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：

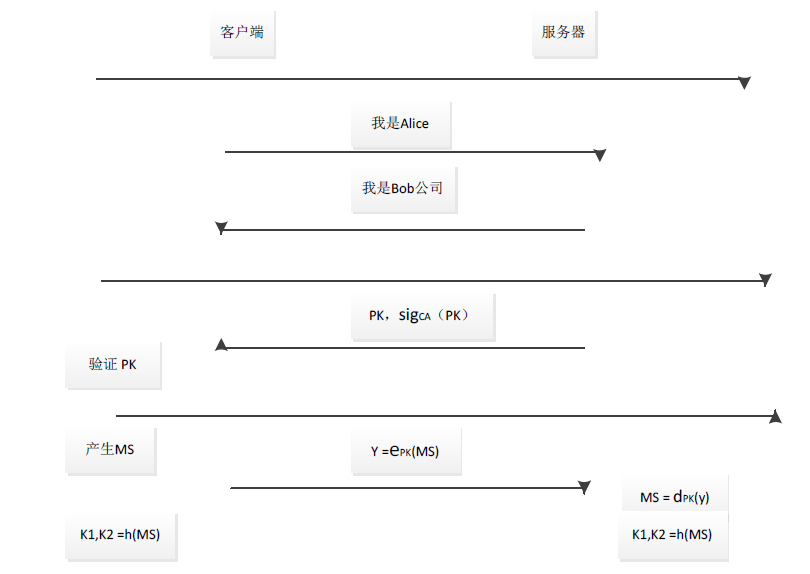
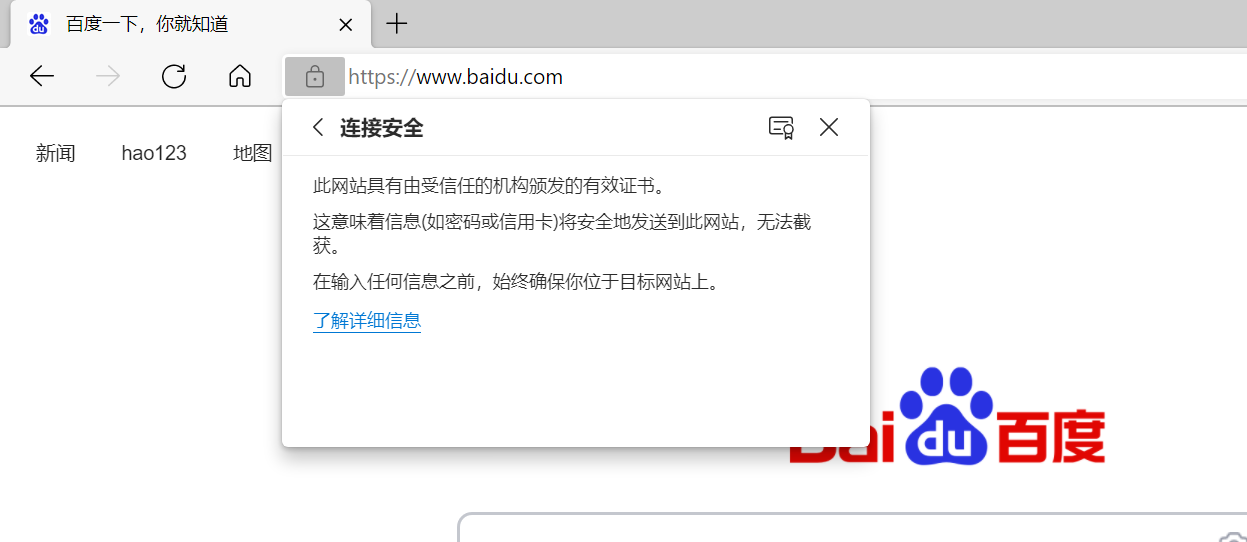


图 1

（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：

首先Alice收到了Bob的公钥，可以用该公钥对自己产生的随机数加密，Bob再用自己的私钥解密，保障了只有Bob能收到Alice的随机数。这种情境下，若无意外，Alice不会将此随机数发送给他人，而由Bob产生随机数，无法保障随机数仅有Alice知道。

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。另外也无法保障Bob不会将随机数泄露给他人。

3.说说你对信息安全的理解。

答：

信息安全