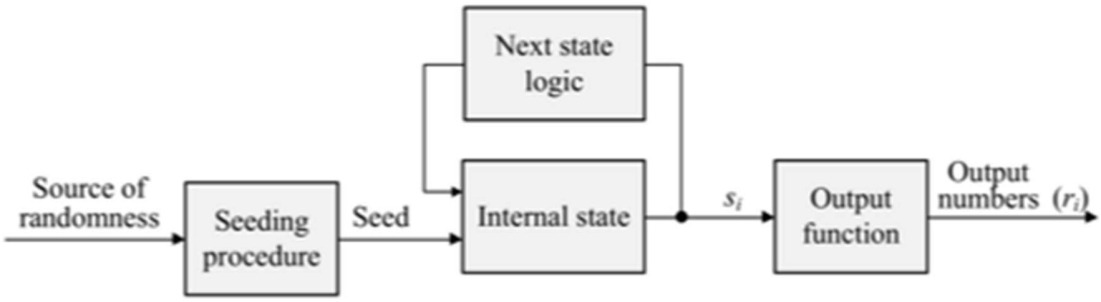
请你利用现有的知识设计一款随机数发生器，并说明原理。

随机数发生器可分为确定性随机数发生器和真随机数发生器。由于真随机数发生器往往涉及到硬件电子器件的噪声等知识，本人没有此方面的背景，故决定设计一个确定性随机数发生器。

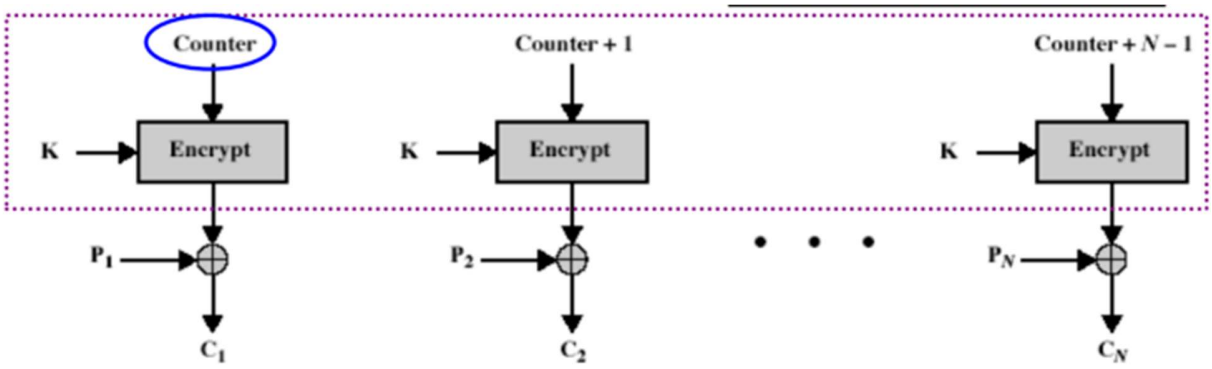
确定性随机数发生器的一般结构如下：



我的看法是，按部就班地对我设计的随机数发生器的各个部分进行说明就可以了。

在 ppt 中，我们知道，任何安全的分组密码都可以构造 DRNG，并举了例子，计数器模式下的 AES 密码使用随机 key 生成周期为 2^{128} 的序列。同时上课时老师也提到，流密码和真随机数发生器可以看作是等价的。而事实上计数器模式下的 AES 密码也可以被看作流密码。

首先我们来看看计数器下 AES 密码是如何工作的：



根据上图，我们可以看到，这个加密模式将明文分为 N 块，每块都根据 counter 和密钥的值进行加密得到密文。这个过程其实便可以作为随机数发生器内部状态迭代的模块。其中迭代需要一段明文，还需要密钥和初始的 counter 值，而这两个值来自于该随机数生成器的生成随机种子部分。

接下来我们讨论生成随机数种子的模块，这个模块需要有一定的随机性来源。这个需要熵的部分我认为可以采用系统的熵源，即可以采用 linux 系统中内核启动时池缓冲区的未初始化 内容、ns 分辨率表示的启动时间、输入事件、磁盘访问定时以及在 boot 时保存的熵。

最后就是可选的输出函数，其作用是将 DRNG 输出与其内部状态隔离。这个也就是使得敌手无法从外部观察到内部状态。这个函数可以采用 SHA3 函数，因为知道 SHA3 函数的输出将无法知道其输入。

该随机数发生器的草图如下所示：


明文、
counter++
生成随机种子：
密钥和counter
AES加密算法
输出函数
hash