Fundamentals Of Information Science **2022 Spring**

Homework9

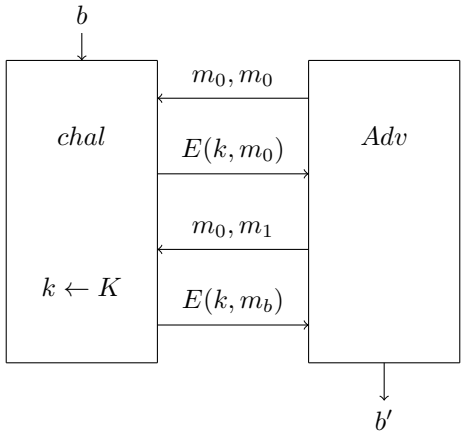
学生：华园（202000120027）) *时间：2022.3.23*

Problem 1.

Ciphertext expansion vs. security
Let $\mathcal{E} = (E, D)$ be an encryption scheme messages and ciphertexts are bit strings.
(a) Suppose that for all keys and all messages m, the encryption of m is the exact same length as m. Show that (E, D) cannót be semantically secure under a chosen plaintext attack.
(b) Suppose that for all keys and all messages m, the encryption of m is exactly ℓ bits longer than the length of m. Show an attacker that can win the CPA security game using $\approx 2^\ell/2$ queries and advantage $\approx 1/2$. You may assume the message space contains more than $\approx 2^\ell/2$ messages.

Solution.

(a)



由于CPA中多次询问用同一个密钥加密按照,所以上图的思路进行攻击，首先第一次发送两个相同的明文m_0，无论b等于0还是1，都会对m_0进行加密，因此我们可以获取到m_0加密后的密文。第二次攻击我们发送两条不同的明文m_0和m_1，系统会随机选取一个进行加密，然后我们收到密文，通过对比第一次获得的明文，我们就可以判断出加密的是m_0还是m_1，从而可以判断出b的数值，即：

$$Adv_{ss} = |Pr(W_0) - Pr(W_1)| = 1$$

这个结果是不可忽略的，因此不是语意安全的。
(b)问题分析：密文长度长于明文长度，即密文包括两部分，其中一部分是用密钥加密，另一部分是l位的随机数，攻击者获得CPA游戏胜利的条件是：能够根据密文区分出是m_0加密的还是m_1加密的。现在我们知道：攻击者具有的能力是具有$\frac{1}{2}$的概率识别出b的数值，同时有2^{l-1}次查询机会，现在我们需要证明的是，在剩下的不能识别的$\frac{1}{2}$中可以通过查询message space来获取明文。
证明：

message space空间包含多于2^{l-1}的消息，因为在CPA游戏中，使用的key是一样的，因此密文的不同之处就在于随机数的不同，则在剩余的$\frac{1}{2}$中最多需要查询次数

$$\frac{1}{2}2^l = 2^l/2$$

这样就一定可以从中找到相对应的明文和密文对，从而可以判断出b的值，因此结论得证。

Problem 2.

Understand public-key encryption
Given two random primers $(p, q) = (31, 43)$, you are asked to construct an RSA encryption based on the two primes (p, q) (although the primes are two small to guarantee security).
(a) Construct a pair of public key and secret key.
(b) Demonstrate the process of encrypting a message $m = 100$ with a random number $x = 13$ using the generated key pair, and then decrypt the resulting ciphertext.

Solution.

(a)由题目条件可知，p=31,q=43,则有

$$N = qp = 1333$$

则我们可以获得非p的整数倍和非q的整数倍的数字的个数为：

$$\varphi(N) = (p-1)(q-1) = N - p - q + 1 = 1260$$

则需要寻找一对整数e.d使得e • d mod $\varphi(N)$=1,经过计算获得e=13,d=97.因此我们可以获得公钥为（1333，13），私钥为（1333，97）
（b）我们假设加密的方式为(E,D),K为（E,D）的密钥空间，假设H（）为从Z_N到K的映射。则整个通信过程：
针对发送方：
(1)生成公钥（1333，13）和密钥（1333，97）
(2)对随机数x进行RSA处理获得y:

$$y = x^{13} mod 1333 = 864$$

(3)将随机数映射到K空间获得，

$$k = H(x) = H(13)$$

(3)利用k=H(13)对m进行加密，获得:

$$E(k, m) = E(H(13), 100)$$

(4)发送方输出(y,E(k,m)),即输出（864，E(H(13),100)）

针对接收方：
(1)接收到发送方消息之后，利用私钥97对y进行解密获得随机数x：

$$x = y^{97} mod 1333 = 13$$

(2)之后利用映射关系获得密钥：

$$k = H(x) = H(13)$$

(3)获得密钥之后，对获得的密文进行解密：

$$m = D(k, E(k, m)) = D(H(13), E(H(13), 100)) = 100$$