1.

~~a 01100001 $\oplus$ key = 11111001~~

~~key = 0110 0001 $\oplus$ 1111 1001 = 1001 1000~~

~~t 0111 0100 $\oplus$ 1001 1000 = 1110 1100~~

alpha 0110 0001 0110 1100 0111 0000 0110 1000 0110 0001

$\oplus$

C_1

= 1001 1000 0001 0101 1011 1100 0111 1111 1110 0111

three 0111 0100 0110 1000 0111 0010 0110 0101 0110 0101

$\oplus$

C_2

= 1001 1000 0001 0101 1011 1100 0111 1111 1110 0111

故 ~~E(C1) E1(k,c)=~~ E(key, "alpha") = C_1 E(key, "three") = C_2 可能是正确的

key = 1001 1000 0001 0101 1011 1100 0111 1111 1110 0111

delta 0110 0100 0110 0101 0110 1100 0111 0100 0110 0001

$\oplus$

C_1

= 1001 1101 0001 1100 1010 0000 0110 0011 1110 0111

simga 0111 0011 0110 1001 0110 0111 0110 1101 0110 0001

$\oplus$ C_2

= 1001 1111 0001 0100 1010 1001 0111 0111 1110 0011

故第二种可能不正确

No.

Date.

2.

$\mathcal{A}$

$(k, c) = \text{EAVESDROP}(m_L, m_R)$

return $k \oplus c \overset{?}{=} m_L$

$\cancel{A}$

$k \oplus m_L \oplus k = m_L$

$\Pr[\mathcal{A} \diamond \mathcal{L}_{left} \Rightarrow 1] = 1$

$\Pr[\mathcal{A} \diamond \mathcal{L}_{right} \Rightarrow 1] = \frac{1}{2^\lambda}$

故 $\mathcal{L}_{left}$ 和 $\mathcal{L}_{right}$ 不是可交换的

No.

Date.

3.

$\lim_{\lambda \to \infty} \frac{\lambda^c}{2^\lambda} = 0$ ✓ negligible

$\lim_{\lambda \to \infty} \frac{\lambda^c}{2^{\log(\lambda^2)}} = \lim_{\lambda \to \infty} \frac{\lambda^c}{2^{2\log(\lambda)}} = 0$ ✓ negligible

$\lim_{\lambda \to \infty} \frac{\lambda^c}{\lambda^{\log \lambda}} = 0$ ✓ negligible

$\lim_{\lambda \to \infty} \frac{\lambda^c}{\lambda^2} \neq 0$ if $(c \geq 2)$ ×

$\lim_{\lambda \to \infty} \frac{\lambda^c}{2^{(\log \lambda)^2}} = 0$ ✓ negligible

$\lim_{\lambda \to \infty} \frac{\lambda^c}{(\log \lambda)^2} = \infty$ if $(c \geq 2)$ ×

$\lim_{\lambda \to \infty} \frac{\lambda^c}{\lambda^{1/2}} = \lim_{\lambda \to \infty} \lambda^c \neq 0$ if $(c \geq 0)$ ×

$\lim_{\lambda \to \infty} \frac{\lambda^c}{\sqrt{\lambda}} \neq 0$ if $(c \geq \frac{1}{2})$ ×

$\lim_{\lambda \to \infty} \frac{\lambda^c}{2^{\sqrt{\lambda}}} = 0$ ✓ negligible

4.

(a) G 为 $\{0,1\}^\lambda \to \{0,1\}^{\lambda+l}$ 的单射

又因 $|\{0,1\}^\lambda| = 2^\lambda$ $\quad |\{0,1\}^{\lambda+l}| = 2^{\lambda+l}$

存在 $t \in \{0,1\}^{\lambda+l}$ $\quad \forall s \in \{0,1\}^\lambda \quad G(s) \neq t$

因此 当 $\mathcal{L}^G_{prg\text{-}rand}$ 返回 t 时 $A \circ \mathcal{L}^G_{prg\text{-}rand}$ 返回 0

而对于 $A \circ \mathcal{L}^G_{prg\text{-}real}$，在任何情况下都返回 1

故 A 可区分 $\mathcal{L}^G_{prg\text{-}real}$ 和 $\mathcal{L}^G_{prg\text{-}rand}$

$\Pr[A \diamond \mathcal{L}^G_{prg\text{-}real} \Rightarrow 1] = 1$

$\Pr[A \diamond \mathcal{L}^G_{prg\text{-}rand} \Rightarrow 1] = \frac{2^\lambda}{2^{\lambda+l}} = \frac{1}{2^l}$

$|\Pr[A \diamond \mathcal{L}^G_{prg\text{-}real} \Rightarrow 1] - \Pr[A \diamond \mathcal{L}^G_{prg\text{-}rand} \Rightarrow 1]| = \frac{2^l - 1}{2^l}$

~~It not~~ It is not negligible

(b)

不矛盾

因为尽管 G只能生成 2^λ 个长为 $\lambda+l$ 的 0.1 序列，

但因为在多项式时间无法区别 G 和真正意义上的 长为$\lambda+l$的随机数生成器，故 G 仍是 ~~PG~~ PRG.

No.

Date.

5.

(a) 无穷多个

(b) $n = pq = 101 \times 103 = 10403$

$c = E(M) = M^e \bmod n$

$c = E(2021) = 2021^{71} \bmod 10403$

$c = 10000$

(c)

$m = D(c) = c^d \bmod n$

$de \bmod \varphi(n) = 1 \quad de = k\varphi(n) + 1 \quad \varphi(n) = (p-1)(q-1)$

$d = \dfrac{3 \times 100 \times 102 + 1}{71} = 431$

$m = D(10000) = 10000^{431} \bmod 10403 = 2021$

6.

$N = pq$

$\phi(N) = (p-1)(q-1) = pq - (p+q) + 1$

$\phi(N) = N - (p + \frac{N}{p}) + 1$

$\cancel{\phi(N) - N + 1}$

$\Rightarrow \quad p^2 + [\phi(N) - N - 1]p + N = 0$

由此一元二次方程求根可得 p