1. $G^{'}(k_1,k_2) = G(k_1)||G(k_2)$ is a ***secure*** PRG, because the $G(k)$ is a secure PRG and k_1, k_2 are different keys, the concatenation of $G(k_1)$ and $G(k_2)$ is still "random" and its output is still "indistinguishable" from a true random.

   $G^{'}(k) = G(0)$ is a ***not secure*** PRG, because the output of $G(0)$ is not "random".

   $G^{'}(k) = G(k)$ is a ***secure*** PRG, because the $G(k)$ is a secure PRG.

   $G^{'}(k) = G(k)||0$ is a ***not secure*** PRG, because the last bit of $G^{'}(k)$ is zero. Its output is not "random".

   $G^{'}(k) = G(k \oplus 1^S)$ is a ***secure*** PRG. Let $k_1 = k \oplus 1^S$, we can easily know $k_1 \overset{R}{\leftarrow} \{0,1\}^S$, and $G^{'}(k) = G(k_1)$. $G(k_1)$ is a secure PRG, so $G^{'}(k)$ is.

   $G^{'}(k) = reserver(G(k))$ is a ***secure*** PRG. After performing the reserver() operation, its output is still "random" and is "indistinguishable" from a true random.

2. First give the advantage formula:

$$Adv_{PRG}[A, G^{'}] = \left|Pr_{k_1,k_2 \overset{R}{\leftarrow} K}\left[A\left(G^{'}(k_1, k_2)\right) = 1\right] - Pr_{r \overset{R}{\leftarrow} \{0,1\}^n}[A(r) = 1]\right|$$

$$= \left|Pr_{k_1,k_2 \overset{R}{\leftarrow} K}[A(G(k_1) \wedge G(k_2)) = 1] - Pr_{r \overset{R}{\leftarrow} \{0,1\}^n}[A(r) = 1]\right|$$

   For a random string r in $\{0,1\}^n$, we have

$$\Pr[\mathrm{A(r)} = 1] = \frac{1}{2}$$

   For a secure PRG, $G{:}K \rightarrow \{0, 1\}^n$, we also have

$$\Pr[\mathrm{A(G(k))} = 1] = \frac{1}{2}$$

   Only when the two corresponding binary bits are both 1, the result bit is 1, thus

$$Pr\,[A(G(k_1) \wedge G(k_2)) = 1] = \frac{1}{2} * \frac{1}{2} = \frac{1}{4}$$

   Finally, we get

$$Adv_{PRG}[A, G^{'}] = \left|\frac{1}{4} - \frac{1}{2}\right| = \frac{1}{4} = 0.25$$

3. $E^{'}((k,k'),m) = E(k,m)||E(k^{'},m)$ is ***semantically secure***. Because (E, D) is a one-time semantically secure cipher and k, k' are different random key in K, for every $m_0, m_1 \in M$, the semantics security advantage of all efficient A against this E' is still negligible.

   $E^{'}(k,m) = E(0^n,m)$ is ***not semantically secure***. Let $m_0 = 0^n$, $m_1 = 1^n$, an adversary A can ask for the encryption of m_0 and m_1, and because the key is 0^n, A can easily distinguish $EXP(0)$ from $EXP(1)$.

$E^{'}(k,m) = E(k,m)||k$ is ***not semantically secure***. Because every CT contains the secret key k. For every $m_0, m_1 \in M$, adversary A can get the secret key k from the CT and use this key to decrypt the CT.

$E^{'}(k,m) = E(k,m)||LSB(m)$ is ***not semantically secure.*** Let the LSB of m_0 be 0, the LSB of m_1 be 1, and the rest are the same. An adversary A can ask for the encryption of m_0,m_1 and can easily distinguish $EXP(0)$ from $EXP(1)$.

4. The ASCII of "attack at dawn": '61747461636b206174206461776e', let it be PT_1.
   The ASCII of "attack at dusk": '61747461636b206174206475736b', let it be PT_2.
   We have the CT_1 of PT_1

   $$CT_1 = \text{'6c73d5240a948c86981bc294814d'}$$

   Thus,

   $$CT_2 = OTP(k,PT_2) = OTP(CT_1 \oplus PT_1, PT_2) = CT_1 \oplus PT_1 \oplus PT_2$$
   $$= \text{'6c73d5240a948c86981bc2808548'}$$