密码学第一次作业：

3.1



单射的条件是不同的明文必须映射到不同的密文，否则就无法唯一解密。

(a). b取值只影响mod26之后的余数，仍然是一对一的关系。

(b). a不能和26互质，就是指不能和26有公因数，假如有公因数，那么就会存在最小公倍数，即a\* x = 26 \* y，b对于mod结果可以不计（以为ap + b 和 aq + b中b的影响是一致的）。

假设a取13的时候，那13和26有最最小公倍数26，所以当 aq = ap+ n\*26 = 26 时，不同的明文映射到同一密文，即2和0被映射到同一密文时，单射性破坏。

(c). a能取除了偶数和13的倍数之外的其他数。

3.3



根据英文字母出现频率最高的两个字母是E和T，推测出 B – E，U – T。

根据仿射凯撒密码的公式，*B*=(*a*⋅*E*+*b*)mod26转换成数字1=(*a*⋅4+*b*)mod26

*U*=(*a*⋅*T*+*b*)mod26转换为数字：20=(*a*⋅19+*b*)mod26，最后求的a=3，b=15

 3.8



对应的例子是“it was disclosed yesterday that several informal butdirect contacts have been made with political representatives of the viet cong in moscow”

3.14



1. **将明文转换为数字**（a=0, b=1, ..., z=25）:

m e e t m e a t t h e u s u a l p l a c e a t t h e n r a t h e r t h a n e i g h t o c l o c k

12 4 4 19 12 4 0 19 19 7 4 20 18 20 0 11 15 11 0 2 4 0 19 19 7 4 13 17 0 19 7 4 17 19 0 13 4 8 14 17 11 14 2 10 14 18 7 14 2 11 14 2 10 14 18 7 14 2

1. **将数字分为两组进行矩阵乘法**:
	* 每两个字母为一组，与密钥矩阵相乘后取模26。
2. **计算示例**:
	* 第一组: (12​4​)

(12​4​)(95​47​)=((12×9+4×5)mod26​(12×4+4×7)mod26​)=(128mod26​64mod26​)=(24​12​)

对应字母: "Y" 和 "M"

* + 第二组: (4​19​)

(4​19​)(95​47​)=((4×9+19×5)mod26​(4×4+19×7)mod26​)=(131mod26​149mod26​)=(1​1​)

对应字母: "B" 和 "B"

* + 重复上述步骤直到所有组加密完成。
1. **密文结果**:

YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS YMXS

**3.14 (b) Hill 密码解密**

**密钥矩阵**:

*K*=(95​47​)

**逆矩阵计算**:

1. **计算行列式**:

det(*K*)=(9×7−4×5)=63−20=43≡17mod26

1. **求行列式的逆元**:

17−1mod26=23(因为 17×23≡1mod26)

1. **计算伴随矩阵**:

adj(*K*)=(7−5​−49​)mod26=(721​229​)

1. **计算逆矩阵**:

*K*−1=23×(721​229​)mod26=((23×7)mod26(23×21)mod26​(23×22)mod26(23×9)mod26​)=(161mod26483mod26​506mod26207mod26​)=(521​41​)

**解密过程**:

1. **将密文转换为数字**。
2. **将数字分为两组与逆矩阵相乘**:
	* 每两个字母为一组，与逆矩阵相乘后取模26。
3. **计算示例**:
	* 第一组密文 "Y" 和 "M" 对应数字 24 和 12:

(24​12​)(521​41​)=((24×5+12×21)mod26​(24×4+12×1)mod26​)=(12​4​)

对应明文: "m" 和 "e"

* + 重复上述步骤直到所有组解密完成。
1. **恢复明文**:

meet me at the usual place at then rather than eight oclock

**最终答案**

(a) 加密后的密文为:

**YMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXSYMXS**

(b) 解密时使用的逆矩阵为:

(5 4)

(21 ​1​)

 3.18





3.20



(a) 加密后的密文为:**BEOKORGZAZYG**

(b) 密钥为:**ZEWDBDNMWVVC**