第 4-6 讲: 加密算法

姓名: 朱宇博　　**学号:** 191220186

评分: ______　　**评阅:** ______

2021 年 4 月 6 日

请独立完成作业，不得抄袭。
若得到他人帮助, 请致谢。
若参考了其它资料，请给出引用。
鼓励讨论，但需独立书写解题过程。

1　作业（必做部分）

题目 1 (TJ 7-7(a,b))
Encrypt each of the following rsa messages x so that x is divided into blocks of integers of length 2; that is, if $x = 142528$, encode 14, 25, and 28 separately.
(a) n = 3551, E = 629, x = 31
(b) n=2257,E =47,x=23

解答:
(a)
$y = x^E \mod n = 31^{629} \mod 3551 = 2791$
(b)
$y = x^E \mod n = 23^{47} \mod 2257 = 769$

题目 2 (TJ 7-9(b))
Decrypt each of the following rsa messages y.
(b)
n=5893,D=81,y=34

解答:
$x = y^D \mod n = 34^{81} \mod 5893 = 2014$

题目 3 (TJ 7-12)
Find integers n, E, and X such that

$$X^E \equiv X \pmod n$$

Is this a potential problem in the rsa cryptosystem?

解答:
对于任意 X，令 $E = k\phi(n) + 1$，其中 $k \in \mathbb{N}$，即可满足该等式。
这是一个 potential problem in rsa。该方程说明，在给定 n 和 X 下，只需将 X 做 E 次乘法，即可获取 X。
这可以看成一个加密-解密的过程。我们需要找到一组对应关系，使得 $ab = E$, 则有加密 $y = x^a$, 解密 $x = y^b$。

题目 4 (TC 31.7-1)
Consider an RSA key set with p=11,q=29,n=319, and e=3. What value of d should be used in the secret key? What is the encryption of the message M=100?

解答:
$m = \phi(pq) = (p-1)(q-1) = 280$, $ed \equiv 1 \pmod{280}$. So d could be 187.
$y = M^d \mod n = 100^3 \mod 319 = 254$

题目 5 (TC 31.7-2)

> Prove that if Alice's public exponent e is 3 and an adversary obtains Alice's secret exponent d, where $0 < d < \phi(n)$, then the adversary can factor Alice's modulus n in time polynomial in the number of bits in n. (Although you are not asked to prove it, you may be interested to know that this result remains true even if the condition $e = 3$ is removed. See Miller [255].)

解答:
当 $n \geq 16$ 时，

$$\phi(n) = (p-1)(q-1) = (p-1)(\frac{n}{p} - 1) = n - (p + \frac{n}{p}) + 1 \geq n - 2\sqrt{n} + 1 \geq \frac{n}{2}$$

则有

$$k\phi(n) = 3d - 1 \leq 3n \rightarrow k \leq 6$$

所以在 $[1, 6]$ 之间枚举整数 k，即可使等式成立，求得 $\phi(n)$。
又有 $\phi(n) = (p-1)(q-1) = n - (p + \frac{n}{p}) + 1, q = \frac{n}{p}$，即可求得 p, q。
因为上述计算经过常数次长度不超过 $|n|$ 的加减乘除即可完成，故在 $|n|$ 的多项式时间内可对 n 进行质因数分解。
若 $n \leq 16$，则显然可在 $|n|$ 的多项式时间内可对 n 进行质因数分解。
综上，得证。

题目 6 (TC Problem 31-3)

解答:
(a)
在该情况下，有

$$T_n = T(n-1) + T(n-2) + O(1)$$

解得 $T(n) = O(\phi^n)$，其中 $\phi = \frac{\sqrt{5}+1}{2}$
(b)

在 (a) 的递归基础上，运用记忆化搜索，将每个计算出的 F_i 存下，避免重复计算。则在这种情况下，每个 F_i 都只会被计算一次，且计算时间为常数，故用时为 $O(n)$
(c)
根据斐波那契数列的性质，有

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$$

利用矩阵快速幂，即可在 $O(\lg n)$ 时间内完成。
(d)
第一种：
在该情况下，有

$$\begin{aligned} T(n) =& T(n-1) + T(n-2) + O(\lg F_{n-1}) \\ =& T(n-1) + T(n-2) + O(n) \end{aligned}$$

解得 $T(n) = O(\phi^n)$

第二种：
计算 F_n 时加法操作耗时 $O(n)$，则 F_n ~ F_1 中每个数被计算一次，耗时可近似为 $O(n^2)$
故此时时间复杂度为 $O(n^2)$

第三种：在该情况下，有

$$\begin{aligned} T(n) =& 2T(n/2) + O((\lg F_{\frac{n}{2}})^2) \\ =& 2T(n/2) + O(n^2) \end{aligned}$$

解得 $T(n) = O(n^2)$

---

2 作业（选做部分）

题目 1 (TC Problem 31-4)

解答：

---

3 Open Topics

Open Topics 1 (中国剩余定理)
向同学介绍中国剩余定理及其应用。

Open Topics 2 (椭圆曲线加密 (Elliptic Curve Cryptography, ECC))
椭圆曲线加密是基于椭圆曲线数学理论实现的一种非对称加密算法。相比 RSA，ECC 优势是可以使用更短的密钥，来实现与 RSA 相当或更高的安全。

(参考资料-1：https://medium.com/dev-genius/introduction-to-elliptic-curve-cryptography-567e47b0e49e) (参考资料-2：https://en.wikipedia.org/wiki/Elliptic-curve_cryptography)
(参考资料-3：https://www.jianshu.com/p/e41bc1eb1d81)

4 反馈