针对本讲介绍的 Enigma 密码机，请回答以下问题：

1.接线板、轮子、反射器分别起的作用？

答：接线板：增加密钥量；轮子：增加加解算法复杂度；反射器：使得加解密算法相同。

2.Enigma 密码机的明文、密文、加密算法、解密算法、密钥分别是什么？

答：明文：有意义的文字；密文：无意义的乱文字；加密算法：由接线板、轮子、反射器三部分构成；解密算法：同加密算法；密钥：由接线板连线、轮子排序、轮子位置决定。

3. 为什么需要每日密钥、通信密钥，而不是双方协商同一密钥后就一直使用？给我们的启示是什么？

答：每日密钥，顾名思义，就是每天使用的密钥，来自于机要部门下发的“密码本”，也称为密钥加密密钥，是用来加密通信密钥的，保证通信密钥的安全传送到对方；通信密钥，也称会话密钥，针对一个会话（譬如任务）而生成的密钥，用来加密通信信息，一旦会话结束，会话密钥就可舍弃。

密钥分为每日密钥、通信(会话)密钥，这大大提高 Enigma 密码机应用的安全性，因为长时间使用同一密钥，由此产生大量密文，有利于敌手破译，还有可能增加泄露密钥风险(譬如内奸等)。

启示：密码系统的安全性来自密钥的安全性；（如密码设备被敌手得到(可能性大)，加解密算法就被敌手掌握了）密钥需要定期更新；（密钥按需要动态变化的，如新任务开始就要使用新的密钥）密钥分发在实际应用中是件重要和困难的事。（如密码本的管理）

4.在实际应用中，为什么密码本是核心？得到敌手的密码本就能够破译其密文了？给我们的启示是什么？

答：因为密码算法很难不能被敌手得到，譬如通过战争的缴获、内奸、密码专家分析等等，而密码本易于控制，且不同使用对象密码本不同，所以，密码本是核心，敌手得到密码本就能破译密码。

启示：密码系统的安全性并不取决对密码算法的保密，而是由密钥的保密性决定的。

5.如果需要增加 Enigma 密码机的安全强度，通常需要怎么做？为什么？

答：增加轮子。因为轮子决定了 Enigma 密码机加解密算法的复杂程度，轮子越多，算法复杂度就越高，但处理效率也变低。接线板的连线所提供的密钥量足以应付当时的穷举攻击，但不能增加算法的复杂度。反射器不提供密钥变化量，也不提供算法的复杂度，只是实现加解密算法相同。

假设你使用的计算机具有如下能力:

1.每台计算机每秒可尝试 1 百万(10^6)个密钥。

2. 共有 100 万(10^6)台计算机参与并行使用。

那么，遍历 64 比特、112 比特、128 比特的密钥分别大约需要多少年？(要求简要过程)　　注：　$2^{10}\approx10^3$

1 年=356*24*3600≈3*10^7 秒

1 年遍历密钥个数≈3*10^{19}

$2^{64}\approx10^{19.2}$

$2^{112}\approx10^{33.6}$

$2^{128}\approx10^{38.4}$

年数≈1

年数≈10^{13}

年数≈10^{18}

答：大约分别为 1 年，10^{13} 年，10^{18} 年。