第一章

1、 在文献/网络上调研最新统计数据：中国范围内最喜欢用的 10 个密钥；全球范围内最喜欢用的 10 个密钥。

第二章

1、 在爱伦·坡的小说《金甲虫》中，据说基德海盗船长（Captain Kidd）用看不见的墨水在羊皮纸上写下了如下单表代换密文，上面透露了财宝的埋藏地点：

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83
(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8¶8
*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806
*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

请将它破译。提示：

a） 英文中最常见的字母是 e，此外，e 经常成对出现。找出代表 e 的字符，首先将它译出来；
b） 英文中最常见的单词是 the。利用这个事实猜测什么字符代表字母 t 和 h。
c） 根据以上结果破译其它部分。
d） 注意，最终得到的英文明文直观上可能不大好懂。

2、 当海军上尉 john F. Kennedy 指挥的美国巡逻舰 PT-109 被日本毁灭者号击沉时，位于澳大利亚的一个无线站截获了一条用 Playfair 密码加密的消息：

KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBNT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

密钥为 royal new zealand navy，请解密这条消息。注意，将 TT 换为 tt。

3、 关于 Playfair 密码，

a） 有多少种可能的密钥？那些会产生相同加密结果的密钥也计算在内。将结果用 2 的幂形式表示，取最佳逼近。
b） 除去那些会产生相同加密结果的密钥，那么有多少有效的唯一密钥？

4、 若将 Hill 密码推广为 $[C]=[K_1][P]+[K_2] \bmod 26$，则 Vigenère 密码也可视为 Hill 密码的一个特例。试写出密钥为 vigenerecode 的维吉尼亚密码所对应的 Hill 密码形式及相应的密钥 K1 和 K2。

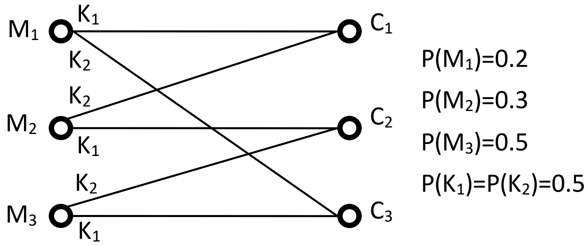
5、 解密由仿射密码加密的密文“DBUHU SPANO SMPUS STMIU SBAKN OSMPU SS”

6、 某加密系统，明文/密文字符集都是英文字母集合。加密算法首先对明文进行单表代换

操作，再对代换结果进行置乱操作。该系统是不能抵抗选择明文攻击的。问，对于一段长 15 个字符的密文，最少需要多少个选择明文就能保证破译？

第三章

1、 有一个如图的密码系统，请计算 $P(C_i)$、$P_{M2}(C_i)$、$P_{C2}(M_i)$，$(1\leqslant i\leqslant 3)$，并回答判断：它是闭合系统么？是单纯系统么？是完美安全系统么？



第四章

1、 求满足如下式子的 x：

a) $5x\equiv 4 \pmod 3$

b) $7x\equiv 6 \pmod 5$

2、 求

a) gcd(24140, 16762)

b) gcd(4655, 12075)

3、 用扩展欧几里得算法求下列元素的乘法逆元。

a) 1234 mod 4321

b) 24140 mod 40902

4、 判断下列多项式在 GF(2) 上是否可约。

a) x^3+1

b) x^3+x^2+1

c) x^4+1（仔细考虑）

5、 求下列各对多项式在相应有限域上的最大公因式：

a) x^3+x+1 和 x^2+x+1 在 GF(2) 上。

b) x^3-x+1 和 x^2+1 在 GF(3) 上。

c) $x^5+x^4+x^3-x^2-x+1$ 和 x^3+x^2+x+1 在 GF(3) 上。

6、 求 x^3+x+1 在 $GF(2^4)$ 里的乘法逆元，模 $m(x)=x^4+x+1$。

7、 利用费马定理计算 3^{201} mod 11。

8、 利用费马定理，找到一个位于 0 到 28 之间的整数 x，使得 x^{85} 模 29 与 6 同余。（你不能也不必用穷举搜索方法）

9、 利用欧拉定理，找到一个位于 0 到 28 之间的整数 x，使得 x^{85} 模 35 与 6 同余。（你不能也不必用穷举搜索方法）

10、利用一般整数 n 的欧拉函数公式，计算：

a) Φ(41)；

b) Φ(27)；

c) Φ(231)；

d) Φ(440)。

11、不用穷举法，证明 x=2 mod 6 且 x=3 mod 4 无解。

12、不解方程，证明 x=2 mod 6 且 x=0 mod 4 有解

13、六位教授分别在周一至周六开始授课，且分别每 2,3,4,1,6 和 5 天（即每隔 1,2,3,0,5 和 4 天）授一次课，该大学禁止周日上课（所以周日的课必须停止，注意是停止，不是推后）。什么时候所有六位教授首次发现必须同时停课？提示：利用 CRT。

14、求方程 6x mod 21=9 的所有解。

15、考虑方程组：$x \bmod p=x_1$ or $p-x_1$

$x \bmod q=x_2$ or $q-x_2$

其中 p、q 为素数，令 n=pq，有四种公共解：

z_1 = crt (n, p, q, x_1, x_2)　　z_2 = crt (n, p, q, x_1, q-x_2)

z_3 = crt (n, p, q, p-x_1, x_2)　　z_4 = crt (n, p, q, p-x_1, q-x_2)

证明 $z_4=n-z_1$ 及 $z_3=n-z_2$。

16、求解方程 $x^2 \bmod 77 = 4$。

17、定理：设 p 是素数，若 n 和 p-1 互素，则每个 $y(0\le y<n)$都有模 p 的 n 次根。

a) 证明，若 r 是 n 模 p-1 的乘法逆元，那么一个 n 次根是 $y^r \bmod p$。

b) 求解 $x^3=4 \bmod 5$

c) 求解 $x^3=4 \bmod 5*11$

18、假定拉各朗日插值多项式为 $h(x)=3x^3+5x+2 \bmod 7$，用来实现(t,n)的密钥共享，n=5。

(a) t 和 K 的值是多少？

(b) 如果 k_1=h(2)，k_2=h(4)，k_3=h(3)，k_4=h(5)，k_5=h(7)。如何从 k_1,k_2,k_4,k_5 重组 K?

19、现有 $p(x)=x^3+x^2+1=1101$ 和二进制多项式 $h(x)=(001x^2+101x+011) \bmod 1101$，运算在 $GF(2^3)$中进行。

(a) t 是多少？K 是什么？

(b) 对于 x_1=001，x_2=011，x_3=100，x_4=110，分别计算相应的 h(x)。

(c) 从 x_1,x_2 和 x_4 重组此二进制多项式。

20、用拉各朗日插值多项式实现秘密共享时，并非所有的多项式 h(x)都可以任意计算影子。考虑多项式 $h(x)=3x^3+5x+2 \bmod 7$，影子 h(1)=3, h(6)=1。注意到(h(1)+h(6))/2=2=K。这并不是巧合，请分析原因。这种现象会导致两个人就能恢复秘密，攻击者将很乐意进行这种尝试（毕竟，收买两个人进行一次尝试，比收买 t 个人划算得多）。为此，应当对模数保密。同时，为安全着想，对多项式的选择还应当增加一个什么样的限制，来确保即使模数泄露，也不会遭此攻击？

第五章

1、 考虑分组长度为 128 比特，密钥长度为 128 比特的 16 轮 Feistel 密码。假设对于给定的 k，前 8 个轮密钥（$k_1, k_2, \cdots k_8$）由密钥扩展算法决定，而后 8 个轮密钥设定为 $k_9=k_8, k_{10}=k_7, \cdots, k_{16}=k_1$。假设已截获密文 c，请解释，如何只向加密 oracle 做一次提问，而解密 c 获得明文 m？这表明上述的密码易于被选择明文攻击。（可以认为 oracle 就是一种黑盒子，给定一个明文，返回相应的密文。黑盒子的内部结构是未知的，当然也不允许打开查看，你所能做的就是对其进行提问并观察相应的输出。）

2、 16 个轮密钥（k1, k2, …, k16）在 DES 解密过程中是逆序使用的。因此，讲义中关于 DES 密钥轮密钥产生的算法不再正确。请对该算法略加修改，以适应解密过程。为提高算法效率，移位的次数应当尽量少。

3、 对于 DES 加密算法，

a) 设 X’是对 X 按位取反的结果。证明，如果明文和密钥都取反，则密文取反。即：

如果 Y=E(K, X)，则 Y’=E(K’, X’)

提示：首先证明对任意两个相同长度的串 A 和 B，有 $(A \oplus B)' = A' \oplus B$。

b) DES 的穷举攻击需要搜索 2^{56} 个密钥的密钥空间。（a）中的结论对此是否有影响？（考虑选择明文攻击）

4、 对于任意的分组密码，它的非线性对安全是至关重要的。为了证明这一点，假设我们有一个线性分组密码 EL，加密 128 比特的明文分组为 128 比特密文的密文分组。令 EL(k, m) 是 128 比特明文 m 在密钥 k 下的加密结果。则对任意的 128 比特的 m_1, m_2，有：

$$EL(k, [m_1 \oplus m_2]) = EL(k, m_1) \oplus EL(k, m_2)$$

请说明给定 128 个选择密文，在不知道密钥 k 的情况下，对手如何解密任何密文？（选择密文即对手可以选择密文，并能得到该密文的解密结果。此处，你有 128 个明密文对，且你可以选择密文的值。）

5、 填满下表中的剩余位置：

操作模式	加密	解密
ECB	$C_j=E(K, P_j)$ j=1, …, N	$P_j=D(K, C_j)$ j=1, …, N
CBC	$C_1=E(K, [P_1 \oplus IV])$ $C_j=E(K, [P_j \oplus C_{j-1}])$ j=2, …, N	$P_1=D(K, C_1) \oplus IV$ $P_j=D(K, C_j) \oplus C_{j-1}$ j=2, …, N
CFB		

OFB		
CTR		

6、 在DES的ECB模式中，若在密文的传输过程中，某一块发生了错误，则只有相应的明文组会有影响。然而，在CBC模式中，这种错误具有扩散性。比如，密文分组C1发生的错误将会影响明文组P_1和P_2。

a） P_2以后的所有块是否会受到影响？

b） 假设 P_1 本来就有一位发生了错误，则这个错误要扩散至多少个密文组？对接收者解密后的结果有什么影响？

7、 除了2DES算法，RSA实验室的学者们曾经讨论过另外两种结构：

$DESV_{k1,k2}(M)=DES_{k1}(M)\oplus k2$，

$DESW_{k1,k2}(M)= DES_{k1}(M\oplus k2)$，

这两种结构都不能增加穷举攻击的计算量$O(2^{56})$。请给出相应的攻击方式。假设有足够多的已知明文-密文对。

8、 设Alice有长度为n比特的密钥k_1,Bob有长度n比特的密钥k_2。他们希望加密消息M，使得密文必须使用双方的密钥才能解密。他们考虑使用某个分组密码算法E，并采用如下方案：

a. $C=E_{k1}[E_{k2}[M]]$

b. $C=E_{k1\oplus k2}[M]$

c. $C=(E_{k1}[r],\ E_{k2}[r\oplus M])$，这里r是每次更换的随机数。

问：

1） 假设攻击者已获得若干明文/密文分组对{M,C}，和待破译密文C'，则以上三种方案都可以在$O(2^n)$时间内破译，请说明攻击方法。

2） 哪种方案的攻击代价最小？哪种方案的攻击代价最大？

第六章

1、 任何时钟振荡器都存在一定误差，即使同一个时钟振荡器，其振荡频率也会随着时间的变化而发生漂移。这将造成时钟的不同步，进而导致流密钥系统的失同步。为此，许多系统采用额外的同步信号来进行辅助时钟同步。本题分析频率漂移对流密码系统的影响。假设移位寄存器每个时钟周期移位一次，加密方的时钟是理想无漂移的，频率为 f；解密方的时钟是有漂移的，其频率为 $f\pm\Delta f$。定义时钟精度为 $P=\Delta f/f$ 求：

a) 加密速率是多少？解密速率是多少？试粗略估计多长时间应进行一次同步？

b) 对 f=1MHz,100MHz，$p=10^{-9}$，分别计算（a）中结果。

2、 画出 LFSR<5,$1+D^2+D^5$>的结构，其周期是多少？当初始状态为 0,0,0,0,1 时，写出其输出的前 20 个比特。

3、 计算 n=11 的二元序列 1,0,0,1,1,0,1,0,0,1,1,0,1 的：

a) 线性复杂度；

b) 生成该序列的最小 LFSR；

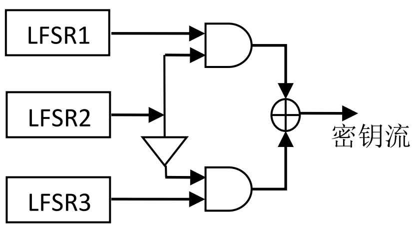
c) 确定此 LFSR 的初始状态（注意，Berlekamp-Massey 算法输出的联结多项式未必是本原多项式，甚至未必是非奇异的）；

d) 写出后续的 5 个比特。

4、 Geffe 非线性组合流密钥生成器的结构如图，

1) 设其中三个线性移位寄存器的结构为 LFSR1<2,$1+D^2$>，LFSR2<3,$1+D+D^3$>，LFSR3<2,$1+D+D^2$>，画出三个 LFSR 的结构。

2) 已知输出密钥流为 11111010 00101011，求三个 LFSR 的初始状态。



5、 RC4 的密钥值取什么的时候，使得 S 在初始化过程中没有变化？即在对 S 进行初始置换后，S 的元素的值按升序分别等于 0 到 255。

6、 许多随机数发生器的输出并不是理想的（伪）随机比特序列。一种常见的情况是输出的比特序列有偏差（1 和 0 的数目不平衡），但满足不相关性。假设某随机数发生器产生 1

的概率为 p，产生 0 的概率为 1-p，p≠0。找出一种方法将它的输出序列改造为无偏差不相关的随机序列。

7、 考虑一个由 $s_{n+1}=s_n-s_{n-1}$ 定义的整数域密钥流。证明，无论选取什么样的种子 $s=(s_0, s_1)$，密钥流的周期都为 6，或 6 的因子。（提示：写成矩阵乘法，验证其系数矩阵）

第七章

1、 Alice 选择 $p=5$, $q=7$, 将 $n=pq$ 发送给 Bob。Bob 选取 $a=3$ 并将 $a^2 \bmod n$ 发送给 Alice。Alice 从方程 $x^2=a^2 \bmod n$ 的四个根中任取一个发送给 Bob。请解此方程，并说明什么情况下 Bob 能确定 p 和 q?

2、 对素数 p 和 q，计算 $n=pq$。选定 a，$0<a<n$，令 x 和 y 是 a 模 n 的平方根，且 $y\neq x$，$y\neq n-x$。证明 $\gcd(x+y, n)=p$ 或 q。

3、 如果 $p=13$, $q=31$, $d=7$, 求 e；若 $m=3$, 给出加、解密过程。

4、 在使用 RSA 的公钥体制中，已截获发给某用户的密文 $C=10$，该用户的公钥 $e=5$, $n=35$，那么明文 M 等于多少？

5、 假定我们已知若干用 RSA 算法编码的分组，但不知私钥。假设 $n=pq$, e 是公钥。若某人说他知道其中有一个明文分组与 n 有公因子，这对我们有帮助吗？

6、 在 RSA 公钥密钥体制中，每个用户都有一个公钥 e，一个私钥 d。假定 Bob 的私钥已泄密。Bob 决定产生新的公钥和新的私钥，但不产生新的模数。请问这样安全吗？

7、 假设 Bob 使用 RSA 密码体制，其中模数非常大以使得因子分解是不可行的。假设 Alice 给 Bob 发消息，其中的字母表示为 0 到 25（$a\rightarrow 0,\ldots,z\rightarrow 25$）。然后对每个字母用 RSA 算法单独加密，参数 e 和 n 都很大。这种方法安全吗？如果不安全，请给出最有效的攻击方式。

8、 设 ElGamal 体制的公用素数 $q=71$，其本原根 $a=7$。

a) 若 B 的公钥 $Y_B=3$，A 选择的随机整数 $k=2$，则 $M=30$ 的密文是什么？

b) 若 A 选择的 k 值使得 $M=30$ 的密文为 $C=(59,C_2)$，则整数 C_2 是多少？

9、 椭圆曲线方程 $y^2=x^3+10x+5$ 在 Z_{17} 上能定义一个群吗？

10、利用课堂给出的方法实现椭圆曲线的加/解密。该密码体制的参数是 $E_{11}(1,6)$和 $G=(2,7)$，B 的私钥 $n_B=7$。

a) 找出 B 的公钥 Y_B。

b) A 要加密消息 $P_m=(10,9)$，其选择的随机值 $k=3$，试确定密文 C_m。

c) 试给出 B 由 C_m 恢复 P_m 的计算过程。

11、用户 A 和 B 使用 Diffie-Hellman 密钥交换技术来交换密钥，设公用素数 q=71，本原根 a=7。

a) 若用户 A 的私钥 X_A=5，则 A 的公钥 Y_A 为多少？

b) 若用户 B 的私钥 X_B=12，则 B 的公钥 Y_B 为多少？

c) 共享的密钥为多少？

12、有人提出一种方法，可以用来确认两个用户的密钥是否相同。首先，A 产生一个与密钥等长的随机二进制串 S，并将自己的密钥与 S 异或，然后将结果发送给 B。B 将收到的内容与自己的密钥异或，再发送回 A。则 A 可以通过将此结果与原始的 S 对比，检验密钥是否相同。但这个方法有不少缺点。你能找出两条么？

第八章

1、 可以利用散列函数构造类似 DES 结构的分组密码。但散列是单向的，而分组密码是可逆的（解密），那么如何利用散列码构造分组密码呢？

2、 在某些场合下，某些文件需要有两个签名者来签名，使得：

a) 第一签名者形成文件，对文件签名，并传给第二签名者；

b) 第二签名者可以验证文件已被第一签名者签名，并对签名文件进行第二次签名；

c) 任何接收者都可以验证该文件确实是由两个签名者签过的文件，但只有第二签名者可以验证步骤 a 中的签名。即接收方仅可以验证具有两个签名的完整文件，而不是只有一个签名的中间文件；

d) 希望利用现有的支持 RSA 数字签名的模块。

请给出实现方案。

3、 考虑 DSA 参数定义域生成问题。假设我们已经找到了参数 p 和 q，使得 q|(p-1)。现在我们需要寻找参数 $g\in Z_p$，使得 g mod p 的阶为 q。考虑如下两种算法：

算法 1	**算法 2**
重复 　选择 $g\in Z_p$ 　$h=g^q \bmod p$ 直至（h=1 和 $g\neq 1$） 返回g	重复 　选择 $h\in Z_p$ 　$g=h^{(p-1)/q} \bmod p$ 直至（$g\neq 1$） 返回g

a) 证明算法 1 返回的参数值的阶为 q；

b) 证明算法 2 返回的参数值的阶为 q；

c) 假设 p=40 193, q=157。算法 1 需要经过多少轮循环才可以找到一个生成元？

d) 如果 p 是 1024 比特长，q 为 160 比特长，你愿意推荐使用算法 1 来寻找 g 吗？为什么？

e) 假设 p=40 193, q=157。算法 2 首次循环找到生成元的概率有多大（如果有用，你可以使用$\sum_{(d|n)}\varphi(d)=n$ 这一事实来回答该问题）？

4、 假定 A 和 B 要用 RSA 方法进行一次保密又认证的通信。A 的公钥是(n_A, e_A)=(33, 7), B 的公钥是(n_B, e_B)=(15, 3)。

a) A 和 B 的秘密密钥 d_A 和 d_B 各是什么?

b) A 送消息 m=2 给 B，即保密又认证，密文 C 是什么?

c) B 如何从 C 解得 m？

5、 在 ElGamal 系统中, $\alpha=7$, $p=13$, $x_a=5$, $x_b=3$.

a) 假定 A 加密传送 m=3 给 B，随机选择 k=8，密文是什么？

b) 如果 A 要签名 m=7，随机选择 k=5，签名是什么？B 如何验证？

第九章

1、 E 国发现政府某些重要文件的拷贝存在于 R 国的电脑中。正常情况下，E 国存储重要文件的电脑管理严格，偶尔文件上网时也会经过最强的加密算法加密。经调查，E 国发现有一名可疑男子经常合法地使用政府的某台不重要的电脑，但他不可能接触到未经加密的文件。E 国的网络通信协议如下：

1. A 产生一个随机数 R 并且将自己的名字，接收者的名字 B，以及 $E_{ka}(R)$给服务器；
2. 服务器做出响应，发送 $E_{kb}(R)$给 A；
3. A 发送 $E_R(M)$和 $E_{kb}(R)$给 B
4. B 知道 k_b，可以将 $E_{kb}(R)$解密获得 R，再用 R 解密 $E_R(M)$得到 M。

请分析，他是如何获得文件明文的？

2、 假设一段视频包含了 n 帧画面，每帧画面包含两个从不同角度拍摄的略存差异的版本，记为（L_1,R_1），⋯，（L_n,R_n），其中 L_i（R_i）是左（右）摄像机拍摄的画面，i=1, ⋯ , n。视频发布者 A 希望进行如下管理：当客户 u 购买视频后，他能够获取视频的某一个版本，同时他的名字被嵌入视频中。例如，若客户 u 的名字用二进制串表示为 u=1011010⋯，他获得的视频画面序列为（$R_1,L_2,R_3,R_4,L_5,R_6,L_7$, ⋯），记该版本视频为 M_u。这样，当该视频出现在盗版市场时，发布者可以从 M_u 中提取出 u 的名字。

具体操作时，发布者首先向所有人公开发布一个免费的大数据 B。当客户 u 下载了大数据 B 后，他联系发布者 A 并购买一个解密密钥 k_u。通过 k_u，客户 u 可以解密 B，并获得且仅能获得 M_u，记为 $D(k_u,B)=M_u$。另一个客户 v 将获得另一个密钥 k_v，使得 $D(k_v,B)=M_v$。

1） 给出一个满足上述要求的实现方案，要求 B 的大小仅为单个版本视频的两倍，客户的解密密钥 k_u 包含 n 个 AES 密钥。
2） 给出一个方案，使得在 B 后附加 4n 个公开短密文后，客户密钥的大小可以缩减为 n/4 个 AES 密钥。
3） 说明，两个共谋的客户如何创建一个视频版本，使得其中不包含任何人的名字。

3、 假设用户 A 准备向用户 B_i(i=1,2,⋯,n)广播消息。这里秘密性并不重要，但所有用户 Bi 需要能够验证他所接收的消息来自 A。A 决定使用 MAC。问：

1） 若 A 和所有的 B_i 共享一个密钥 k，用户 A 使用密钥 k 计算消息的 MAC 值，并发送给所有 B_i。如此，所有的 B_i 都可以验证 MAC 值。请用一句话解释，为什么这个方案是不安全的。
2） 假设用户 A 有密钥集 $S=\{k_1,k_2,\cdots,k_m\}$，每个用户拥有 S 的一个子集 $S_i\subseteq S$。当用户 A 广播消息时，她使用每个密钥分别计算一个 MAC 值，并将这 m 个 MAC 值附加在消息后面。当用户 B_i 收到消息后，他验证他的密钥子集 S_i 中每个密钥对应的 MAC 值，若

都正确则确认消息来自用户 A。问 S_i应满足什么条件，才能保证该方案不会收到问题 1 中的攻击。（假设所有的 B_i不会共谋）

3） 当 n=6 时，用户 A 的密钥集 S 中最少应包含几个密钥？构造此时的 S_1~S_6。

4、 Alice 将一副牌（去掉大小王后的 52 张）随机且秘密地分一半给 Bob。现在，Alice 准备大声地告诉 Bob 一条秘密消息 M，偷听者 Eve 可以听到 Alice 说的所有内容。

1） 请为 Alice 设计一个具体的传讯方法。

2） 证明，Alice 有可能找到一种方法将 48 比特的信息 M 安全地传递给 Bob，且 Eve 不能获得 M 的任何信息；但完美安全地传递 49 比特的信息则不可能实现。