《密码学原理》作业 4

注意：因为课本版本不同，以下习题的题号可能会有出入，有的习题甚至在某些版本中不存在。请大家以以下影印内容为准。

1. （30 分）《Introduction to Modern Cryptography》338 页，习题 8.10。

8.10 Corollary 8.21 shows that if $N = pq$ and $ed = 1 \bmod \phi(N)$ then for all $x \in \mathbb{Z}_N^*$ we have $(x^e)^d = x \bmod N$. Show that this holds for all $x \in \{0, \ldots, N-1\}$.

Hint: Use the Chinese remainder theorem.

2. （30 分）《Introduction to Modern Cryptography》437 页，习题 11.21。

11.21 Fix an RSA public key $\langle N, e \rangle$ and define

$$\mathsf{half}(x) = \begin{cases} 0 & \text{if } 0 < x < N/2 \\ 1 & \text{if } N/2 < x < N \end{cases}$$

Prove that half is a hard-core predicate for the RSA problem.

Hint: Reduce to hardness of computing lsb.

3. （40 分）请用 Crypto++或者 Java Cryptography Architecture(JCA)实现一个程序，具有加密和解密两种功能。在用加密功能时，读出一个名为“key.txt”的文件中的 1024 位的密钥，一个名为“plain.txt”的文件中的一段不超过 1000 位的明文，用 RSA 加密后，密文写入一个叫做“encrypted.txt”的文件。在用解密功能时，读出一个名为“key.txt”的文件中的 1024 位的密钥，一个名为“encrypted.txt”的文件中的密文，用 RSA 解密后，密文写入一个叫做“decrypted.txt”的文件。所有文件格式均为纯文本，密钥、明文、密文均用二进制书写，形如“00111010……”。请提交全部源代码。提示：网上可以找到类似的源代码，但需要稍加修改才能达到本作业题的要求。

4. （附加题，做对奖励 30 分，做错或者不做不扣分）Define a new public key encryption scheme (Gen,E,D) as follows. Gen is the key generation algorithm of ElGamal, which outputs a pair of keys ((G,q,g,x),(G,q,g,y)) where $y=g^x$. The encryption algorithm differs from that of ElGamal. $E(m)=(g^r, y^r m, g^s, y^s m)$ where r and s are picked uniformly and independently from {0,1,…, q-1}. In other words, this algorithm generates two ElGamal ciphertexts and then puts them together. The decryption algorithm D only looks at the first two components of the ciphertext and decrypts it in

the same way as the ElGamal decryption algorithm. Is (Gen, E, D) CPA-secure? Prove your answer.

关于参考别人的作业：如果你参考了别人的作业，请在显眼处明确指出自己参考了谁的作业（姓名、学号一定要写清楚，参考了哪一题也请写清楚）。我们会在对方得分的基础上，适当降低一些，作为你的得分。如果你不做这样的说明，那么就会被视为抄袭，有可能受到严惩。无理由雷同的作业有可能全部得 0 分。