دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

پاسخنامه تمرین شماره ۲

نگارنده: آیسان نیشابوری

- Upload your answers on courseware with the name: StudentNumber.pdf
- Upload a PDF file. Image and zip formats are not accepted.
- Similar answers will not be graded.
- NO answers will be accepted via e-mail.
- You can't upload files bigger than 2 Mb, so you'd better type.
- Deadline time is always at 23:55 and will not be extended.
- You should submit your answers before soft deadline.
- You will lose 5 percent for each day delay if you submit within a week after soft deadline.
- You can not submit any time after hard deadline.
- This problem set includes 55 points.
- For any question contact Aysan Nishaburi via `aysannishaburi@gmail.com`.

Problem 1

Let $\{p_k\}_{k\in\{0,1\}^*}$ be a pseudorandom permutation collection, where for $k \in \{0,1\}^n$, p_k is a permutation over $\{0,1\}^m$.

1. (10 Points) Consider the following encryption scheme (E, D) : $E_k(x) = p_k(x)$, $D_k(y) = p_k^{-1}(y)$. Prove that this scheme is not a CPA-secure encryption.

   Solution:
   We describe the distinguisher $\mathcal{D}$ such that it outputs the two messages m_0 and m_1 such that $m_0 \neq m_1$, we know that a uniform bit b is chosen and $c \leftarrow E_k(m_b)$ is computed and given to $\mathcal{D}$. Now $\mathcal{D}$ has oracle access to the function so $\mathcal{D}$ queries it's oracle $\mathcal{O}$ on m_1 and receives $E(m_1)$.
   $\mathcal{D}$ outputs 1 if $E(m_1) = c$ and 0 otherwise. This distinguisher always wins because if $m_b = m_1$ then c will always be equal to $E_k(m_b)$ because the encryption described is deterministic, more so if $m_b = m_0$ then $\mathcal{D}$ will never output 1 because p_k is a pseudorandom permutation and can't map m_1 and m_0 to the same value. So the advantage of this distinguisher is

   $$\left| \Pr\left[\text{out}_{\mathcal{D}}(\text{PrivK}^{\mathsf{eav}}_{\mathcal{D},\Pi}(n,0)) = 1\right] - \Pr\left[\mathsf{out}_{\mathcal{D}}(\text{PrivK}^{\mathsf{eav}}_{\mathcal{D},\Pi}(n,1)) = 1\right] \right| = |0 - 1| = 1$$

   which is not negligible so we have proven this scheme is not CPA secure.

2. (10 Points) Consider the following scheme (E, D) that encrypts $m/2$-bit messages in the following way: on input $x \in \{0,1\}^{m/2}$, E_k chooses random $r \leftarrow_R \{0,1\}^{m/2}$ and outputs $p_k(x, r)$ (where comma denotes concatenation), on input $y \in \{0,1\}^m$, D_k computes $(x, r) = p_k^{-1}(y)$ and outputs x. Prove that (E, D) is a CPA-secure encryption scheme.

   Solution:
   First we observe that if there was a random permutation like q instead of p_k then the scheme described would be CPA-secure. The reason for this is to encrypt we would just concat random numbers and so, any query that a distinguisher would ask would give it no information since the permutation is completely random. So any output from the distinguisher will have the chance of $\frac{1}{2}$ of winning. That means

   $$\Pr\left[\mathcal{D}^{q(.)}(1^n)\right] = \frac{1}{2}$$

   Now we imagine that a distinguisher such as $\mathcal{D}$ for the scheme in our question. We

use reduction to show that if the scheme described is not CPA-secure then we can construct a distinguisher $\mathcal{D}'$ that can distinguish p_k from a random permutation. We build $\mathcal{D}'$ such that it runs $\mathcal{D}$ and whenever $\mathcal{D}$ requests an encryption of m, $\mathcal{D}'$ chooses a random string $r \in \{0,1\}^{m/2}$ and queries it's oracle $\mathcal{O}$ on (m, r) and gives $\mathcal{O}(m, r)$ to $\mathcal{D}$. When $\mathcal{D}$ outputs m_0 and m_1, $\mathcal{D}'$ chooses a random bit b and chooses a random string $r \in \{0,1\}^{m/2}$ and returns it to $\mathcal{D}$. At the end when $\mathcal{D}$ makes a decision and outputs it, $\mathcal{D}'$ outputs the same decision.
Now we have

$$\Pr_{k \leftarrow \{0,1\}^n}\left[\mathcal{D}'^{p_k(.)}(1^n) = 1\right] = \Pr\left[\mathrm{PrivK}^{\mathsf{cpa}}_{\mathcal{D},\Pi}(n) = 1\right]$$

And as we said before

$$\Pr_{k \leftarrow \{0,1\}^n}\left[\mathcal{D}'^{q(.)}(1^n) = 1\right] = \frac{1}{2}$$

So we have

$$\left|\Pr\left[\mathrm{PrivK}^{\mathsf{cpa}}_{\mathcal{D},\Pi}(n) = 1\right] - \frac{1}{2}\right| =$$

$$\left|\Pr_{k \leftarrow \{0,1\}^n}\left[\mathcal{D}'^{p_k(.)}(1^n) = 1\right] - \Pr_{k \leftarrow \{0,1\}^n}\left[\mathcal{D}'^{q(.)}(1^n) = 1\right]\right| \leq \mathrm{negl}(n)$$

And this gives us

$$\Pr\left[\mathrm{PrivK}^{\mathsf{cpa}}_{\mathcal{D},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

which shows that the scheme described is CPA-secure.

Problem 2

(25 Points) Suppose that $\{F_S : \{0,1\}^k \rightarrow \{0,1\}^k | S \in \{0,1\}^k\}$ is a pseudo-random family of functions from k-bit input to k-bit output, indexed by k-bit key ("seed"). We would like to get a new pseudo-random function family in which each function maps k bits to $2k$ bits. Consider the following construction, and for each show whether it is good or bad (namely whether the specified family is pseudo-random or not).

1. $F^1_S(x) = F_S(0^k)||F_S(x)$

Solution:
F^1_S is not a pseudorandom function. Consider the distinguisher $\mathcal{D}_1$, that queries it's oracle $\mathcal{O}$ on any arbitrary x_1 and x_2 such that $x_1 \neq x_2$ and receives the values $y_1 = \mathcal{O}(x_1)$ and $y_2 = \mathcal{O}(x_2)$, and outputs 1 if the first k bits of y_1 and y_2 are equal and 0 if they are not.
If $\mathcal{O} = F^1_S$ then $\mathcal{D}_1$ will always output 1 but if $\mathcal{O} = f$ where f is chosen uniformly from the set of all functions mapping k-bit strings to $2k$-bit strings, then the probability that $\mathcal{D}_1$ outputs 1 is equal to the probability that the first k bits of

$f(x_1)$ is equal to the first k bits of $f(x_2)$ which happens with the probability of 2^{-k}, so

$$\big|Pr[\mathcal{D}_1^{F_S^1(.)}(1^n) = 1] - Pr[\mathcal{D}_1^{f(.)}(1^n) = 1]\big| = |1 - 2^{-k}|$$

which is not negligible.

2. $F_S^2(x) = F_S(x)||F_S(\bar{x})$

Solution:
F_S^2 is not a pseudorandom function. Consider the distinguisher $\mathcal{D}_2$, that queries it's oracle $\mathcal{O}$ on any arbitrary x and $\bar{x}$ and receives the values $y_1||y_2 = y = \mathcal{O}(x)$ where $|y_1 = y_2|$ and $z_1||z_2 = z = \mathcal{O}(\bar{x})$ where $|z_1| = |z_2|$, and outputs 1 if $z_1 = y_2$ and $z_2 = y_1$ and 0 if it is not.
If $\mathcal{O} = F_S^2$ then $\mathcal{D}_2$ will output 1 with the probability of 1, but if $\mathcal{O} = f$ where f is chosen uniformly from the set of all functions mapping k-bit strings to $2k$-bit strings, then the probability that $\mathcal{D}_2$ outputs 1 is equal to the probability that $y_2||y_1 = f(\bar{x})$ which happens with the probability of 2^{-2k}, so

$$\big|Pr[\mathcal{D}_2^{F_S^2(.)}(1^n) = 1] - Pr[\mathcal{D}_2^{f(.)}(1^n) = 1]\big| = |1 - 2^{-2k}|$$

which is not negligible.

3. $F_S^3(x) = F_{0^k}(x)||F_S(x)$

Solution:
F_S^3 is not a pseudorandom function. Consider the distinguisher $\mathcal{D}_3$, that queries it's oracle $\mathcal{O}$ on any arbitrary x and receives the values $y = \mathcal{O}(x)$. Now the distinguisher $\mathcal{D}_3$ independently calculates $F_{0^k}(x) = x'$, and outputs 1 if the first k bits of y is equal to x', and 0 if it is not.
If $\mathcal{O} = F_S^3$ then $\mathcal{D}_3$ will output 1 with the probability of 1, but if $\mathcal{O} = f$ where f is chosen uniformly from the set of all functions mapping k-bit strings to $2k$-bit strings, then the probability that $\mathcal{D}_3$ outputs 1 is equal to the probability that the first k bits of $f(x)$ are equal to x' which happens with the probability of 2^{-k}, so

$$\big|Pr[\mathcal{D}_3^{F_S^3(.)}(1^n) = 1] - Pr[\mathcal{D}_3^{f(.)}(1^n) = 1]\big| = |1 - 2^{-k}|$$

which is not negligible.

4. $F_S^4(x) = F_{S_1}(x)||F_{S_2}(x)$,where $S_1 = F_S(0^k)$ and $S_2 = F_S(1^k)$

Solution:
Let us define R_1, R_2 and $R = (R_1||R_2)$ random functions such that $R_1 : \{0,1\}^k \rightarrow \{0,1\}^k$, $R_2 : \{0,1\}^k \rightarrow \{0,1\}^k$ and $R_3 : \{0,1\}^k \rightarrow \{0,1\}^{2k}$. We also define the functions g_1, g_2 and $g = (g_1||g_2)$ such that $g_1 = F_{S_3}$, $g_2 = F_{S_4}$ and $g = (F_{S_3}||F_{S_4})$

where S_3 and S_4 are chosen randomly from $\{0,1\}^k$.
We claim that F_S^4 is a pseudorandom function. Suppose that it is not. Hence there is a distinguisher $\mathcal{A}$ such that

$$\Big|\Pr[\mathcal{A}^{F_S^4(.)}(1^n)=1]-\Pr[\mathcal{A}^{f(.)}(1^n)=1]\Big|>\text{negl}(n)$$

where f is chosen uniformly from the set of all functions mapping k-bit strings to $2k$-bit strings.
Now we use $\mathcal{A}$ to build a distinguisher $\mathcal{B}$ for F_S. $\mathcal{B}$ works such that given the oracle $\mathcal{O}$, it choses the random $i\in\{1,2,3\}$ and outputs $\mathcal{A}^{f_i(.)}(1^n)$ such that $f_1=F_{\mathcal{O}(0^k)}||F_{\mathcal{O}(1^k)}$, $f_2=g_1||\mathcal{O}$ and $f_3=\mathcal{O}||R_2$.
If $\mathcal{O}=F_S$ we will have

$$f_1=(F_{F_S(0^k)}||F_{F_S(1^k)})=(F_{S_1}||F_{S_2})=F_S^4$$

$$f_2=(g_1||F_S)\approx(F_{S_3}||F_{S_4})\approx(g_1||g_2)\approx g$$

because S like S_4 is chosen randomly from $\{0,1\}^k$ and

$$f_3=(F_S||R_2)\approx(F_{S_3}||R_2)\approx(g_1||R_2)$$

because S like S_3 is chosen randomly from $\{0,1\}^k$.
But if $\mathcal{O}$ is a random function we will have

$$f_1\approx(F_{S_5}||F_{S_6})$$

where S_5 and S_6 (like S_3 and S_4) are randomly chosen from $\{0,1\}^k$. So

$$f_1\approx(F_{S_3}||F_{S_4})\approx(g_1||g_2)\approx g$$

$$f_2=(g_1||\mathcal{O})\approx(g_1||R_2)$$

$$f_3=(\mathcal{O}||R_2)\approx(R_1||R_2)\approx R$$

Now we write the advantage of $\mathcal{B}$ as

$$\frac{1}{3}\Big|\Pr[\mathcal{A}^{F_S^4(.)}(1^n)=1]-\Pr[\mathcal{A}^{g(.)}(1^n)=1]+\Pr[\mathcal{A}^{g(.)}(1^n)=1]-\Pr[\mathcal{A}^{(g_1||R_2)(.)}(1^n)=1]+$$

$$\Pr[\mathcal{A}^{(g_1||R_2)(.)}(1^n)=1]-\Pr[\mathcal{A}^{R(.)}(1^n)=1]\Big|=\frac{1}{3}\Big|\Pr[\mathcal{A}^{F_S^4(.)}(1^n)=1]-\Pr[\mathcal{A}^{R(.)}(1^n)=1]\Big|=$$

$$\frac{1}{3}\Big|\Pr[\mathcal{A}^{F_S^4(.)}(1^n)=1]-\Pr[\mathcal{A}^{f(.)}(1^n)=1]\Big|>\frac{1}{3}\text{negl}(n)$$

which means $\mathcal{B}$ has non negligible advantage which is not possible since $\mathcal{B}$ is a distinguisher for F_S which was considered to be pseudorandom.

Problem 3

What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

1. (10 Points) Each round function outputs all 0's, regardless of the input.

   Solution:
   The structure of a Feistel network is as follows

   $$L_{i+1} = R_i$$

   $$R_{i+1} = L_i \oplus F(R_i, K_i)$$

   So if in each round the function outputs all 0's we will have

   $$L_{i+1} = R_i$$

   $$R_{i+1} = L_i$$

   This shows us that R_0 and L_0 just switch places in each round. So if r is even the output of the Feistel network will be (L_0, R_0), and (R_0, L_0) if r is odd.

2. (10 Points) Each round function is the identity function.

   Solution:
   If each round's function is the identity function we will have

   $$(L_1, R_1) = (R_0, L_0 \oplus F(R_0, K_0)) = (R_0, L_0 \oplus R_0)$$

   $$(L_2, R_2) = (L_0 \oplus R_0, R_0 \oplus F(L_0 \oplus R_0, K_1)) = (L_0 \oplus R_0, R_0 \oplus L_0 \oplus R_0) = (L_0 \oplus R_0, L_0)$$

   $$(L_3, R_3) = (L_0, L_0 \oplus R_0 \oplus F(L_0, K_2)) = (L_0, L_0 \oplus R_0 \oplus L_0) = (L_0, R_0)$$

   So the output repeats itself after 3 rounds which gives us the output (L_0, R_0) if r mod $3 = 0$, $(R_0, L_0 \oplus R_0)$ if r mod $3 = 1$ and $(L_0 \oplus R_0, L_0)$ if r mod $3 = 2$.