要证明两个密码体制S1=（P1，C1，K1，E1，D1）和S2=（P2，C2，K2，E2，D2）相等，需要证明：

（1）P1=P2

（2）C1=C2

（3）K1=K2，且分布相同

（4）E1=E2（{e1k}={e2k}）

（5）D1=D2

在实际的证明中，一般（1）和（2）显然成立，若（4）成立，由d与e的对应关系，则（5）也是成立的。所以，一般我们主要证明（3）和（4），其他一笔带过，或者省略。

2.20（a）

证明：已知S1=（P1，C1，K1，E1，D1），其中P1=C1=K1=26m1，K1等概分布，对于任意，

S2=（P2，C2，K2，E2，D2），其中P2=C2=K2=26m2，K2等概分布，对于任意，



要证明，即要证上述（3）（4）

假设=（P，C，K，E，D），

1.首先证明（4）：

∵ m2|m1，∴ 为整数，，则S是一个密钥长度为m1维吉尼亚密码，其中，

，

所以。

反之，对于任意

任取，计算出



则



所以，即

所以，

（4）得证。

2.证明（3）

由1的证明，若我们将S的密钥[k2,k1]和S1的密钥等同起来，那么K=K1，由于S1的密钥是随机均匀分布的，接下来只需证明S作为密钥长度是m1的维吉尼亚密码，它的密钥也是随机均匀分布的。

因为K1和K2随机均匀分布，且分布独立，我们有，



所以S也是随机均匀分布，则（3）得证。

所以S=S2×S1=S1。

（b）若，S=S2×S1，记，

S3=（P3，C3，K3，E3，D3），其中P3=C3=K3=26[m1,m2]，K3等概分布，



是一个密钥长度为的维吉尼亚密码，所以。

但S的密钥个数为|K|<=|K2|×|K1|=26m2×26m1=26m1+m2，而S3的密钥个数为|K3|=26[m1，m2]，，所以S和S3的密钥空间不相等，（3）不成立，所以二者不相等。