1. 接线板、轮子、反射器分别起的作用?

1) 接线板：可以看作一种单表代换，用于增加密钥量。接线板上的每条插线负责连接一对字母。当两个字母相互连接后，它们就会被互换。
2) 轮子：可以看作一种多表代换，用于增加加解密算法的复杂度。每个轮子上有 26 个字母的任意组合。Enigma 密码机中通常设置多个不同转速的轮子，每次按键时，最快速的轮子会转动一定角度，当快速轮子转动一圈时，相邻的慢速轮子就会转动一定角度。
3) 反射器：反射器和转子一样，把某一个字母连在另一个字母上，但是它并不转动，也并不增加可以使用的编码数目。当一个键被按下时，信号首先通过三个转子，然后经过反射器再回到三个转子，最后到达显示器上。假设 A 键被按下时亮的是 D 灯泡，那么如果这时按的是 D 键，信号最后会到达 A 灯泡。换句话说，在这种设计可以让恩格玛机既可作为加密机也可作为解密机，使得加解密算法相同。

2. 接线板取 10 对连线，只能安装三个轮子，而使用者有 6 个轮子可供使用，其密钥量是什么?

10 对连线可配置的连线方案共有：$C_{26}^{20} \times 19 \times 17 \times \ldots \times 1 = 150738274937250 \approx 1.5 \times 10^{14}$

3 个轮子可以将密钥量扩大为$26 \times 26 \times 26 = 17576$

6 个轮子选取 3 个轮子为$C_6^3 = 6 \times 5 \times 4 = 120$

3 个轮子的不同排序，即那个是快轮，中轮，慢轮，共有 3!=6 种。

相乘得到密钥量约为10^{21}。

3. 每日密钥和通信密钥分别来自哪里或如何生成的，二者之间关系及密钥这么划分的好处?

1) 每日密钥：顾名思义，每日密钥在一天内不会改变。它用于加密通信密钥。操作员每个月都会收到一本新的密码本，指定每月中每天所使用的密钥。具体包括：1）三个轮子的排列顺序；2）三个轮子的位置；3）插线板的位置
2) 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(通信完成)，会话密钥就可舍弃。
3) 关系：每日密钥用于加密通信密钥，通信密钥用于加密消息。
4) 好处：由于对加密算法的保密是困难的，因此密码算法的安全性取决于密钥的安全性。设置每日密钥的好处在于让当天的密文只与当天的密钥相关，如果每日密钥被窃取，敌手也只能获得当天的情报。类似的，通信密钥只与单次的通信消息相关，窃取单个通信密钥只能解密一个会话消息。如果通信双方只协商一个密钥，那么如果该密钥被窃取，敌手可以获得由此密钥加密的全部消息。因此，通过对密钥的多级划分有助于提高加密系统的安全性。

4. 如果需要增加 Enigma 密码机的安全强度，通常需要怎么做?

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，只是实现了加解密算法相同。

5. 如果截获 Enigma 产生的大量密文中，字母 H 一次没出现，那么能推测出明文是什么?（注：Enigma 的缺陷）

由于 Enigma 密码机的构造，无论接线板如何连线，轮子的旋转位置如何变化，输入的字母都不会被替换成该字母本身。因此可推测出明文都是 H，也断定这类密文用于干扰作用。

6. 查阅 Enigma 相关资料，从 Enigma 的兴衰过程，能带给我们哪些启示?（至少 5 点）

1. 科学技术的发展是密码学得以前进发展的基石 ；
2. 密码学的发展促进新科学技术的出现；

3. 实际需求是推动密码学前进的最大动力；
4. 密码编码和密码分析，两者既彼此对抗，有相互促进；
5. 在密码对抗中，人的因素是第一位的；
6. 密码系统的保密性只应建立在密钥的保密上；
7. 复合密码体制更有利于增强算法的安全性；
8. 破译需要过程，积累的过程，很难一蹴而就。同时，有时还需要些运气，如一些“意外”，“巧合”，譬如德国的邮递件恰好是周六到，德奸施密德等；
9. 操作者安全意识不强，极大降低密码系统的安全强度，譬如使用女友的缩写，天气预报等固定的格式作为通信密码；
10. 破译需要天才，譬如图灵，不是一般人能做到的；同时，破译工作也是一个工程，需要多方人才参与，需要大量人力物力的支撑；
11. 破译也促进新技术的发展，譬如“巨人”，就是后来的计算机雏形，破译的需求促使更高性能的计算机的出现；
12. 密码破译通常是数学问题，与数学关系更密切些。