算法思路：

根据密码学课程学习的知识，我们可以知道长度扩展攻击是指针对某些允许包含额外信息的加密散列函数的攻击手段。对于满足以下条件的散列函数，都可以作为攻击对象：

① 加密前将待加密的明文按一定规则填充到固定长度（例如 512 或 1024 比特）的倍数。

② 按照该固定长度，将明文分块加密，并用前一个块的加密结果，作为下一块加密的初始向量（Initial Vector）。

所以根据上面的思路，我大致的描述过程如下：

随机生成一个消息（secret），用 SM3 函数算出哈希值（hash1）生成一个附加消息（append）。首先用 hash1 推算出这一次加密结束后 8 个向量的值，再以它们作为初始向量，去加密 append，得到另一个 hash 值(result) 计算 secret + padding + append 的 hash 值（result2），如果攻击成功，hash2 应该和 hash3 相等。

运行指导：

需要使用 sm3.h 库，需要提前下载安装。

输出结果：