Solutions to Crypto Midterm

1.

(a)

$$
\begin{aligned}
&Pr[C=0|M=0]=Pr[k\in\{0,26\}]=\frac{2}{31},\\
&Pr[C=0|M=16]=Pr[k=10]=\frac{1}{31},\\
&Pr[C=0|M=0]\neq Pr[C=0|M=16].
\end{aligned}
$$

(b) We select the keys $\{0,1,2,3,4,26,27,28,29,30\}$ with probability $\frac{1}{52}$ and other keys with probability $\frac{1}{26}$, then the shift cipher is still perfectly secure.

Actually, you just need to guarantee that $Pr[k\in\{0,26\}]$=$Pr[k\in\{1,27\}]$=$\ldots$=$Pr[k\in\{4,30\}]$=$Pr[k=5]$=$Pr[k=6]$=$\ldots$=$Pr[k=25]$ holds.

2.

(a) No. When $n>2$, $\sqrt{\log n}<\log n,\ f_1(n)=2^{-\sqrt{\log n}}>2^{-\log n}.\ 2^{-\log n}=n^{-1}\neq O(n^{-2})$ is non-negligible. Therefore, $f_1(n)$ is non-negligible.

(b) Yes. For all constants c, we have $0<n^{c-\log\log\log n}<n^{-1}$ for all n satisfies $\log\log\log n\geq c+1$ (all $n>2^{2^{2^{c+1}}}$). By Squeeze Lemma:

$$
\lim_{n\to\infty}n^{-1}=0\Rightarrow\lim_{n\to\infty}\frac{n^c}{n^{\log\log\log n}}=0
$$

(c) Yes. With Stirling's approximation, we know

$$
n!\sim\sqrt{2\pi n}(\frac{n}{e})^n
$$

Therefore,

$$
f_3(n)\sim\sqrt{2\pi n}(\frac{1}{e})^n
$$

For all constants c, we have

$$
\lim_{n\to\infty}n^c\cdot f_3(n)\sim\lim_{n\to\infty}\frac{\sqrt{2\pi}n^{c-\frac{1}{2}}}{e^n}=0
$$

(d) No. Suppose that $g(n)=\frac{n}{n+1}$, which satisfies the requirements that $0<g(n)<1$ for all $n\geq 1$, $f_4(n)$ is non-negligible, because

$$
\lim_{n\to\infty}f_4(n)=\lim_{n\to\infty}(g(n))^n=\lim_{n\to\infty}(\frac{n}{n+1})^n=1
$$

(e) No. Because $h(n)$ is negligible, when $n\to\infty, h(n)\to 0$,but when $n\to 0$, the negligible function may not be negligible. For example, when $g(n)=e^{-n}$, for any $h(n)$

$$
\lim_{n\to\infty}f_5(n)=\lim_{n\to\infty}\frac{1}{e^{h(n)}}=1
$$

3.

G' is a PRG.

Firstly, we define $H(y)=y_{[0,n)}||G(y_{[n,2n)})$, where y is a random $2n$-bit string. Since G is a PRG, For any PPT Algorithm D, there is a negligible function $negl_1$ such that

$$
|Pr[D(H(y))=1]-Pr[D(G'(x))=1]|\leq negl_1(n).
$$

Otherwise, we can construct a distinguisher D' based on a D: $D'(s)=D(s_{[0,n)}||G(s_{[n,2n)}))$ such that

$$
\begin{aligned}
&|Pr[D'(r)=1]-Pr[D'(G(x))=1]|\\
=&|Pr[D(H(r))=1]-Pr[D(G'(x))=1]|
\end{aligned}
$$

is non-negligible, which contradicts that G is a PRG.

Similarly, we can prove that for ant PPT Algorithm D, there is a negligible function $negl_2$ such that

$$|Pr[D(H(y)) = 1] - Pr[D(r) = 1]| \leq negl_2(n),$$

where r is a random $3n$-bit string.

In conclusion, for ant PPT Algorithm D, there are negligible functions $negl_1$ and $negl_2$ such that

$$\begin{aligned}
&|Pr[D(G'(x)) = 1] - Pr[D(r) = 1]| \\
=&|(Pr[D(G'(x)) = 1] - Pr[D(H(y)) = 1]) + (Pr[D(H(y)) = 1] - Pr[D(r) = 1])| \\
\leq&|Pr[D(H(y)) = 1] - Pr[D(r) = 1]| + |Pr[D(H(y)) = 1] - Pr[D(G'(x)) = 1]| \\
\leq&negl_1(n) + negl_2(n)
\end{aligned}$$

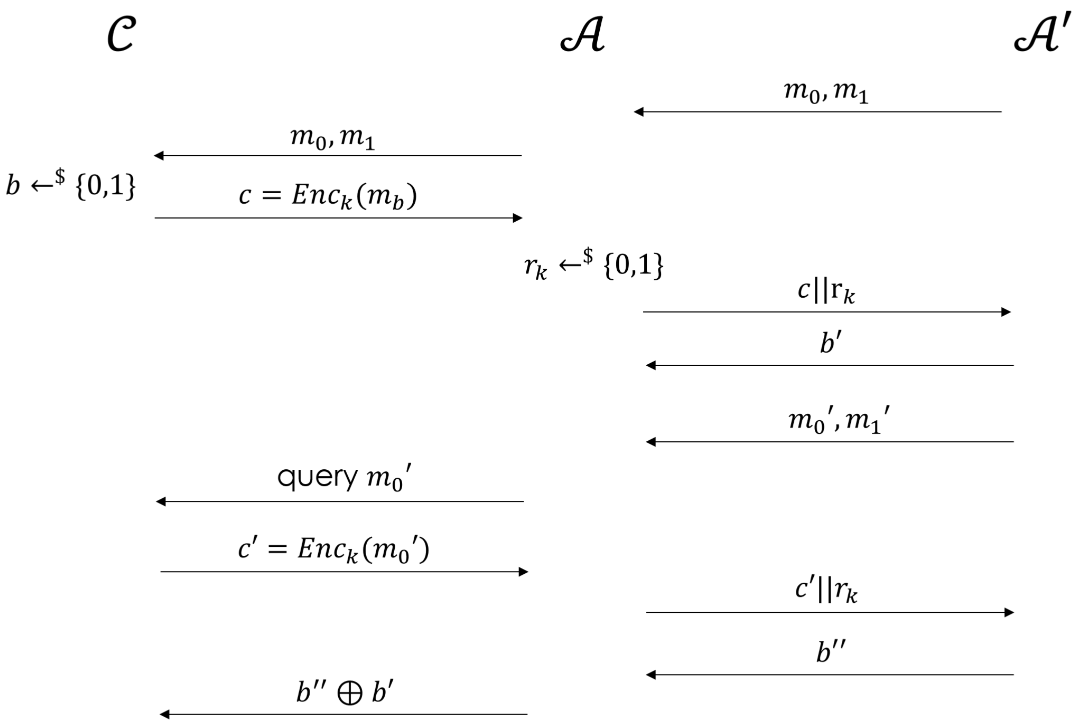
is negligible, which means that G' is also a PRG.

4.

Π' is CPA secure.

Suppose that Π' is not CPA secure and there is an adversary $\mathcal{A}'$ that can win the CPA-game of Π' with non-negligible probability. We construct an adversary $\mathcal{A}$ to break Π based on $\mathcal{A}'$:

1. $\mathcal{A}$ run $\mathcal{A}'$ for the first time and receive m_0, m_1;
2. $\mathcal{A}$ send m_0, m_1 to $\mathcal{C}$;
3. $\mathcal{C}$ uniformly choose a bit $b \xleftarrow{\$} \{0,1\}$ and send $c = Enc_{\Pi(k)}(m_b)$ to $\mathcal{A}$;
4. $\mathcal{A}$ choose a random bit $r_k \xleftarrow{\$} \{0,1\}$ and send $c||r_k$ to $\mathcal{A}'$;
5. $\mathcal{A}'$ send a guess b' to $\mathcal{A}$;
6. $\mathcal{A}$ run $\mathcal{A}'$ for the second time and receive m_0', m_1';
7. $\mathcal{A}$ query $\mathcal{C}$'s oracle for message m_0' and get the ciphertext $c' = Enc_{\Pi(k)}(m_0')$;
8. $\mathcal{A}$ sends $c'||r_k$ to $\mathcal{A}'$;
9. $\mathcal{A}'$ sends a guess b'' to $\mathcal{A}$.
10. If $b'' = 0$ then $\mathcal{A}$ outputs b', otherwise it outputs $\overline{b'}$.



We denote $Pr[\mathcal{A}'\ wins|r_k = LSB(k)] = \frac{1}{2} + \epsilon_1(n)$ and $Pr[\mathcal{A}'\ wins|r_k \neq LSB(k)] = \frac{1}{2} + \epsilon_2(n)$.

In this way,

$$
\begin{aligned}
&Pr[\mathcal{A}\ wins] \\
=&Pr[\mathcal{A}\ wins|r_k = LSB(k)] \times Pr[r_k = LSB(k)] + Pr[\mathcal{A}\ wins|r_k \neq LSB(k)] \times Pr[r_k \neq LSB(k)] \\
=&\frac{1}{2}Pr[\mathcal{A}\ wins|r_k = LSB(k)] + \frac{1}{2}Pr[\mathcal{A}\ wins|r_k \neq LSB(k)] \\
=&\frac{1}{2}(Pr[b' = b|r_k = LSB(k)] \times Pr[b'' = 0|r_k = LSB(k)] + Pr[\overline{b'} = b|r_k = LSB(k)] \times Pr[b'' = 1|r_k = LSB(k)]) \\
&+ \frac{1}{2}(Pr[b' = b|r_k \neq LSB(k)] \times Pr[b'' = 0|r_k \neq LSB(k)] + Pr[\overline{b'} = b|r_k \neq LSB(k)] \times Pr[b'' = 1|r_k \neq LSB(k)]) \\
=&\frac{1}{2}(Pr[\mathcal{A}'\ wins|r_k = LSB(k)] \times Pr[\mathcal{A}'\ wins|r_k = LSB(k)] + Pr[\mathcal{A}'\ loses|r_k = LSB(k)] \times Pr[\mathcal{A}'\ loses|r_k = LSB(k)]) \\
&+ \frac{1}{2}(Pr[\mathcal{A}'\ wins|r_k \neq LSB(k)] \times Pr[\mathcal{A}'\ wins|r_k \neq LSB(k)] + Pr[\mathcal{A}'\ loses|r_k \neq LSB(k)] \times Pr[\mathcal{A}'\ loses|r_k \neq LSB(k)]) \\
=&\frac{1}{2}[(\frac{1}{2} + \epsilon_1(n))^2 + (\frac{1}{2} - \epsilon_1(n))^2] + \frac{1}{2}[(\frac{1}{2} + \epsilon_2(n))^2 + (\frac{1}{2} - \epsilon_2(n))^2] \\
=&\frac{1}{2}(\frac{1}{2} + 2 \times \epsilon_1^2(n)) + \frac{1}{2}(\frac{1}{2} + 2 \times \epsilon_2^2(n)) \\
\geq&\frac{1}{2} + \epsilon_1^2(n)
\end{aligned}
$$

where $\epsilon_1(n)$ is non-negligible, which contradicts Π is CPA secure.

5.

(a) We can simply query a message x of one block to the oracle $\mathcal{O}$. The oracle returns the value $y = x \oplus E_k(IV)$.

Hence, $E_k(IV)$ is found by computing $x \oplus y$.

(b) Set $m = x_l||x_2$ and $x_l = E_k(IV) \oplus IV$. We then have $y_l = IV$ and $y_2 = h \oplus IV$. Thus,

$$x_2 = E_k(y_1) \oplus y_2 = E_k(IV) \oplus IV \oplus h.$$