数据隐私加密方法 HW3

王嵘晟　PB1711614

1.

”alpha” 转化为二进制:0110000101101100011100000110100001100001
”bravo” 转化为二进制:0110001001110010011000010111011001101111
”delta” 转化为二进制:0110010001100101011011000111010001100001
”gamma” 转化为二进制:0110011101100001011011010110110101100001
由此可判断出: c_1 是由”alpha” 加密而来，c_2 由”bravo” 加密而来，按位异或后求得 k:

$$k = 1001100000010101101111000111111111100111$$

2.

令 $m_L = \{0\}^\lambda$,$m_R = \{1\}^\lambda$，这样左边得到的 c 为 k 本身，右边得到的 c 为 k 按位取反。所以不可以互换

3.

$\frac{1}{2^{\frac{\lambda}{2}}}, \frac{1}{\lambda^{log\lambda}}, \frac{1}{2^{(log\lambda)^2}}, \frac{1}{2^{\sqrt{\lambda}}}$, 这些函数与 λ^c 相乘，当 $\lambda \to \infty$ 时，积趋近于 0

4.

a.

用 $\mathcal{A}$ 来验证 $\mathcal{L}^G_{prg-real}$ 时，当且仅当遍历到 s' 与 s 完全一致时，才会返回 1。但验证 $\mathcal{L}^G_{prg-rand}$ 时可能找不到，返回 0。所以是可以区分的，非 negligible。

b.

不违背，通过 G 生成的长度为 $\lambda + l$ 的伪随机数依然是均匀分布中不可区分的，没有违背 prg 的定义。

5.

a.

$p = 101, q = 73, n = p \times q = 7373$
$\Phi(n) = (p-1) \times (q-1) = 7200$
此时选取 e 使得 $1 < e < \Phi(n)$，且 e 与 $\Phi(n)$ 互质。则 e 共有 1919 个，所以由 (n, e) 组成的公钥共有 1919 个

b.

$c = M^e mod N$ 所以当 $M = 2008, e = 91, N = 7373$ 时，密文 $c = 2008^{91} mod\, 7373 = 2957$

c.

先计算私钥,$ed = 1 mod\, \Phi(n)$, 所以 $d = 2661$
解密：$M = 2957^{2661} mod\, 7373 = 2008$

6.

$\Phi(N) = (p-1) \times (q-1), N = p \times q$，所以 $\Phi(N) = p \times q - p - q + 1 = N - (p+q) + 1$。所以可得到方程组:

$$p \times q = N$$

$$p + q = p \times q - \Phi(N) + 1$$

整理得 $p^2 - (N - \Phi(N) + 1)p + N = 0$ 这个二次方程可以在多项式时间内求解。