | | |
| p^* | 1240630014530794433520921337301819672571520166653538561879 4522686524721950743049201561939737652055430279463659191670 498628785792792237461236532551241091557 | | | | | | | | |
| q^* | 1251513280490515970812776613632570799232137711399871047744 5811836263405233128780498152047439057240132542217905573440 500557504942936575400253824837109325257 | | | | | | | | |
| e | 3 | | | | | | | | |
| d | 1035109959573620692332367999919312091445546576111380537633 5734860610224874024467142686775676330042325332219314677607 8529855392563595790739430295819088351899898061110109385502 5258245112065973652462902841756347562809531681396236580188 5712240707911148249316752604733035028656597729772068250707 3080361216052758891 | | | | | | | | |
| c | 1249299432320818281058083189932575263645965800215640213775 0391567054444567983658876536950391931140432804320327269385 1622132258819278328852726005776082575583793735570095307898 8282545680158866300102696155468573357907915778655650217308 9036423944365147958096811203152148517406873157734869081090 6553798608040451024 | | | | | | | | |
| m | 7985094500508197619216095179278604919477144474177324223958 8177404244365562328087419811303787262136127719805229093120 08473391926692389569271534373566444385 | | | | | | | | |
| 通讯序号 | 2 | 明文分片 | a | m | o | u | s | s | a |

| Frame 8 | | | | | | | | | |
|---------|---|------|---|--|---|---|--|---|---|
| N | 1029001639304977910644025774479497411954645557465992335523 3845590533936352443564708263732603351808328952325067046390 7211548409422234391456982344516192210687545692054217151133 1519152161232750054642295348916295688643611546581070932283 5282909825146890480080958506108848448554201957584877464326 0318502441084765867 | | | | | | | | |
| p^* | 8649620751833675845720949489383858845796447401365353800898 8781448451754061726768449992751502196306063596846692423203 99096050331623719946048021382644892803 | | | | | | | | |
| q^* | 1189649429527687405559328186931933415165178313380867339657 5485807068776793606182148494465816391713137317129560972663 854384901692609500496853548961122888889 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 8232013114439823285152206195835979295637164459727938684187 0764724271490819548517666109860826814466631618600536371125 7692387275377875131655858756129537685335996616056852809854 7014708593606560641279919977408189711199776219532391475959 5068483608401834765652726597486615601030830899059633138253 933545677853587341 | | | | | | | | |
| c | 2558508895009529071232821570130927352140623598288578164113 7768116285362079062975527364909549362511146004390419156826 7095433268145814662482805641949517069378220889026077549444 0540769873582431590094291532205461443763211673227178782381 4807624841386886185122143173564380877370643120953803688563 589496390425159539 | | | | | | | | |
| m | 7985094500508197619216095179109374591466840832845633905102 4283542283649573939527498442602871359657302154848183780635 70600824813771406220340542500306493542 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 9 | | | | | | | | | |
|---------|--|------|---|---|--|---|---|---|---|
| N | 9776795104615437232140044337123449547646182813725193902505 1233003462769415459435471728054384852461870179980010660162 9225474252128699256484247415266715855981675028561116419448 2517929519709882691122648315582119725198929710218918713923 4080795582529077092266799813985026581245196104843272305656 744384140745492897 | | | | | | | | |
| p^* | 9578503710865082752572619447703250581238252879412822133271 4322045327876716430278936702563319283584587344935597471718 10834463456086852684437858903431104943 | | | | | | | | |
| q^* | 1020701708715258804071504840268078539886222262991063717247 5793288776252558629748676497021478354292685455714591071372 731030921157909006333951719151324136879 | | | | | | | | |
| e | 65537 | | | | | | | | |
| d | 5442973376672701570896770643823888493452837727414703522083 7378692407992506407875896386312957348168573407186027266226 7786451219359563621650125138371017817631695835538950002507 7433575805193113857419564568484300430966953240454755085264 1541919592382469963208562095891891823354101113238100316341 105229944206178201 | | | | | | | | |
| c | 1437595054387388201179675934884847928352295579674985311349 2047625299699702886303193822347995567175524401038661237990 8471852361389678140880307677859166454921427413977862564453 0536682227755151435342386424067452226440791860566200855054 5442780563568811883349771003546081844527788515420708612431 091464410712019656 | | | | | | | | |
| m | 7985094500508197619216095181140138527590484528825917731379 1009885812241434602246554867013862189403208934332727530448 25071630168823206423126265343981085984 | | | | | | | | |
| 通讯序号 | 13 | 明文分片 | l | l | | t | a | k | e |

| Frame 10 | | | | | | | | | | |
|----------|--|------|---|---|---|---|--|---|---|---|
| N | 9383651435834417376289508438495363315969975098795404441483 0106276642828025218933012478990865656107605541657809389659 0631086202080047406460996627001127822522008343933635740898 1878771795102669093498696427552653823675059634454245086428 4576226592039259070002692883820960186403938410354082341916 474419847211138467 | | | | | | | | | |
| p^* | 9686924917554805418937638872796017160525664579857640590160 3203008051154435781849859343385833031801785820095916343217 55204008394655858254980766008932978633 | | | | | | | | | |
| q | 9686924917554805418937638872796017160525664579857640590160 3203008051154435781849859343385833031801785820095916343217 55204008394655858254980766008932978699 | | | | | | | | | |
| e | 65537 | | | | | | | | | |
| d | 3944206266733764064034775606988903569968489617262264158407 1973657669407870526663528918912391110804525838168480022841 1158803906323131451024323269054123138405432800345792746952 2999022244797843680951403851596928261157944405368083136948 4773582060225475139121494478449951766667502048484500914263 289600089033243889 | | | | | | | | | |
| c | 7885278540812733821037570530236161158003329804735856671238 5067002412358292419274287993295604646693755514055710305938 8058471840121734491606248232610131520921512426615387720128 8071498149227573165852746544278726655494782830157158672138 7286510359738598116104180351027973922256460236377354127082 438812404967605644 | | | | | | | | | |
| m | 7985094500508197619216095180293986887538966322167466137097 1540576008661492659446948023509282677009081109547500968026 35708794604218289672526108082271905140 | | | | | | | | | |
| 通讯序号 | 8 | 明文分片 | w | i | l | l | | g | e | t |

| Frame 11 | | | | | | | | | |
|----------|---|------|---|---|---|---|--|---|---|
| N | 1123060666016528190622064357247955956030859080110016711843 3222748897005712812882183126064905856973956910329809172718 8365019228385820143813415009397359257831092635374404034997 0114416532866424584318650262131294126770643083425807572485 7795507138497271455725046868659990168272817309674571084931 8629959223270431039 | | | | | | | | |
| p^* | 1056746104850503964197271026871312894463468774825071208047 4984695584136876402672898538333956369978635390580930966654 058991315304961329166742263216335895001 | | | | | | | | |
| q^* | 1062753542087014015726494338123799584518861375728348831198 6534170673076876359166440468642831586000127005789867628311 873382408383407839525066568105400526039 | | | | | | | | |
| e | 3 | | | | | | | | |
| d | 7487071106776854604147095714986373040205727200733444745622 1484992646704752085881220840432705713159712735532061151458 9100128189238800958756100062649061718732650926033525701318 4919200222367844573904234711928601347703029472357800299115 9077376272123172385658714877200871144530532915371561120417 880751934356006667 | | | | | | | | |
| c | 1083878323903377709473615183765527025037410922847788244489 4397179204492272046195503572686310941865721849865946066350 4872870862538725835055240750735576735249122665348803252691 2218691466790040179163590674546937014953897841596203418603 9403537359982380128844260427304672987346793600422701318665 9110262247417571857 | | | | | | | | |
| m | 7985094500508197619216095179447835247487448115509014542815 2071266205081550716647341180004703164614953284762274405604 46345959039613372921278195549267256864 | | | | | | | | |
| 通讯序号 | 3 | 明文分片 | y | i | n | g | | o | f |

| Frame 12 | | | | | | | | | |
|----------|--|------|---|--|---|---|--|---|---|
| N | 9026748093936816074945804920736708318040726602753121267487 9245323647502822038591438536367206422215464489854541063867 9462152431903454768745460911884081205519025731135078767545 7829067479264301884579826315684902720944097974648541465416 0320058352559498237296080490768064578067282805498131582552 189186085941328701 | | | | | | | | |
| p^* | 6985860474362742689823213380101231514167124463232248283942 1517806078459428414600916931386939543965019184805079645693 22391710334462720533595017918609916463 | | | | | | | | |
| q^* | 1292145488313699141434064112918417839373104536522240607476 1149065515779165690863384311170163255060973667442222325395 407973824379536104548265452893540473427 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 3610699237574726429978321968294683327216290641101248506995 1698129459001128815436575414546882568886185795941816425547 1784860972761381907498184364753632482127981031024032570601 6577446620289324437905137388087786740245605344914412244873 4737621617480915511928197827215109845334766908313653102988 131486109516375525 | | | | | | | | |
| c | 4437497929112057550398874153198745489891925488008646425490 4878064332010355432423956182135846738023874326776872139229 3799433213213628225229004794382942912062872056471457599722 3309727625340881269955730531434422080735602499497739984084 3758750494467535572805794732065369887057841293267499209427 585419962565568495 | | | | | | | | |
| m | 7985094500508197619216095179109374591466840832845633905102 4283542283649573939527498442602871359657302154848183780635 70600824813771406220340542500306493542 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 13 | | | | | | | | | |
|----------|--|------|---|---|---|--|---|---|-----|
| N | 9439053399235889555070422518048460401602978160462260783304 4135524814562613596803297695605669157378162035217814540004 2310752014207967875477337622659593200181074190588328190106 8134413301177747972238252579793855818162983576847146143456 0813554411133962651212455645589624432040989600687436833459 731886703583047283 | | | | | | | | |
| p^* | 2815987057259792059456389325049957273923776966064723883901 1417383170724985058502301163390234256825164330439886062865 686161169349465086627567328776299903327 | | | | | | | | |
| q | 3351951982485649274893506249551461531869841455148098344430 8903609304410075183867442004685745417258569225079645466215 12713438470702986642490397676148760429 | | | | | | | | |
| e | 65537 | | | | | | | | |
| d | 4572115753829795595247120906288789164119299658267459123334 8888143113634895839457416197674626049422002133268070289644 5414877438561910679570747559871962191277366557976642188990 6700218767015263374087795307280743154400994552662789125054 2293379451051502729154061517001465270366555387774409063463 710670570399331753 | | | | | | | | |
| c | 4166368995265718598451373355838803328929285775874846807093 4326941659317694408873831451567385012905508903797893149006 0672807882984089590174598905798597840726774108906578549426 3904005692459692559997376221490072864865705247497440587886 8755028761443878403349272421153452240103741921751653022646 614028009138548572 | | | | | | | | |
| m | 7985094500508197619216095181309368855600788170157608050235 4903747772957422990806476235714778091882034499289772842932 62944197281744189774342357568909108594 | | | | | | | | |
| 通讯序号 | 14 | 明文分片 | y | o | u | | e | v | e r |

| Frame 14 | | | | | | | | | | |
|----------|---|------|--|---|---|---|--|---|---|---|
| N | 1200088765368551312212559793707452337385919341882245284875 3512048345621408549323748291544641959935791034345028585899 5374277365393767669569942204888383426461862651659865189178 7844731319142341817520559504310933415141383908988924131825 3882369394112463730158238901447975462741956056800483109311 6617428970538503551 | | | | | | | | | |
| p^* | 1095485629923346512635991417150030582284616543108518367399 9109759449706415739193445885099004577509868426540084786683 485568001351280541116090063034118634519 | | | | | | | | | |
| q | 1095485629923346512635991417150030582284616543108518367399 9109759449706417636519711881707731622506407722143163847672 064459333431572992021257881551867597529 | | | | | | | | | |
| e | 65537 | | | | | | | | | |
| d | 3304515290574923627902994344758637850445748270993026597320 6872213321495329154690687957827579658666293087231699019049 2473596492957555482408284942767561425383430846438194146906 2914963853602136633861481213288770128306562650262612718302 6015339748038111894817224056905210742422716888577808063344 155166016198945505 | | | | | | | | | |
| c | 3513376526014685559919476150099315959231113637803385881872 8078464540389548474611501950689942825550399101504201020687 9612566424557458884104105249559377739515789938822755259441 4513179497000170865571884450777487760212518387778239356409 2461821246419013099835940432551540513624090850765797735157 630551978900512155 | | | | | | | | | |
| m | 7985094500508197619216095180463217215549269963499156455953 5434437969377481048006869392210198579487906674504546280510 73581361717139273016540010317514961519 | | | | | | | | | |
| 通讯序号 | 9 | 明文分片 | | y | o | u | | f | r | o |

| Frame 15 | | | | | | | | | | |
|----------|---|------|---|---|---|---|---|---|--|---|
| N | 1477333493876965210156649923963551458112497931039584640532 2538947605009750392802281926948255595536553413715607917270 4297584033078453033637103720972881068435459202133846880715 8798943401316566916317561623234228688466161604237558837264 5048684517522768232958361573979778202564737604224960577543 3971714513081755709 | | | | | | | | | |
| p^* | 1212959022867974150412171184397036249304931573458929924302 2334854180628199056110072388206407916677887428330057500003 256795368137540193144088105889375346813 | | | | | | | | | |
| q^* | 1217958287151277646895689174587744501035061806367681377096 1929030122878089063984750168929497808121238411849832804023 412100455762402728468432020965274841793 | | | | | | | | | |
| e | 3 | | | | | | | | | |
| d | 9848889959179768067710999493090343054083319540263897603548 3592984033398335952015212846321703970243689424770719448469 5317226887189686890914024806485873789407666860224362418285 3419383352256612548788157603820656990823485074683306373757 0442858692881305020305183706604985332652320145566441902547 634391772287711403 | | | | | | | | | |
| c | 5225381759005611636827329451976127435084719347709028091637 3828903718796358618956145225746496960677477661151583828604 0210499369637791034405606304511251373446395037058800246773 4506311324053079835272743276898075199292629380120677983915 7443722614687126711272753610923903360818026083573711899014 859313677159790039 | | | | | | | | | |
| m | 7985094500508197619216095179617065575497751756840704861671 5965128165797539105207262548705619067093778849719319718088 84218526152534356267522207486445887557 | | | | | | | | | |
| 通讯序号 | 4 | 明文分片 | A | l | b | e | r | t | | E |

| Frame 16 | | | | | | | | | |
|----------|--|------|---|--|---|---|--|---|---|
| N | 9067317719301733260278181318787944272556290947341199405251 1479411887936365983777106776080722300002656952655125041151 1566843407439073491087297741576163238630625255933822791433 9583726105397665213876427945652849391496178030026959172210 1449703932139132398288208673556967030162666354552157189525 415838326249712949 | | | | | | | | |
| p^* | 6998204055345503454608535735199373144581147952412423572966 4941831793060052162789355105536344877949453792090067736288 64213102839984362642462197184843259867 | | | | | | | | |
| q^* | 1295663522754207120237556092714452033350735861983158067037 7595997503810379893056493870213428580918250332435506596912 071784762831942734238145246920736537647 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 7253854175441386608222545055030355418045032757872959524200 9183529510349092787021685420864577840002125562124100032920 9253474725951258792869838193260930590744861490483957635891 2939247896806653924020616577001940045669727969372256529021 2816258532060850948073997623234877191381334791104184074115 846715376535932349 | | | | | | | | |
| c | 2408637170160294812231779021100403201432648727990748672499 1846810668564197542368948703436295770758262739732290677177 5272970405566664345777303547323977846512209184124074851711 8073232773024255295564675027984225120022793725732241466221 3662054605527282812231172173474061845763736546747711105935 349033514358348526 | | | | | | | | |
| m | 7985094500508197619216095179109374591466840832845633905102 4283542283649573939527498442602871359657302154848183780635 70600824813771406220340542500306493542 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |

| Frame 17 | | | | | | | | | | | | |
|----------|---|--|------|--|---|---|---|---|---|---|---|---|
| N | 1111783070331507391046086474741997862515169136989363314301 2106058789356440548289681404541937040181630559214968529103 4839621072343496556225594365571727260237484885924615887468 0536445197790818717789968516012075719810722612323845771263 7771400555031899048661963673470126603256941342191552014337 7137845245405768733 | | | | | | | | | | | |
| p^* | 3316822783084922286009469115817426366342233689972333930241 4624335921937096795361698659264621281924482566876836548283 550012466892022559940789243695658550143 | | | | | | | | | | | |
| q | 3351951982485649274893506249551461531869841455148098344430 8903609304410075183867442004685745417258569225117538105187 51644117399610974624147782234049900131 | | | | | | | | | | | |
| e | 65537 | | | | | | | | | | | |
| d | 4872119532465766249728184621601565315994881916220534108477 7711217851033305239312090870568447105301803509567709256733 1521723178922627080092019802435266629990952646522726209677 8368922987278031873142541199748221996571727801079979094524 7915945311316925576971265571819052682504386474458062215314 80549202354131233 | | | | | | | | | | | |
| c | 1395222187334055833498435136007269572138525113145744882969 5310374422440862775948038652173017199470661531762446386608 6403594970566467063324511084741616879664019923873347854008 0417312141011028469385167826450855601412915611725028631975 6059322790239187717642040318064147340154760341068910493341 59757621016327648 | | | | | | | | | | | |
| m | 7985094500508197619216095181478599183611091811489298369091 8797609733673411379366397604415693994360860064246818155417 00816764394665173124623001351367241250 | | | | | | | | | | | |
| 通讯序号 | 15 | | 明文分片 | | y | w | h | e | r | e | . | " |

| Frame 18 | | | | | | | | | | |
|----------|--|------|---|--|---|--|---|---|--|---|
| N | 9339463910866721248218045861603674161505898105894273950902 5631675767304945732437421192075466824789572910657586684470 5536910492595041064420901409277826730668341268485563170799 9533222926287107979908977197310073188984101596071390811790 8583988637159206246729697336281050046919985463146705713899 703248595045701819 | | | | | | | | | |
| p^* | 7273268163465293471933643674908027120929096536045429682300 3471302263984423914189568624761737988340573922478722744413 20512158525416407044516675402521694747 | | | | | | | | | |
| q^* | 1284080787476011949756298986465156549164507794697695074821 1992253853323703532620362223764981952516328133916264333884 385029280730688894521589959051436522977 | | | | | | | | | |
| e | 65537 | | | | | | | | | |
| d | 4630328843124975308560061433010766145164558055094324567995 5762766208878531161608811654071990906984799472253632399283 1107699402252133516413078544795384990560145855154992101615 6253288716051885129120874572511411923581767586366761275620 1842550141918980980087810087817831155007090883382721036933 994860714897150209 | | | | | | | | | |
| c | 4904797845888580712719238528222772675459388874938877537749 2411121925201201621099927332087316607446894372751446254341 8080515691110532930662329804349015928753472001220222107805 3681752481307690875064713730161011759235581840828029176606 8780616226847056325075159440352473034526412778650516438709 293396458312728764 | | | | | | | | | |
| m | 7985094500508197619216095180632447543559573604830846774809 9328299930093469436566790760911114481966732239461591592995 11453928830060256372341748824036810818 | | | | | | | | | |
| 通讯序号 | 10 | 明文分片 | m | | A | | t | o | | B |

| Frame 19 | | | | | | | | | | |
|----------|--|------|---|---|---|---|---|---|---|---|
| N | 9415499359327410982841878683415972819079744571153924388740 9583756844882924221269576486611543668906670821879426307992 4047219256237414786777560839929027117658655034666879197993 9425830657470218466620718053059805798988472915427342303247 1322027993848437082723045300784582836897839491321003685598 931080456249945287 | | | | | | | | | |
| p^* | 8672576161185989538639614103149718994898444713854221542046 2553101081991008304507461163078354877970282649251051457532 9029550098560094058539173966300170113205003570816644830717 8213558489995356047886604103239733599072268921111393779740 6269980402604895207480485168493674422769645640726941944110 986793 | | | | | | | | | |
| q | 1085663496559 | | | | | | | | | |
| e | 65537 | | | | | | | | | |
| d | 4795602005188816821261295483797326432124124329234909837368 5816663148254451500554825568242197058371318744350650809862 4360211823072797033741932723456320667110957251305394580311 0295530507236326408492966166078060679086151084264272910658 1408151895223149333589518908985209522876017568214337736756 410182145898514113 | | | | | | | | | |
| c | 5295869599237118040941401167811598140583502680064827839308 5136639708219930134280877954018305615378579281651249142230 8482628224217138952270695611459459724488932292310206324925 1786903421794326066413064732269458318280080083853969154217 5229797652856708373533581250607375664993806654537737027000 328299623032632769 | | | | | | | | | |
| m | 7985094500508197619216095179786295903508055398172395180527 9858990126513527493767183917406534969572604414676365030573 22091093265455339620683498933545692718 | | | | | | | | | |
| 通讯序号 | 5 | 明文分片 | i | n | s | t | e | i | n | . |

| Frame 20 | | | | | | | | | |
|----------|--|------|---|--|---|---|--|---|---|
| N | 9091673975583808383746102637570033088500144622418751139551 8230504776419813625940046511904838818660297497622072999229 7060616982251916452685911986009552401163024613319131787127 2209659125761953892705088652151245369190294623498655691303 9431677697816965623861908091178749411071673467596883926097 177996147858865293 | | | | | | | | |
| p^* | 7006433107252813175095285828299335809650512229854304253471 0359557876174658258429900813205354104359733469403387722665 19696972554709877157476961995216696227 | | | | | | | | |
| q^* | 1297618037082581604633072369305156532409192035901658824746 7647785104809172783057319885443026117787490599861213721564 637212466483142611446237049740392927759 | | | | | | | | |
| e | 5 | | | | | | | | |
| d | 5455004385350285030247661582542019853100086773451250683731 0938302865851888175564027907142903291196178498573243799537 8236370189351149871611547191605731440577919087123007296947 7765224194403104311077097859037197165193152320553595098248 3473026560553262440238776773775753347948858417135418862496 078390647349544785 | | | | | | | | |
| c | 2320403909875403051395433221249665270517564434987968663944 9689791620605370809827884267260830136516742466455588549253 4810165047966740148710205035436396812518341141592509867288 4038077777414485392521688480252923021278375982126279984522 9436535491711201551797166082529740271577684082458494926929 260818927584104158 | | | | | | | | |
| m | 7985094500508197619216095179109374591466840832845633905102 4283542283649573939527498442602871359657302154848183780635 70600824813771406220340542500306493542 | | | | | | | | |
| 通讯序号 | 1 | 明文分片 | t | | i | s | | a | f |