1.5.11 RSA加密

- 例: 用RSA密码系统以及密钥(2537,13)加密消息“STOP”. $2537 = 43 \cdot 59$, $p = 43, q = 59$ 是素数，并且 $\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$.
- 解:
  - 首先, 消息中每个字母翻译成两位数字:18 19 14 15
  - 因为2525 < 2537 < 252525, 所以划分为2N=4位等长的分组:1819 1415.
  - 对每个分组采用$C = M^{13}$ **mod** 2537来进行加密.
  - 因此 1819^{13} **mod** 2537= 2081, 1415^{13} **mod** 2537= 2182
  - 综上, 加密后的消息为2081 2182.

1.5.11 RSA解密

- RSA中，用解密密钥d**解密**：
  - 因为$\gcd(e,(p-1)(q-1))=1$，所以e模$(p-1)(q-1)$的逆d一定存在. 也就是$de \equiv 1\ (mod\ (p-1)(q-1))$
  - 当已知解密密钥d，RSA能够快速完成解密. 对每个分组用解密函数$M = C^d \bmod pq = C^d \bmod n$，这儿$C$是加密后的消息，$p$和$q$是$n=pq$中的两个大素数.
- RSA和一般的公钥密码系统一样，只有知道解密密钥d才能解密消息. 当前不知道d的情况下，因为两个大素数是无法在短时间内破译加密的消息.
- 例如按照现有的能力分解一个400位的整数需要上亿年的时间. 因此当p和q是200位的素数时，就目前的水平而言，RSA是安全的. 随着因子分解能力的提高，可能需要使用更大的素数.

1.5.11 RSA解密

- 例: 由上个例子中的密钥加密后的消息为0981 0461, 求解密后的消息是多少？【备注，上例题中RSA加密密钥是(2537,13)，其中2537=43*59】
- 解:
  - 加密密钥中n = 43· 59=2537, e=13. 那么d=13模42∗58的逆=937. 我们用937作为解密密钥d.
  - 要解密每个分组C, 需要计算$M = C^{937}\ \boldsymbol{mod}\ 2537$.
  - 因此, $0981^{937}\ \boldsymbol{mod}\ 2537 = 0704$, $0461^{937}\ \boldsymbol{mod}\ 2537 = 1115$.
  - 那么, 解密后的消息为0704 1115.
  - 对这个解密后的消息每两位翻译为一个字母:HELP.
  - 综上, 最终解密后的消息是HELP.

1.5.11 RSA解密

- 例:构造RSA公钥密码体系的密钥，令N=77
  - (1) 以d = 13为解密私钥, 求对应的加密公钥e.
  - (2) 求明文25对应的密文.
  - (3) 求密文15对应的明文.
- 解:
  - (1)N=77=7*11. 因此$(p-1)(q-1)$=60. e模$(p-1)(q-1)$的逆为d. 那么$de\equiv 1(mod\ 60)$, 可以得e=37.
  - (2) 要加密, $C = 25^{37}\ \boldsymbol{mod}\ 77$. 计算可得$C = 53$.
  - (3) 要解密, $M = 15^{13}\ \boldsymbol{mod}\ 77$. 计算可得$M = 64$.

1.5.12 密码协议: 密钥交换

- **密码协议**, 两方或者多方为了达到一个特定的安全目标而进行的消息交换.
- **密钥交换**是一种在双方以往没有共享过任何信息的情况下可以用来在不安全的通信信道上交换密钥的协议. 其中**迪菲-赫尔曼密钥协商协议**(或Diff-Helmen key交换协议, DH协议, DHKE), 它是在1976年由惠特菲尔德.迪菲和马丁.赫尔曼两个人的名字命名的协议.
  - 其实, 早在1974年, 为英国GCHQ秘密工作的马尔科姆.威廉姆森已经发明了该协议, 但因为保密的原因, 直到1997年他的发现才公之于众.

1.5.12 密码协议: 密钥交换

- 接下来将DH协议描述为如下例子:
  - 假设A和B想要共享一个公共密钥. 两人同意使用素数p和p的一个原根a.
  - A选择一个秘密整数k_1, 然后将$a^{k_1} \bmod p$ 发送给B.
  - B选择一个秘密整数k_2, 然后将$a^{k_2} \bmod p$ 发送给A.
  - A计算$(a^{k_2})^{k_1} \bmod p$.
  - B计算$(a^{k_1})^{k_2} \bmod p$.
- 在协议的最后，A和B已经计算了共享的密钥，即$(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p$.
- 想要找密钥, 那么需从p, a, $a^{k_1} \bmod p$ 和$a^{k_2} \bmod p$中计算出k_1, k_2. 这是求解离散对数的实例. 如果p和a足够大, 目前计算能力无法破解.

1.5.12 密码协议: 数字签名

- 密码学除了能够确保消息的保密性, 还可以用来使得消息的接受方知道消息来自哪个该来自的人. 例如利用RSA密码系统对消息施加**数字签名**可以达到以上要求.

1.5.12 密码协议: 数字签名

- 假设A的RSA公钥是(n, e)，私钥是d．A用加密函数$E_{(n,e)}(x) = x^e \ \boldsymbol{mod}\ n$来加密明文消息$x$. A用解密函数$D_{(n,e)}(y) = y^d \ \boldsymbol{mod}\ n$来解密密文消息$y$.
- A想要发送消息M, 使得每个收到该消息的人都知道来自她.
  - 首先像RSA加密一样, 将字母翻译成对应的数值, 并将所得的串分割成分组$m_1, m_2, \ldots, m_k$使得每个分组具有相同的大小, 并且其大小满足$0 \le m_i \le n$, $i = 1,2, \ldots, k$.
  - 然后, 针对每个分组应用解密函数$D_{(n,e)}$将得到$D_{(n,e)}(m_i)$, $i = 1,2, \ldots, k$. 将这个结果发送给所有预期的消息接收者.
  - 最后，消息接收者对每个分组应用A的加密函数$E_{(n,e)}$将得到$E_{(n,e)}(D_{(n,e)}(x)) = x$, 即结果为原始的明文信息M.

1.5.12 密码协议: 数字签名

- 例: Alice的RSA公钥是(2537,13), $2537 = 43 \cdot 59$, 她的解密密钥是d=937. 如果她想要发送消息“MEET AT NOON”给她的朋友使得朋友们能够确信消息来自她, 她该如何发送?
- 解:
  - 首先, 将消息翻译成数字分组为1204 0419 0019 1314 1413.
  - 然后, 对每个分组应用解密函数$D_{(2537,13)}(x) = x^{937} \ \boldsymbol{mod}\ 2537$. 可得结果分别为 $1204^{937} \ \boldsymbol{mod}\ 2537 = 817$, $419^{937} \ \boldsymbol{mod}\ 2537 = 555$, $19^{937} \ \boldsymbol{mod}\ 2537 = 1310$, $1314^{937} \ \boldsymbol{mod}\ 2537 = 2173$, $1413^{937} \ \boldsymbol{mod}\ 2537 = 1026$.
  - 因此, 她将发送0817 0555 1310 2173 1026.
  - 当她的朋友收到该消息时, 针对每个分组应用她的加密函数$E_{(2537,13)}$就能获得原始消息的数字分组, 然后通过翻译可以得到最初的英文字母消息.

1.5.13 同态加密

- **同态加密**是一种特殊的加密方法. 允许对密文进行处理得到仍然是加密的结果. 即对密文直接进行处理, 跟对明文进行处理后再对处理结果加密得到的结果相同. 从抽象代数的角度讲, 保持了同态性.
  - 备注:有兴趣的同学自学同态加密.

第1.5节 密码学小结

- 欧拉函数$\Phi(n)$, 欧拉定理$a^{\Phi(n)} \equiv 1 \ (mod \ n)$
- 古典密码学: 移位密码; 仿射密码; 换位密码; 维吉利亚密码
- 私钥加密, 加密和解密密钥都需要保密的加密
- 公钥加密, 加密密钥公开, 解密密钥保密的加密
- RSA加密密钥$k = (n, e)$, 解密密钥d是e模$(p-1)(q-1)$的逆
- 密码协议: 迪菲-赫尔曼密钥协商协议; 数字签名