Data Pravicy HW3

PB18111760 王嘉梁

一、

1. (10 pts) You (Eve) have intercepted two ciphertexts:

   $c_1 = 1111100101111100111001100000010111110000110$

   $c_2 = 1110110001111101110011100001101010000010$

   You know that both are OTP ciphertexts, encrypted with the same key. You know that either c_1 is an encryption of "alpha" and c_2 is an encryption of "three" **or** c_1 is an encryption of "delta" and c_2 is an encryption of "sigma" (all converted to binary from ascii in the standard way). Which of these two possibilities is correct, and why? What was the key k?

由OTP机制可知，key是一个与明文长度相同的密钥

" $alpha$ " 对应$ASCII$的二进制表示：0110000101101100011100000110100001100001

" $three$ " 对应$ASCII$的二进制表示：0111010001101000011100100110010101100101

" $delta$ " 对应$ASCII$的二进制表示：0110010001100101011011000111010001100001

" $sigma$ " 对应$ASCII$的二进制表示：0111001101101001011001110110110101100001

若为$c1 = enc(alpha)$且$c2 = enc(three)$，对加密过程来说：

$$0110000101101100011100000110100001100001 \oplus k = c1 \quad (1)$$
$$0111010001101000011100100110010101100101 \oplus k = c2 \quad (2)$$

由(1)得$k = 0110000101101100011100000110100001100001 \oplus c1 = 1001100000010101101111000111111111100111$

将(1)所得k代入(2)式，得到$c2' = 1110110001111101110011100001101010000010 = c2$，可知该情况合法。

若为$c1 = enc(delta)$且$c2 = enc(sigma)$，对加密过程来说：

$$0110010001100101011011000111010001100001 \oplus k = c1 \quad (3)$$
$$0111001101101001011001110110110101100001 \oplus k = c2 \quad (4)$$

由(3)得$k = 0110010001100101011011000111010001100001 \oplus c1 = 1001110100011100101000000110001111100111$

将(3)所得k代入(4)式，得到$c2' = 1110111001110101110001110000111010000110 \neq c2$，可知该情况非法。

综上所述，$c1 = enc(alpha)$、$c2 = enc(three)$、$k = 1001100000010101101111000111111111100111$

二、

2. (20 pts) Show that the following libraries are **not** interchangeable. Describe an explicit distinguishing calling program, and compute its output probabilities when linked to both libraries:

$\mathcal{L}_{\text{left}}$	$\mathcal{L}_{\text{right}}$
EAVESDROP$(m_L, m_R \in \{0,1\}^\lambda)$:	EAVESDROP$(m_L, m_R \in \{0,1\}^\lambda)$:
$k \leftarrow \{0,1\}^\lambda$	$k \leftarrow \{0,1\}^\lambda$
$c := k \oplus m_L$	$c := k \oplus m_R$
return (k, c)	return (k, c)

```
A:
    m_L={0}^lambda
    m_R={1}^lambda
    m={m_L,m_R}
    c:=EAVESDOP(m)
    L:=first half of c
    R:=second half of c
    return L=R ? L_left :L_right
```

在上述程序A中：

令$m_L=\{0\}^\lambda \qquad m_R=\{1\}^\lambda \qquad m=\{m_L,m_R\}$

$A\diamond\mathcal{L}_{left}$的输出$c$中，前半部分$L=k$，后半部分$R=k\oplus\{0\}^\lambda$，$k$中若为$1$的位与$0$异或得到$1$，为$0$的位与$0$异或得$0$

因此，若$A\diamond\mathcal{L}_{left}$，则其调用结果中，前后部分应相同，即$Pr[A\diamond\mathcal{L}_{left}\Rightarrow L=R]=1$

与此相反的是：

$A\diamond\mathcal{L}_{right}$的输出$c$中，前半部分$L=k$，后半部分$R=k\oplus\{1\}^\lambda$，$k$中若为$1$的位与$1$异或得到$0$，为$0$的位与$1$异或得$1$

因此，若$A\diamond\mathcal{L}_{right}$，则其调用结果中，前后部分按位相反，即$Pr[A\diamond\mathcal{L}_{right}\Rightarrow L=R]=0, Pr[A\diamond\mathcal{L}_{right}\Rightarrow L=\sim R]=1$

三、

3. (10 pts) Which of the following are negligible functions in λ? Justify your answers.

$$\frac{1}{2^\lambda},\ \frac{1}{2^{log(\lambda^2)}},\ \frac{1}{\lambda^{log\lambda}},\ \frac{1}{\lambda^2},\ \frac{1}{2^{(log\lambda)^2}},\ \frac{1}{(log\lambda)^2},\ \frac{1}{\lambda^{1/\lambda}},\ \frac{1}{\sqrt{\lambda}},\ \frac{1}{2^{\sqrt{\lambda}}}$$

$for\ every\ polynomial\ function\ p(\lambda)$

$(1)\lim\limits_{\lambda\to\infty}\frac{p}{2^\lambda}=0$ 因为指数函数增长速度快于任意多项式

$(2)\lim\limits_{\lambda\to\infty}\frac{\lambda^{100}}{2^{log(\lambda^2)}}=\lim\limits_{x\to\infty}\frac{x^{50}}{2^{logx}}=\lim\limits_{t\to\infty}\frac{(2^t)^{50}}{2^t}=\infty$

$(3)\lim\limits_{\lambda\to\infty}\frac{p}{\lambda^{log(\lambda)}}=\lim\limits_{\lambda\to\infty}\lambda^{C-log\lambda}=\lim\limits_{\lambda\to\infty}\lambda^{-\infty}=0$

$(4)\lim\limits_{\lambda\to\infty}\frac{\lambda^3}{\lambda^2}=\lim\limits_{\lambda\to\infty}\lambda=\infty$

$(5)\lim\limits_{\lambda\to\infty}\frac{p}{2^{(log\lambda)^2}}=\lim\limits_{\lambda\to\infty}\frac{p'}{log(2)*2^{(log\lambda)^2}*2log\lambda}=\ldots$洛必达！$\ldots=\lim\limits_{\lambda\to\infty}\frac{C}{O(2^{log^2\lambda})}=0$

$(6)\lim\limits_{\lambda\to\infty}\frac{p}{log^2\lambda}>\lim\limits_{\lambda\to\infty}\frac{p}{\lambda^2}=\lim\limits_{\lambda\to\infty}\frac{\lambda^3}{\lambda^2}=\infty$

$(7)\lim\limits_{\lambda\to\infty}\frac{p}{\lambda^{1/\lambda}}=\lim\limits_{\lambda\to\infty}\frac{p}{1}=\infty$

$(8)\lim\limits_{\lambda\to\infty}\frac{p}{\sqrt{\lambda}}>\lim\limits_{\lambda\to\infty}\frac{\lambda^3}{\sqrt{\lambda}}=\lim\limits_{\lambda\to\infty}\lambda^{2.5}=\infty$

$(9)\lim\limits_{\lambda\to\infty}\frac{p}{2^{\sqrt{\lambda}}}=\lim\limits_{x\to\infty}\frac{p(x^2)}{2^x}=0$

综上所述：$(1)\frac{1}{2^\lambda},(3)\frac{1}{\lambda^{log(\lambda)}},(5)\frac{1}{2^{(log\lambda)^2}},(9)\frac{1}{2^{\sqrt{\lambda}}}$ 是$negligible$的

四、

4. (20 pts) Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+l}$ be an injective (i.e., 1-to-1) PRG. Consider the following distinguisher:

```
𝒜
x := QUERY()
for all s′ ∈ {0,1}^λ:
  if G(s′) = x then return 1
return 0
```

```
ℒ^G_prg-real
QUERY():
  s ← {0,1}^λ
  return G(s)
```

```
ℒ^G_prg-rand
QUERY():
  r ← {0,1}^(λ+ℓ)
  return r
```

(a) What is the advantage of $\mathscr{A}$ in distinguishing $\mathscr{L}^G_{prg-real}$ and $\mathscr{L}^G_{prg-rand}$? Is it negligible?

(b) Does this contradict the fact that G is a PRG? Why or why not?

(a):

$$The\ x\ from\ L^G_{prg-real}\ is\ G(s)$$

由于PRG是单射的，所以对于$\{0,1\}^\lambda$中的数s'，能够映射到$\{0,1\}^{\lambda+l}$空间中的也只有2^λ个数

固定x，任意一个长度为λ的串s'，得到$G(s')$，$P[G(s')=x]=\dfrac{1}{2^\lambda}$，故$P[A \diamond L^G_{prg-real}=1]=\dfrac{2^\lambda}{2^\lambda}=1$

$$The\ x\ from\ L^G_{prg-rand}\ is\ r \leftarrow\ \{0,1\}^{\lambda+l}$$

则此时x的取值空间大小为$\{0,1\}^{\lambda+l}$，而$G(s')$取值空间大小仍是$\{0,1\}^\lambda$

x有$2^{\lambda+l}-2^\lambda$种取值是$G(s')$不可能取到的

固定x，任意一个长度为λ的串s'，得到$G(s')$，$P[G(s')=x]=\dfrac{2^\lambda}{2^{\lambda+l}} * \dfrac{1}{2^\lambda}=\dfrac{1}{2^{\lambda+l}}$

故$P[A \diamond L^G_{prg-real}=1]=\dfrac{2^\lambda}{2^{\lambda+l}}$

故$advantages=1-\dfrac{2^\lambda}{2^{\lambda+l}}$，这个函数不是$negligible$的

(b):

这与G是PRG不冲突。因为G是所产生的长度为$\lambda+l$的串和随即均匀分布在$\{0,1\}^{\lambda+l}$的空间中依旧是不可区分的

五、

5. (20 pts) Assume that Bob uses RSA and selects two "large" prime numbers p = 101 and q = 103.

   (a) How many possible public keys from which Bob can choose?

   (b) Assume also that Bob uses a public encryption key e = 71. Alice sends Bob a message M = 2021. What will be the ciphertext received by Bob?

   (c) Show the detailed procedure that Bob decrypts the received ciphertext.

(a):

$$n = p * q = 10403,\ \phi(n) = (p-1)(q-1) = 10200$$
$$\text{欲选取}\,pub\text{满足}\,gcd(pub, \phi(n)) = 1,\text{即计算}\,\phi(10200),\text{使用}\,wolframe,\text{算得}\,2560$$
$$\text{所以}\,pub\text{的选择共}\,2560\text{种}$$

(b):

$$\begin{aligned} &e = 71, n = 10403, M = 2021 \\ &c = M^e \ mod\ n = 2021^{71} mod\ 10403 \\ &\quad = 10000 \end{aligned}$$

(c):

$$\begin{aligned}
&\text{由}\,e * d \equiv 1\ mod\ \phi(n) \\
&\text{得}\,d * 71 = 10200k + 1, k \geq 1 \\
&k = 3\text{时，得到}\,d = 431 \\
&M = c^d\ mod\ n \\
&\quad = 10000^{431}\ mod\ 10403 \\
&\text{由}\,10000^4 \equiv 1617\ mod\ 10403 \\
&M \equiv (10000^4)^{107} * 10000^3\ mod\ 10403 \\
&\quad \equiv 1617^{107} * 4849\ mod\ 10403 \\
&\text{由}\,1617^7 \equiv 1920\ mod\ 10403 \\
&M \equiv (1617^7)^{15} * 1617^2 * 4849\ mod\ 10403 \\
&\quad \equiv 1920^{15} * 1617^2 * 4849 \\
&\text{由}\,1920^5 \equiv 1617\ mod\ 10403 \\
&M \equiv 1617^5 * 4849\ mod\ 10403 \\
&\quad \equiv 2021
\end{aligned}$$

六、

6. (20 pts) Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time. (Hint: Derive a quadratic equation (over the integers) in the unknown p.)

由pq互质，得$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = N - p - q + 1$

可以得到方程组：

$$\begin{cases} p * q = N \\ N - p - q + 1 = \phi(n) \end{cases}$$

即是：

$$\begin{cases} p * q = N \\ p + q = N + 1 - \phi(n) \end{cases}$$

N和$\phi(n)$是已知的

又有$(p+q)^2 - 4pq = (N + 1 - \phi(n))^2 - 4N = (p-q)^2$

假设$p > q$, 则$|p - q| = p - q$

所以$p - q = \sqrt{(N + 1 - \phi(n))^2 - 4N}$

所以$p = \dfrac{p + q + (p - q)}{2} = \dfrac{N + 1 - \phi(n) + \sqrt{(N + 1 - \phi(n))^2 - 4N}}{2}$

$q = \dfrac{p + q - (p - q)}{2} = \dfrac{N + 1 - \phi(n) - \sqrt{(N + 1 - \phi(n))^2 - 4N}}{2}$

(因为p, q在算法中是对称的，所以解出的两个值是可以互换的)

以上涉及运算为实数的加、减、开根号、除，均可在多项式时间内完成

证毕！