应用密码学 第二次作业参考答案

题目 1：从具体的功能来看，在一般的密码系统中，密钥可以分为哪几类，并具体说明。

答：密钥可以分为四类：

（1）基本密钥(Base Key)：又称为初始密钥(Primary Key)或用户密钥(User Key)。它是由用户选定或由系统分配给用户的，可以在较长时间内(相对于会话密钥)由一对用户(例如密钥分配中心与某一用户之间，或者两个用户之间)所专用的密钥。在某种程度上，基本密钥还起到了标识用户的作用；

（2）会话密钥(Session Key)：也称为数据加密密钥，是在一次通信或数据交换中，用户之间所使用的密钥，它可由通信用户之间进行协商得到。它一般是动态地、仅在需要进行会话数据加密时产生，并在使用完毕后立即清除(或由用户双方进行预先约定)；会话密钥可以使大家不必很频繁地去更换基本密钥，而是通过密钥分配或者密钥协商的方法得到某次数据通信所使用的数据加密密钥这样就可以做到一次一密，从而大大提高通信的安全性，并方便密钥的管理；

（3）密钥加密密钥(Key Encrypting Key)：用来对传送的会话密钥或文件加密密钥进行加密时所采用的密钥，另外也可以称为二级密钥。密钥加密密钥所保护的对象是用来保护通信或文件数据的会话密钥或者文件加密密钥。在通信网中，一般在每个节点都分配有一个这类密钥。同时，为了安全，各节点的密钥加密密钥应互不相同。节点之间进行密钥协商时，应用各节点的密钥加密密钥加以完成；

（4）主密钥(Master Key)：对应于层次化密钥结构中的最上面一层，它是对密钥加密密钥进行加密的密钥，通常主密钥都受到了严格的保护。

题目 2：Diffie-Hellman 密钥交换算法：设 p 是素数，a 是 Z_p 的生成元，a 和 p 公开，两个用户 A 与 B 通信时，通过如下步骤协商密钥：

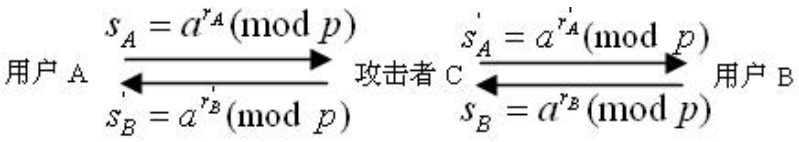
若 p=41，a=6，r_A=9，r_B 为学号尾号+10。例如尾号为“7”，则 r_B=17。根据协议回答下面问题（提示：用 Fermat 小定理和模重复平方减少计算量）：

（1）求 K’的值。

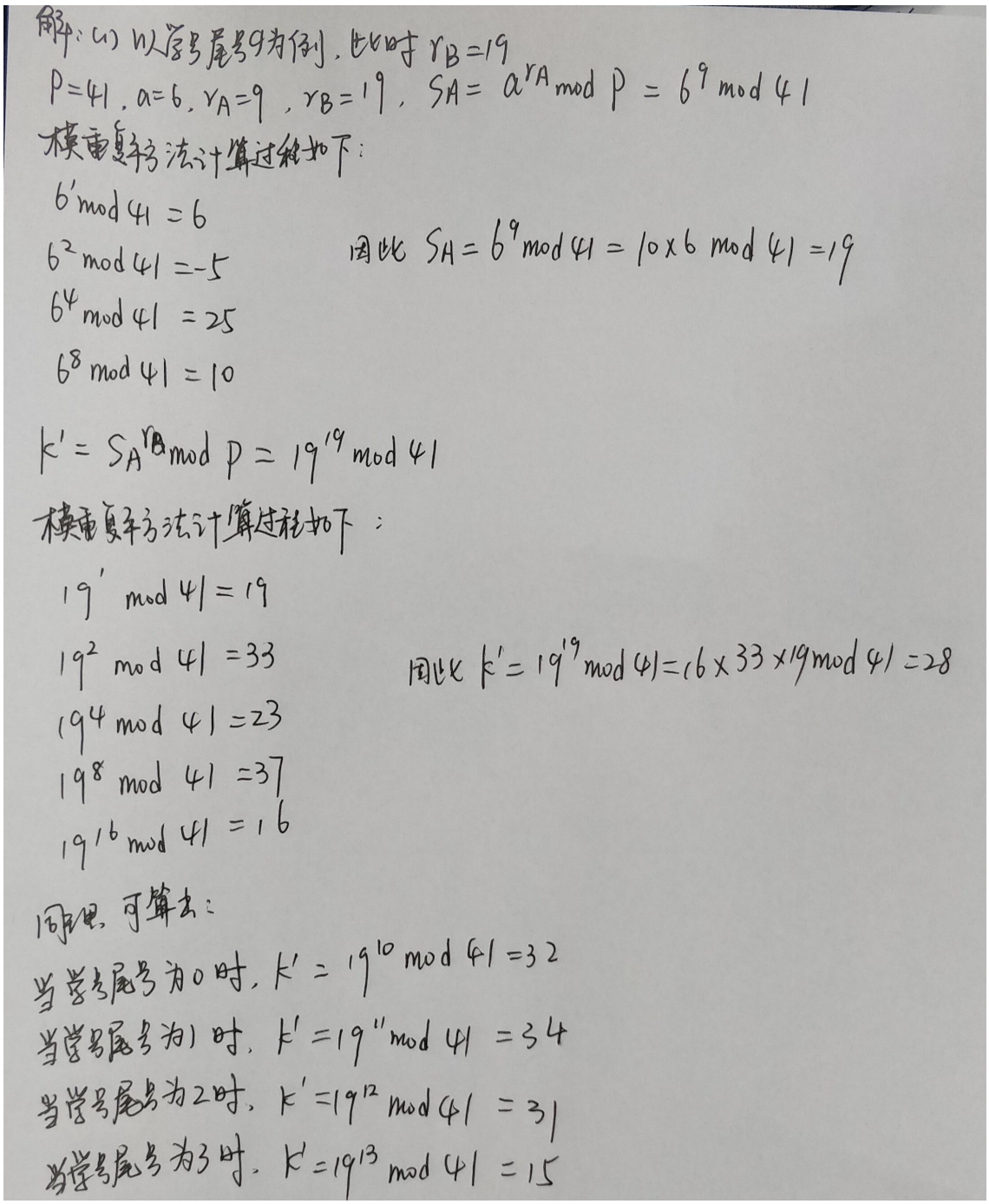
（2）实际应用中，参数 p 和 a 都很大，比如 p 接近 2^{2048}. 在计算安全的情

况下为参数 p 和 a 选取值，则参数 a，p，S_A，S_B 为什么可以在不安全信道上传输？

（3）对于 Diffie-Hellman 密钥交换协议，一个完整的中间人攻击过程如图。若攻击者 C 选择 $r_A'=r_B'=5$，计算 A 和 C 的共享密钥、B 和 C 的共享密钥的值。



解：



当学号尾号为4时，$k'=19^{14} \bmod 41 = 39$

当学号尾号为5时，$k'=19^{15} \bmod 41 = 5$

当学号尾号为6时，$k'=19^{16} \bmod 41 = 16$

当学号尾号为7时，$k'=19^{17} \bmod 41 = 17$

当学号尾号为8时，$k'=19^{18} \bmod 41 = 36$

当学号尾号为9时，$k'=19^{19} \bmod 41 = 28$

(2) Diffe-Hellman密钥交换协议的~~安全~~性基于Zp上的离散对数问题。~~如果只公~~开 a、P、S_A、S_B，而A、B分别保留 Y_A 和 Y_B，那么即使攻击者能够获得 S_A、S_B、a、P 也很难得到 Y_A、Y_B。同此参数 a、P、S_A S_B 可以在不安全信道上传输。

(3) A与C的共享密钥 $K_{AC}=a^{Y_A Y_B'} = 6^{9\times5} \bmod 41 = 6^5 \bmod 41 = 27$

B与C的共享密钥 $K_{BC}=a^{Y_A' Y_B} = 6^{5\times19} \bmod 41 = 6^{15} \bmod 41 = 3$

同理，可算出：

当学号尾号为0时，$K_{AC}=27$，$K_{BC}=6^{5\times10} \bmod 41 = 6^{10} \bmod 41 = 32$

当学号尾号为1时，$K_{AC}=27$，$K_{BC}=6^{5\times11} \bmod 41 = 6^{15} \bmod 41 = 3$

当学号尾号为2时，$K_{AC}=27$，$K_{BC}=6^{5\times12} \bmod 41 = 6^{20} \bmod 41 = 40$

当学号尾号为3时，$K_{AC}=27$，$K_{BC}=6^{5\times13} \bmod 41 = 6^{25} \bmod 41 = 14$

当学号尾号为4时，$K_{AC}=27$，$K_{BC}=6^{5\times14} \bmod 41 = 6^{30} \bmod 41 = 9$

当学号尾号为5时，$K_{AC}=27$，$K_{BC}=6^{5\times15} \bmod 41 = 6^{35} \bmod 41 = 38$

当学号尾号为6时，$K_{AC}=27$，$K_{BC}=6^{5\times16} \bmod 41 = 6^{40} \bmod 41 = 1$

当学号尾号为7时，$K_{AC}=27$，$K_{BC}=6^{5\times17} \bmod 41 = 6^{5} \bmod 41 = 27$

当学号尾号为8时，$K_{AC}=27$，$K_{BC}=6^{5\times18} \bmod 41 = 6^{10} \bmod 41 = 32$

当学号尾号为9时，$K_{AC}=27$，$K_{BC}=6^{5\times19} \bmod 41 = 6^{15} \bmod 41 = 3$