1.利用扩展Euclidean算法计算下列的乘法逆：

(1)

解：

进行欧几里得算法：

求解其逆元：

可见逆元为6。

(2)

解：

进行欧几里得算法：

求解其逆元：

可见逆元为-159。

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

解：

则问题转化为：

下求19模31时的乘法逆元。

进行欧几里得算法：

求解其逆元：

故s=-13，t=8。

(4)求解下列同余方程组

X≡12(mod25)

X≡9(mod26)

X≡23(mod27)

解：

式子的一般形式如下：

定义如下参数：

余数：。

模，亦即除数：例中。

模的最小公倍数为G：。

衍数（局部公倍数）：。

乘率由此式定义：。

下利用“大衍求一术”求解，先求衍数：

寻找模25时的乘法逆元，称为乘率：

同理可求得对应的衍数和乘法逆元：

表 1 参数表

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 702 | 13 |
|  | 675 | 25 |
|  | 650 | 14 |

25，26，27的最小公倍数

2.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：

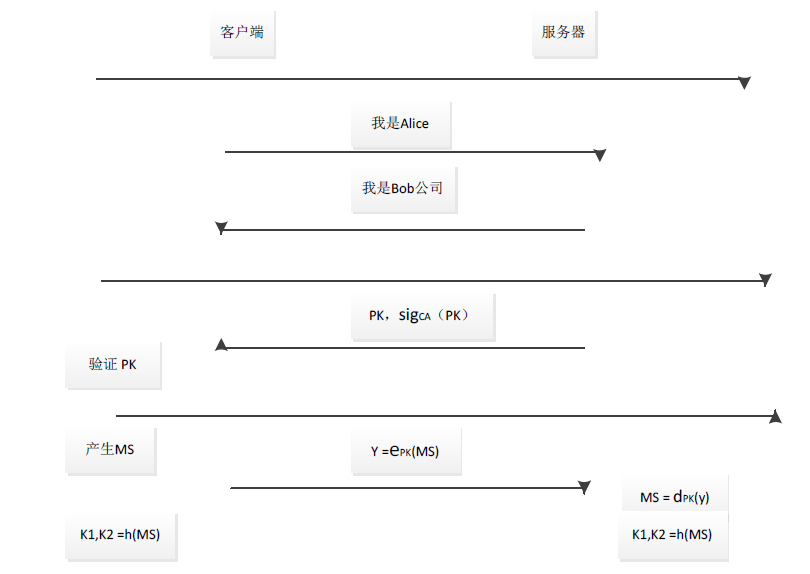
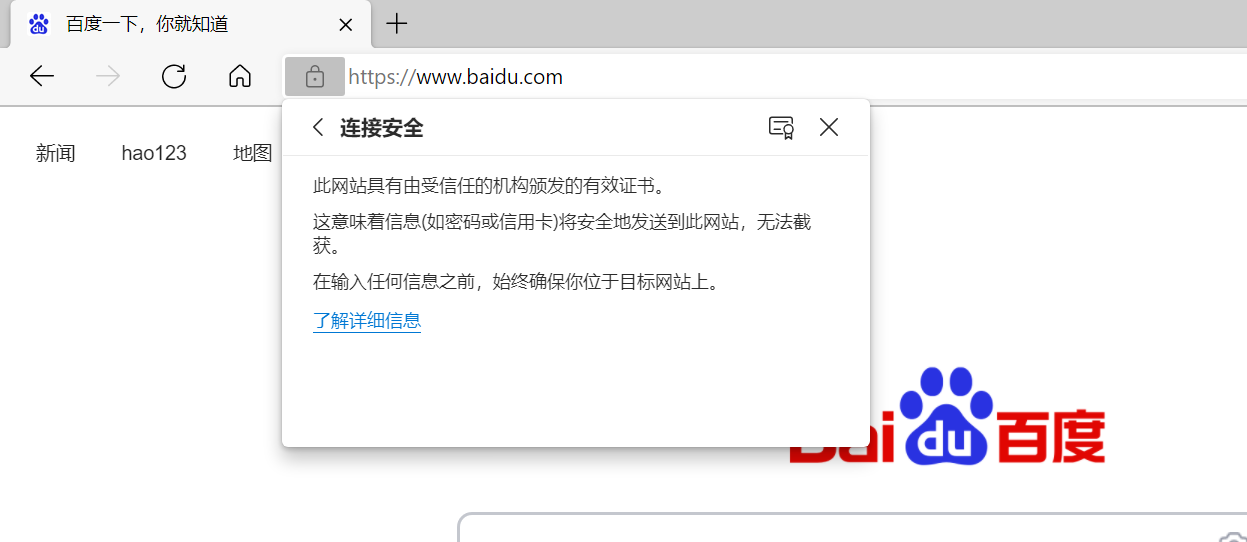


图 1

（a）为什么需要Alice的Web浏览器认证Bob的公钥？

答：

该认证为单向认证，用户需要确定服务器端的合法性，即该平台并非虚假网站，在日常使用中我们也可以看到，一些网页有这样的认证信息，其实http后带s的网页是受SSL协议保护的，数字证书中也存放有题目所说的公钥，而数字证书进一步保障了公钥的合法。



（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？

答：

没有问题。在该场景下Alice合法与否对Bob其实影响不大，不论是谁来购买对Bob来说都是一样的，但对Alice则涉及财产安全问题。

（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？

答：

这样更能保障不同用户的会话产生的随机数都相互独立，进一步确保用户的信息安全。

这样产生K1和K2可能涉及真随机与伪随机数的问题，计算机所产生的随机数多为伪随机，易被寻找到规律而破解。另外也难以避免中间人攻击。

3.说说你对信息安全的理解。

答：

信息安全的话题已是老生常谈。夏朝起，我国便有了完善的公文保密制度，到周朝，我国历史上最早的中央档案机构——天府成立，到如今，世界各国也都设有信息安全机构。其实，小到个人隐私的存储，大到国防安全，信息安全无处不在，可谓渗入了我们生活的方方面面。

近百年来，计算机技术飞速发展，创造了一个又一个奇迹，深刻改变着人类社会的面貌，但也带来了更高级的犯罪手段，对信息安全提出了新的挑战。随着互联网的发展，传统的网络边界变得模糊，融合、开放的背后暗藏黑客驰骋的天地，“网络安全”将成为重要研究领域，也或许将成为信息安全的“主战场”。

若经历过十多年前国内互联网的“蛮荒时代”，一定对“熊猫烧香”、“灰鸽子”等病毒有印象，卡巴斯基、瑞星等杀毒软件也是家中常备。另外，主打中文编程的“易语言”横空出世，低门槛、易上手、封装库极为丰富的它，被许多不法分子用来编写木马，盗取账号，以致“易语言”成为灰色产业代名词。虽近几年来监管力度加大，互联网的一些不良现象得到整顿，我们的日常上网已变得相对安全，但仍能不时见到用户数据泄露、电信诈骗事件……

仅切身体会便有如此之多，其他有关信息安全的例子更是不胜枚举。在我们看不见的角落，或许国外的黑客正不断地尝试攻击我们的网络，黑客与“红客”、破解与加密不断斗争，矛与盾的故事仍在信息安全领域不断上演。

可见，不管从技术上、制度上、还是群众意识上，信息安全都仍任重道远。而于外行的我们而言，也需学习一定相关知识，将信息安全理念、方法贯彻到自己的学习、工作中，为这一事业尽绵薄之力。