1. 不是。

反例如下：

假设 $|M|=|K|=2$，$M=\{aa,ab\}$，$K=\{2,3\}$。在集合 K 中随机选取密钥 k，设集合 M 上的明文的分布为 $\Pr(M=aa)=0.6$，$\Pr(M=ab)=0.4$，则由此可知密文空间为 $C=\{cc,dd,cd,de\}$，所以 $\forall c\in C$，$\Pr(C=c)>0$。

显然，$\Pr(M=aa\,|\,C=cd)=\dfrac{\Pr(M=aa,C=cd)}{\Pr(C=cd)}=0$，然而 $\Pr(M=aa)=0.6\neq 0$。

所以 $\exists aa\in M\wedge cd\in C$，使得 $\Pr(M=aa\,|\,C=cd)\neq\Pr(M=aa)$。

由 perfectly secret 的定义可知，该密码体制非 perfectly secret。

2. 否。

我们可以构造出一个 G，使得 G' 不是伪随机发生器。假设 H 是伪随机发生器，其满足

$$\begin{cases}|H(s)|>|s| & (1)\\ \left|\Pr\left[D(H(s)=1)\right]-\Pr\left[D(r)=1\right]\right|\le negl(n) & (2)\end{cases}$$

构造 $G(s)=\begin{cases}H(s) & \text{当s的后半部分不全为0时}\\ O^{|H(s)|} & \text{当s的后半部分全部为0时}\end{cases}$

下面证明所构造的 G 是一个伪随机发生器。

显然，$|G(s)|=|H(s)|>|s|$，并且有

$$\begin{aligned}&\left|\Pr\left[D(G(s))=1\right]-\Pr\left[D(G(r))=1\right]\right|\\ &\le\left|\Pr\left[D(G(s))=1\right]-\Pr\left[D(H(s))=1\right]\right|+\left|\Pr\left[D(H(s))=1\right]-\Pr\left[D(G(r))=1\right]\right|\end{aligned}$$

根据（2）式可知，$\left|\Pr\left[D(H(s)=1)\right]-\Pr\left[D(r)=1\right]\right|\le negl(n)$，所以要证明 G 是一个伪随机发生器，只需要证明 $\left|\Pr\left[D(G(s))=1\right]-\Pr\left[D(H(s))=1\right]\right|\le negl(n)$ 即可，而该式显然成立，因为

$$
\begin{aligned}
&\left|\Pr\left[D\left(G\left(s\right)\right)=1\right]-\Pr\left[D\left(H\left(s\right)\right)=1\right]\right| \\
&=\left|\Pr\left[D\left(O^{|H(s)|}\right)=1\right]-\Pr\left[D\left(H\left(s\right)\right)=1\right]\right| \quad \text{当s的后半部分为0时} \\
&=\left|1-\Pr\left[D\left(H\left(s\right)\right)=1\right]\right| \\
&=\Pr\left[D\left(H\left(s\right)\right)=0\right]=\Pr\left[\text{s的后半部分为0}\right] \\
&\le \frac{1}{2^{\left|\frac{s}{2}\right|}} \le negl\left(n\right)
\end{aligned}
$$

其中，s 是在 $\{0,1\}^{s}$ 上随机选取的。

所以，综上可以证明 G 是一个伪随机发生器。

显然，$G'(s) \triangleq G\left(s0^{|s|}\right)=O^{|H(s)|}$，即 G' 生成的是一个确定的比特串，从而 G' 不是一个伪随机发生器。

3. 程序代码如下所示：

```
#include<iostream>
#include<string>
#include "../libcryptopp/include/randpool.h"

using namespace std;
using namespace CryptoPP;

#ifdef _DEBUG
#pragma comment(lib, "../libcryptopp/lib/Debug/cryptlib.lib")
#else
#pragma comment(lib, "../libcryptopp/lib/Release/cryptlib.lib")
#endif

int main() {
    string message, seed, key;
    cout << "Please input the seed:" << endl;
    getline(cin, seed);
    int seed_len = seed.length();
    byte *pSeed = (byte *)seed.c_str();
    cout << "Please imput the message:" << endl;
    getline(cin, message);
    int message_len = message.length();
    cout << "Input a primary key:" << endl;
    cout << "The key length is " << message_len << endl;
```

```
    getline(cin, key);
    byte *pKey = (byte *)key.c_str();
    RandomPool otp;
    otp.IncorporateEntropy(pSeed, seed_len);
    otp.GenerateBlock(pKey, message_len);
    cout << "The plaintext is:" << endl << message << endl;
    cout << "The primary key is:" << endl << pKey << endl;
    cout << "The ciphertext is:" << endl;
    for (int i = 0; i < message_len; i++) {
        message[i] = message[i] ^ pKey[i];
        cout << message[i];
    }
    cout << endl;
    cout << "Decode the ciphertext:" << endl;
    for (int i = 0; i < message_len; i++) {
        message[i] = message[i] ^ pKey[i];
        cout << message[i];
    }
    cout << endl;
    system("pause");
    return 0;
}
```

利用该程序对字符串 hello world 进行加密和解密，结果如下图 1 所示。

```
Please input the seed:
123456789
Please input the message:
hello world
Input a primary key:
The key length is 11
12453698721
The plaintext is:
hello world
The primary key is:
h\y-HU彧艉E
The ciphertext is:
 9Ε}'uą ?!
Decode the ciphertext:
hello world
请按任意键继续. . .
```

图 1

4. 假设攻击者 C 以等概率加密 m_0 和 m_1，分别用 0 和 1 表示加密 m_0 和 m_1，所以有

$$\Pr(C=0)=\Pr(C=1)=\frac{1}{2}$$

$Definition\ 3.8 \Rightarrow Definition\ 3.9$:

$$\Pr\left(PrivK_{\mathrm{A},\Pi}^{eav}(n)=1\right)=\Pr(A=0\,\&\,C=0)+\Pr(A=1\,\&\,C=1)$$
$$=\Pr(A=0\mid C=0)\Pr(C=0)+\Pr(A=1\mid C=1)\Pr(C=1)$$
$$=\frac{1}{2}\left(\Pr(A=0\mid C=0)+\Pr(A=1\mid C=1)\right)$$
$$=\frac{1}{2}\left(1-\Pr(A=1\mid C=0)+\Pr(A=1\mid C=1)\right)$$
$$=\frac{1}{2}+\frac{1}{2}\left(\Pr(A=1\mid C=1)-\Pr(A=1\mid C=0)\right)$$

由 Definition 3.8 可知，上式得结果$\leq \frac{1}{2}+negl(n)$，即

$$\Pr(A=1\mid C=1)-\Pr(A=1\mid C=0)\leq negl(n) \quad (1)$$

同时，$\Pr\left(PrivK_{\mathrm{A},\Pi}^{eav}(n)=0\right)\leq \frac{1}{2}+negl(n)$

利用跟上述过程相类似的方法，可得 $\Pr(A=1\mid C=0)-\Pr(A=1\mid C=1)\leq negl(n)$ (2)

由上述（1）和（2）两式，可得 $\left|\Pr(A=1\mid C=1)-\Pr(A=1\mid C=0)\right|\leq negl(n)$

因为

$$\Pr\left[out_A\left(PrivK_{\mathrm{A},\Pi}^{eva}(n,0)\right)=1\right]=\Pr(A=1\mid C=0)$$

$$\Pr\left[out_A\left(PrivK_{\mathrm{A},\Pi}^{eva}(n,1)\right)=1\right]=\Pr(A=1\mid C=1)$$

所以该式即等价于 Definition 3.9。

$Definition\ 3.9 \Rightarrow Definition\ 3.8$：

逆推上述过程即可。

综上，可以证明两个定义等价，即 $Definition\ 3.9 \Leftrightarrow Definition\ 3.8$

5. 作业参考了助教的答案和周宇（MG1533095）的作业。