数据隐私HW3

范翔宇 PB1800000

Q1

解：先考虑单词的ASCII码

alpha：01100001 01101100 01110000 01101000 01100001

delta：01100100 01100101 01101100 01110100 01100001

sigma：01110011 01101001 01100111 01101101 01100001

three：01110100 01101000 01110010 01100101 01100101

case 1：alpha & three

key $\oplus$ alpha = c_1 $\rightarrow$ alpha $\oplus$ c_1 = key = 01100001 01101100 01110000 01101000 01100001 $\oplus$ 11111001 01111001 11001100 00010111 10000110 = 10011000 00010101 10111100 01111111 11100111 ①

key $\oplus$ three = c_2 $\rightarrow$ three $\oplus$ c_2 = key = 01110100 01101000 01110010 01100101 01100101 $\oplus$ 11101100 01111101 11001110 00011010 10000010 = 10011000 00010101 10111100 01111111 11100111 ②

可得①和②所得key一致。

case2：delta & sigma

key $\oplus$ delta = c_1 $\rightarrow$ delta $\oplus$ c_1 = key = 01100100 01100101 01101100 01110100 01100001 $\oplus$ 11111001 01111001 11001100 00010111 10000110 = 10011101 00011100 10100000 01100011 11100111 ③

key $\oplus$ sigma = c_2 $\rightarrow$ sigma $\oplus$ c_2 = key = 01110011 01101001 01100111 01101101 01100001 $\oplus$ 11101100 01111101 11001110 00011010 10000010 = 10011111 00010100 10101001 01110111 11100011 ④

可得③和④所得key并不一致。

综上，case1合理而case2不合理，即key = 10011000 00010101 10111100 01111111 11100111

Q2

解：令calling program P为：

P：

(k,c) := EAVESDROP(0^λ,1^λ)

f := k & c

return f $\stackrel{?}{=}$ 0^λ

则对于A $\diamond$ L_{left}，令c和k逐位取反，即c = ~k，则k & c = 0^λ，Pr[A $\diamond$ L_{left}] = 1

对于A $\diamond$ L_{right}，令c和k相同，即c = k，则 k & c = c，Pr[A $\diamond$ L_{right}] = $\frac{1}{2^\lambda}$

Q3

解：有定义如下：

Def (Negligible Function) : 一个函数$\mu(\cdot): \mathbb{Z}^+ \to [0,1]$ 被称为是negligible 函数 **iff** $\forall c \in \mathbb{Z}^+ \exists n_0 \in \mathbb{Z}^+ ; \forall n \geq n_0, \mu(n) < n^{-c}$.

e.g. 显然$\mu(n) = 2^{-n}$是一个Negligible Function。经过简化和计算，可得$\mu(n) = 2^{-n} = n^{\frac{-n}{\log_2 n}} \leq n^{-c}, \forall c \in Z^+$

需要提前声明的是，这里的log理解为底数为2的对数！

下面逐个讨论：

对于$\frac{1}{2^\lambda}$ = $\lambda^{\frac{-\lambda}{log\lambda}}$，而$lim_{\lambda->\infty}\frac{-\lambda}{log\lambda} = -\infty$，即对于$\forall c \in Z^+$，均有$2^{-\lambda} \leq \lambda^{-c}$，故为negligible function

对于$\frac{1}{2^{log(\lambda^2)}}$ = $\lambda^{\frac{-2log\lambda}{log\lambda}} = \lambda^{-2}$，$\exists c = 3$，有$\lambda^{-3} \leq \lambda^{-2}$，故不为negligible function

对于$\frac{1}{\lambda^{log\lambda}} = \lambda^{-log\lambda}$，又$lim_{\lambda->\infty} -log\lambda = -\infty$，即对于$\forall c \in Z^+$，均有$\lambda^{-log\lambda} \leq \lambda^{-c}$，故为negligible function

对于$\frac{1}{\lambda^2}$，$\exists c = 3$，有$\lambda^{-3} \leq \lambda^{-2}$，故不为negligible function

对于$\frac{1}{(log\lambda)^2}$，有$\lambda \geq log\lambda$恒成立，则$\lambda^{-2} \leq (log\lambda)^2$同样恒成立，故不为negligible function

对于$\frac{1}{\lambda^{1/\lambda}} = \lambda^{-1/\lambda}$，又$lim_{\lambda->\infty}\frac{-1}{\lambda} = 0$，$\exists c = 3$，有$\lambda^{-3} \leq \lambda^{-0}$，故不为negligible function

对于$\frac{1}{\sqrt{\lambda}} = \lambda^{-1/2}$，$\exists c = 3$，有$\lambda^{-3} \leq \lambda^{-1/2}$，故不为negligible function

对于$\frac{1}{2^{\sqrt{\lambda}}} = \lambda^{\frac{-\sqrt{\lambda}}{log\lambda}}$，而$lim_{\lambda->\infty}\frac{-\sqrt{\lambda}}{log\lambda} = -\infty$，即对于$\forall c \in Z^+$，均有$2^{-\sqrt{\lambda}} \leq \lambda^{-c}$，故为negligible function

Q4

解：(a)对于A $\diamond L^G_{prg-real}$时，s'无论如何都会遍历到对应的s，且G为一一映射，即有Pr[A $\diamond$ $L^G_{prg-real}$ $\to$ 1] = 1

对于A $\diamond L^G_{prg-rand}$时，由于只有 2^λ 种s'的值，且G为一一映射的，即只有2^λ种对应的G(s')，而r有$2^{\lambda+l}$种取值，故Pr[A $\diamond$ $L^G_{prg-rand}$ $\to$ 1] = $\frac{2^\lambda}{2^{\lambda+l}} = \frac{1}{2^l}$

则A在区分二者中的优势为1 - $\frac{1}{2^l}$，很明显不是negligible的。

(b)A遍历寻找所有的s'需要指数时间，不是多项式时间内的program。而两个library不可区分，要求输出1bit的program为多项式时间内的。故G为PRG不矛盾。

Q5

解：

需要提前声明的是，本题中的计算内容均由程序完成，(a)问代码贴在本题答案后面，(b)(c)问直接结合lab2中的powmod函数求解

(a)$\phi(n)$= (p - 1) (q - 1) = 10200，则只要是与10200互质的数均可作为公钥。经过程序计算得到有2559个互质数，即有2559个公钥可以选择

(b)n = pq = 101 × 103 = 10403

c = M^e mod n = 2021^{71} mod 10403 = 10000

即密文为10000

(c)私钥应该满足(de) mod n = 1

使用程序遍历计算得d = 431

解密有M = c^d mod n = 10000^{431} mod 10403 = 2021

附录：(a)问代码

```c
#include<stdio.h>
#include<math.h>
int gcd(int m, int n){
    return (m == 0) ? n : gcd(n%m, m);
}

int main(void){
    int i,count;
    count = 0;
    for(i = 2; i < 10200; i ++){
        if(gcd(i, 10200) == 1){
            count ++;
        }
    }
    printf("count:%d",count);
    return 0;
}
```

Q6

解：$\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$，而N = pq

$\phi(N)$ = pq - p - q + 1，可以结合N化为只关于p的方程，即$\phi(N)$ = N - p - $\frac{N}{p}$ + 1

令$\phi(N) = 0$，即方程化为$p^2 + (\phi(N) - N - 1)p + N = 0$。

而解这个二次方程需要多项式时间。

故此时可以在多项式时间内解出p和q。