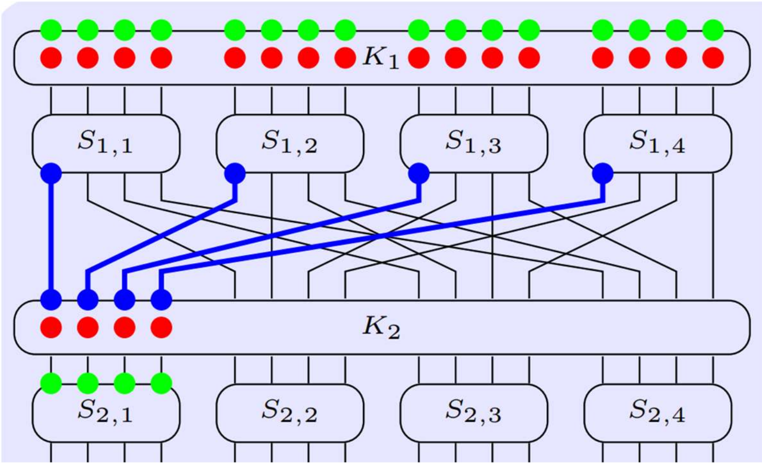
HomeWork3

120L020614-刘昕烨

Problem 1：



1. 此时我们先猜测 8+8*8=72 位的密钥，其中 8 位属于K_2另外的 64 位属于K_1。如果我们猜测错误的话，由于输出是随机的，因此测试通过的概率为2^{-8}。并且由于我们要遍历所有的密钥，所以遍历的次数为2^{72}。因此我们选择使用 16 对输入输出对（其实大于 9 对即可，**但是**一般使用 2 的幂，所以选择了 16 对输入输出对。）来使得随机遍历时出错的期望下降到小于 1（$2^{72-16\times 8}=1.38778\times 10^{-17}$）。此时我们的复杂度为$16*2^{72}*8=2^{79}$。

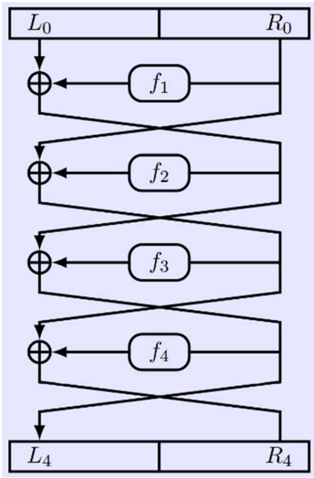
2. 同样的我们先猜测 72 位的密钥，其中 8 位属于K_2另外的 64 位属于K_1，接着选择的 IO 对的数目与第 1 问相同，唯一不同的是复杂度为$16*2^{72}*16=2^{80}$。

3. 从上面看我们发现复杂度其实与分块长度和 Sbox 的长度均相关。下面我们进行分析：

   我们假设分块长度为 B，Sbox 的长度为 S（S<B，且$B\%S=0$，且$S^2\leq B$）。首先我们要猜测 S+S*S 位的密钥，然后我们用的输入输出对的数目为 k，由于出错的期望：$2^{(S+1)*S-k*S}<1$所以我们假设 k 选择 S+2（先抛去 2 的幂次这一习惯）。因此我们的复杂度为$(S+2)*2^{S*(S+1)}*\dfrac{B}{S}$，我们发现当任意一者增加时都会使复杂度增加。复杂度的上界为$2B*2^{S^2+S}$（假设 S 大于等于 2）。

我们以复杂度的上界为准，假设 S 增加百分之 a，B 不变其变化率为：$2^{a^2S^2+3aS}$，S 不变，B 增加百分之 a 变化率为：$1+a$。考虑到二者的实际值，我认为在某一固定的个 S，B 点，两者增加相同比率，S 增加产生的变化率大于 B 增加产生的变化率。

Problem 2：



证明:

我们先对如果输入 x 与密钥 k 取反进行简单的分析，由于 DES 会对 k 以及输入进行扩展我们需要分析经过取反 DES 变化之后的 x 与 k 与原 x 与 k 的关系。

先分析 k，DES 需要的 16 个子密钥是由主密钥先经过置换移位选择得到的，这些操作都不会改变密钥本身的数值，而且对密钥进行选择操作得到的位数也与密钥本身无关，所以我们认为得到的第 i 轮的密钥K_i'是原来的第 i 轮密钥K_i的按位取反即$K_i'=\bar{K}_i$。

由于明文输入进行处理之前先要进行 IP 置换，假设其产生的新明文叫$IP(x')$，我们接下来的分析就由它进行，由于其进行的是置换其与之前的输入满足$IP(x')=\overline{IP(x)}$。

接下来，我们对 sp 网络中用到的扩展函数进行分析，由于其只会复制输入 x 一半的比特因此其不会对 x 的数值位产生变化。我们假设每一轮用到的 sp 网络为函数f_i，观察其构造我们容易得出：$f_i(k,x)=f_i\left(\bar{k},\bar{x}\right)$。

首先我们有：$R_0'=\overline{R_0}$，$L_0{}'=\overline{L_0}$。接下来我们分析当 x 与 k 反转后得到的L_1',R_1' 与原来的有何区别:

$$L_1{}'=R_0{}'=\bar{L}_1 \tag{1.1}$$

$$R_1{}'=f_1(K_1{}',R_0{}')\oplus L_0{}'=L_0{}'\oplus f_1(K_1,R_0) \tag{1.2}$$

并且我们可以由异或的性质得到以下的公式:

$$x\oplus\bar{y}=\overline{x\oplus y} \tag{1.3}$$

所以有

$$R_1{}'=\overline{R_1} \tag{1.4}$$

假设对于第 i 轮我们的假设$R_i{}'=\overline{R_i}$，$L_i{}'=\overline{L_i}$成立，我们对第 i+1 轮进行推理:

$$L_{i+1}{}'=R_i{}'=\overline{R_i}=\overline{L_{i+1}} \tag{1.5}$$

$$R_{i+1}{}'=L_i{}'\oplus f_{i+1}(K_{i+1}{}',R_i{}')=L_i{}'\oplus f_{i+1}(K_{i+1},R_i)=\overline{R_{i+1}} \tag{1.6}$$

发现其仍然符合此规律。

所以我们不难知道 16 轮以后我们的规律仍然存在，因此经过 Feistel 网络之后的 $Feistel(IP(x'))=\overline{Feistel(IP(x)}$，再经过一次逆 IP 置换我们可以知道这不会对这一关系产生影响，所以我们有:

$$DES_k(x)=\overline{DES_{\bar{k}}(\overline{x})} \tag{1.7}$$

■

Problem 3:

我认为这个函数不是单向函数, 因为加法给定一个$f(x,y)$可以找到多个符合要求的(x, y）对，这样的话就可以轻易的构造攻击者 A。例如我有一个攻击者 A 他返回以下的值:

$$\begin{cases}(0,0)\,(f(x,y)=0)\\(f(x,y)-1,1)\,(f(x,y)>0)\end{cases}$$

很容易验证这个攻击者成功的概率为 1，这与我们的定义不符合。

Problem 4:

我认为不一定是单向函数:

证明:

下面说明存在反例使得 f 不为单向函数。假设f_1,f_2均由单向函数f_3构造而来，且均定义如下：$f_1,f_2:\{0,1\}^{256}\rightarrow\{0,1\}^{256}$。构造如下的函数 f:

$$f_1(x||x_1)=f_3(x)||x_1(|x|=|x_1|,|x_1|>128)$$
$$f_2(x||x_1)=f_3(x_1)||x(|x|=|x_1|,|x|>128)$$
$$f(x_1||x_2)=f_1(x_1,x_2)||f_2(x_1,x_2)=f_3(x_1)||x_2||f(x_2)||x_1$$

其中f_1,f_2均为 ppt 上的例子，均是可逆函数。我们可以很轻松的为 f 构造攻击者 A: 把输入的值的 129 到 256 位作为x_2第 385 到 512 位作为x_1然后返回(x_1,x_2)。实验每次都会成功，所以以f_1,f_2作为参数的函数 f 不一定是可逆的。

■

Problem 5：

第一问我认为$f(f(x))$不一定是单向函数，我们可以构造一个函数 f 来证明。

证明:

假设存在单向函数h, 有: $h\colon\{0,1\}^n\to\{0,1\}^n, f\colon\{0,1\}^{2n}\to\{0,1\}^{2n}$。且有$x\in\{0,1\}^n$, $x_1\in\{0,1\}^n$。

构造 f 如下:

$$f(x||x_1)=\begin{cases}\{0\}^{2n}(x=\{0\}^n)\\ 0^n||h(x)\end{cases}\tag{1.8}$$

我们很容易知道$f(f(x))$的值恒为为长度为 2n 的 0 串，因此不是单向函数。

下证 f 是单向函数:

我们假设$Pr[Invert_{\mathcal{A},f}(1^{2n})=1]=c(n)$，下面我们构造$\mathcal{A}'$攻击函数 h，函数 h 向$\mathcal{A}'$输入$(1^n,h(x))$、然后$\mathcal{A}'$将$(1^{2n},0^n||h(x))$ 输入给$\mathcal{A}$，并把$\mathcal{A}$的输出的前 n 位直接当作$\mathcal{A}'$的输出。我们可以得到:

$$Pr[Invert_{\mathcal{A}',h}[1^n]=1]\geq Pr[Invert_{\mathcal{A},f}[1^{2n}]=1\,|x\neq\{0\}^n]\tag{1.9}$$

由于我们有:

$$\begin{aligned}Pr[Invert_{\mathcal{A},f}[1^{2n}]=1]=&Pr[Invert_{\mathcal{A},f}(1^{2n})=1\,|x\neq\{0\}^n]\cdot Pr[x\neq\{0\}^n]\\&+Pr[Invert_{\mathcal{A},f}(1^{2n})=1\,|x=\{0\}^n]\cdot Pr[x=\{0\}^n]\end{aligned}\tag{1.10}$$

化简得:

$$\begin{aligned} Pr[Invert_{\mathcal{A},f}[1^{2n}]=1] &\leq Pr[Invert_{\mathcal{A},f}(1^{2n})=1\,|x\neq\{0\}^n]+Pr[x=\{0\}^n] \\ &\leq Pr[Invert_{\mathcal{A}',h}(1^n)=1]+Pr[x=\{0\}^n] \end{aligned} \tag{1.11}$$

及:

$$Pr[Invert_{\mathcal{A}',h}(1^n)=1]\geq c(n)-\frac{1}{2^n} \tag{1.12}$$

由于 h 是单向函数，且 $\frac{1}{2^n}$ 可忽略，所以 c(n)可忽略，所以 f 是单向函数。

■

第二问我认为 g（x）是单向函数,

证明:

我们构造 $g(x)=f(x)||f(f(x))$，其中：f: $\{0,1\}^n\rightarrow\{0,1\}^{2n}$，$x\in\{0,1\}^n$。假设有一个对其的攻击者 $\mathcal{A}'$，我们有一个对单向函数 f 的攻击者 $\mathcal{A}$ 利用 $\mathcal{A}'$ 进行攻击。

首先 $\mathcal{A}$ 收到 f(x)后计算 f(f(x))然后将 $(1^n,f(x)||f(f(x)))$ 传给 $\mathcal{A}'$，然后将 $\mathcal{A}'$ 的输出直接输出，那么我们可以得到:

$$Pr[Invert_{\mathcal{A}',g}(1^{2n})=1]=Pr[Invert_{\mathcal{A},f}(1^n)=1]=\varepsilon(n)$$

又因为 f 是单向函数所以我们得到 g 也是单向函数。

■