作业

----------可以采用 matlab，java，c，C++等）

1、 密码分析（单表代换）：

密文 1：

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZQWSFPAPPD
TSVPQUZWYMXUZUHSXEPYEPOPPZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

密文 2：

JXQCEFMPJASOQMDPQABCSTYSMGRQBTQOASKQAOUWCPQBDPMEEASIVMWPOQVJXQVQC
SORWBQKMMYVJQAOXQPVASBFPAOJCOARQHFQPCQSOQASBQAOXXAVCJVMGSABZASJATQV
JXQYSMGRQBTQGQTACSDPMEKMMYVASBDMPEARQBWOAJCMSQSAKRQVWVJMRQAPSAKM
WJJXCSTVXAJGQXAZQSMMFFMPJWSCJIJMQHFQPCQSOQCSBACRIRCDQGOOASVJWBIARRJXQ
FRAOQVCSJXQGMPRBASBRQAPSDPMEFQMFRQGQGCRRSQZQPEQQJCSMWRCDQJCEQLWVJK
IPQABCSTJXQCPKMMYVGQOASARVMBQZQRMFMWPASARIJCOARVYCRRVASBRQAPSXMGJMZ
CQGASBCSJQPFPQJJXQGMPRBAPMWSBWVCSBCDDQPQSJGAIVGQOASRQAPSJXQFAVJKIPQAB
CSTKMMYVCSJXCVGAIGQGMSJPQFQAJJXQECVJAYQVMMJXQPVASBOASKWCRBMSJXQCPAOXC
QZQEQSJV

2、 Playfair 密码编写；（或者，维吉尼亚密码编写，输入明文长度是任意的）

明文：量子通信保密技术的诞生和快速发展主要取决于以下两个因素：a、经典保密通信面临着三个难以彻底解决的关键问题，即密钥协商、身份识别和窃听检测，这些问题的有效解决需要新技术。b、在对新技术的探索中，人们发现了量子内在的安全特性及其可能的应用。

请写出你的密码机输出结果。

3、 转轮机编写（2 个转子）；

4、 DES 密码编写；

5、 AES 密码编写；

6、 利用扩展 Euclidean 算法计算下列的乘法逆：

(1) $17^{-1}\ mod\ 101$

(2) $357^{-1}\ mod\ 1234$

(3)计算 gcd(57,93)，并找出整数 s 和 t，使得 57s+93t=gcd(57,93)

(4) 求解下列同余方程组

$$X \equiv 12(\mathrm{mod}\ 25)$$
$$X \equiv 9(\mathrm{mod}\ 26)$$
$$X \equiv 23(\mathrm{mod}\ 27)$$

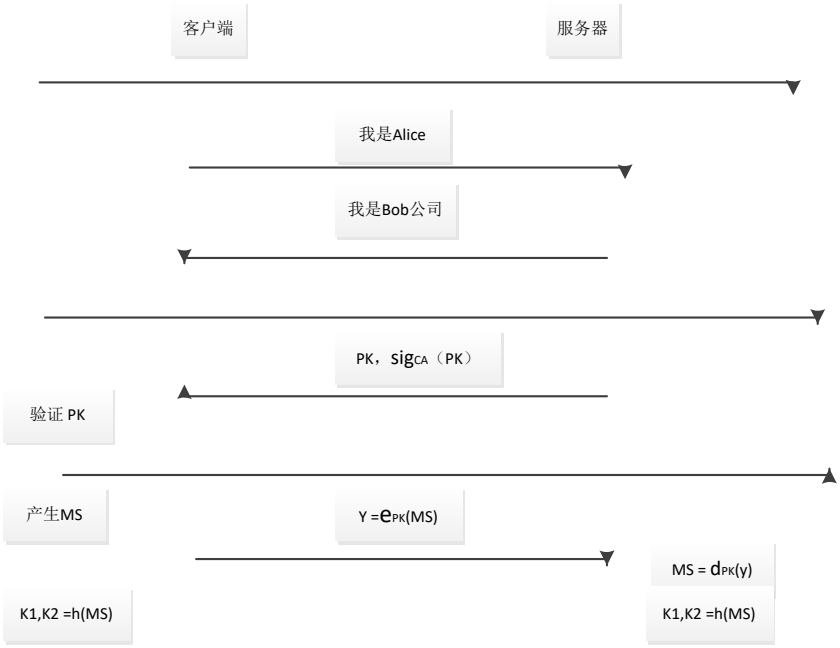
7、 建立一个 SSL 会话，如图 1。结合服务器到客户端的认证，但是没有客户端到服务器的认证。设客户端（Alice）准备使用信用卡从服务器（Bob 公司）购买一些东西。图 1 协议被用来派生密钥 K1 和 K2，这两个密钥将被用来加密和认证 Alice 的信用卡号以保证 SSL 会话的安全（当卡号被发送给 Bob 公司时）。简明地讨论下面几点关于 SSL 的问题：

（a） 为什么需要 Alice 的 Web 浏览器认证 Bob 的公钥？

（b） 在这个版本的协议中，Bob 没有办法建立阶段认证 Alice，这对 Bob 来说有问题

吗？为什么？

（c） 密钥 k1 和 k2 从一个由 Alice 提供的随机数 MS 派生出来，为什么随机数是由 Alice 生成而不是 Bob 公司？这种方法产生密钥 K1 和 K2 有潜在安全威胁吗？



8、说说你对信息安全的理解。