1.a. $49 = 7 \times 7 = 7^2$

$256 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^8$

Because 49 and 256 share no common factors, $\gcd(49, 256) = 1$

$\therefore$ 49 is an element of $\mathbb{Z}_{256}^*$

b. Tabular form of extended Euclidean algorithm:

q	d	x	y
	256	1	0
5	49	0	1
4	11	1	-5
2	5	-4	21
5	1	9	-47

$q = \lfloor u/v \rfloor$

Solving for $Nx + ay = \gcd(a, N) = 1$:

$256 \cdot 9 + 49 \cdot (-47) \stackrel{?}{=} 1$

$2304 - 2303 = 1$ ✓

in $\mathbb{Z}_{256}$: $-47 \longrightarrow \boxed{209}$

2. Ciphertext: LMNYBSOZWGN

Plaintext: IL...

Recall: affine cipher

$e_k(x): P \mapsto C$

$e_k(x) = ax + b$

a.

Two letters of plaintext are known (or we can say two "points" on a line)

Solve a system of equations (in $\mathbb{Z}_{26}$):

$I = 8 \quad L = 11$

$M = 12$

$11 = 8a + b$

$12 = 11a + b$

$\downarrow$

$1 = 3a$

plug into one eq: $11 = 8 \cdot 9 + b$

$11 = 20 + b \rightarrow b = 17$

Find the inverse of 3 in $\mathbb{Z}_{26}$:

$a = 9$

$\boxed{e_k(x) = 9x + 17}$

b. Find corresponding $d_k(y)$

Recall: $d_k(y) = a'y + b'$
where $a'a = 1$, $b' = -a'b$

a' = multiplicative inverse of a in $e_k(x) = ax + b$

$a' = 3$

$b' = -3 \cdot 17 = 1$

$d_k(y) = 3y + 1$

Plug in rest of the ciphertext for y to recover plaintext: (math not shown)

we should recover the plaintext: $\boxed{\text{ILOVECRYPTO}}$

3. $M1 = \begin{bmatrix} 9 & 2 \\ 13 & 3 \end{bmatrix}$

a. Find the determinant in $\mathbb{Z}_{26}$

$9 \cdot 3 - 13 \cdot 2 \pmod{26} = \boxed{1}$

Find the inverse of M1 in $\mathbb{Z}_{26}$

$M1^{-1} = \cancel{\frac{1}{det}} \cdot (\text{adjugate of } M1) = \boxed{\begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix}}$

check: $M1^{-1} \cdot M1 \bmod 26 = \begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix} \cdot \begin{bmatrix} 9 & 2 \\ 13 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

b. Ciphertext: TZRUOOEZBW, block size = 2

Decryption w/ Hill cipher: $d_k(y) = M1^{-1} \cdot y$; $y, d_k(y)$ column vectors

TZ: $\begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 25 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \rightarrow$ HE

RU: $\begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 20 \end{bmatrix} = \begin{bmatrix} 11 \\ 11 \end{bmatrix} \rightarrow$ LL

OO: $\begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix} \begin{bmatrix} 14 \\ 14 \end{bmatrix} = \begin{bmatrix} 14 \\ 22 \end{bmatrix} \rightarrow$ OW

EZ: $\begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 25 \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix} \rightarrow$ OR

BW: $\begin{bmatrix} 3 & 24 \\ 13 & 9 \end{bmatrix} \begin{bmatrix} 1 \\ 22 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix} \rightarrow$ LD

The recovered plaintext reads: $\boxed{\text{HELLOWORLD}}$

4. $MM = \begin{bmatrix} 3 & 7 & 8 \\ 15 & 4 & 23 \\ 7 & 0 & 8 \end{bmatrix}$

Find the determinant in $\mathbb{Z}_{26}$:

$$\det(MM) = 3\cdot\det\left(\begin{bmatrix} 4 & 23 \\ 0 & 8 \end{bmatrix}\right) - 7\cdot\det\left(\begin{bmatrix} 15 & 23 \\ 7 & 8 \end{bmatrix}\right) + 8\cdot\det\left(\begin{bmatrix} 15 & 4 \\ 7 & 0 \end{bmatrix}\right) \bmod 26$$

$$= 3\cdot(4\cdot 8 - 0\cdot 23) - 7\cdot(15\cdot 8 - 7\cdot 23) + 8\cdot(15\cdot 0 - 7\cdot 4) \bmod 26$$

$$= 159 \bmod 26 = \boxed{3}$$

Find the inverse in $\mathbb{Z}_{26}$:

$$MM^{-1} = \frac{1}{\det}\cdot(\text{adjugate of } MM)$$

Note: $\frac{1}{\det} = \det^{-1}$

This should be in $\mathbb{Z}_{26}$!

$3^{-1} \bmod 26 = 9$ (from #2)

$\text{adj}(MM) = C^T$

What is C? $\rightarrow$ matrix of cofactors!

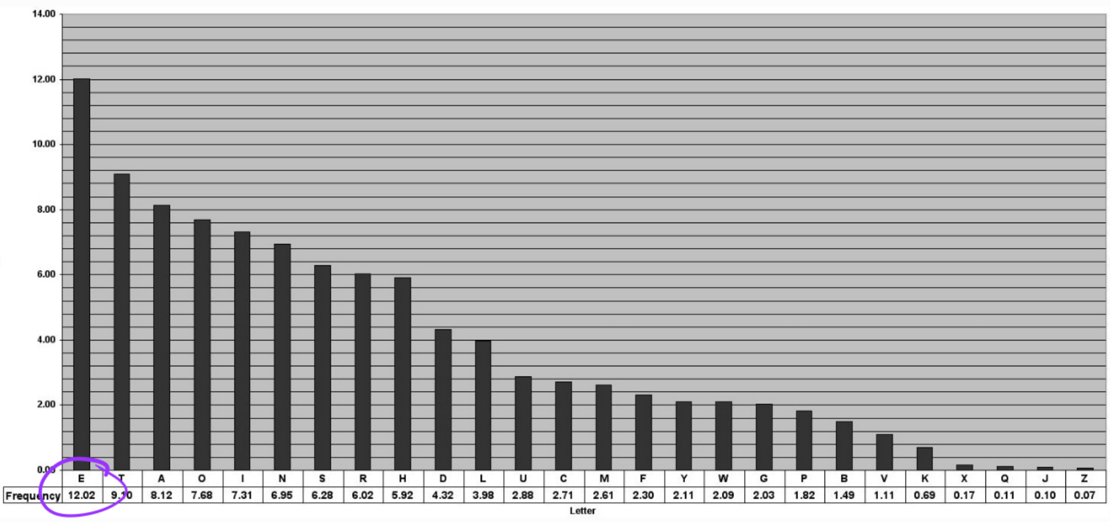
$$\text{adj}(MM) = \begin{bmatrix} \det\begin{bmatrix} 4 & 23 \\ 0 & 8 \end{bmatrix} & -\det\begin{bmatrix} 15 & 23 \\ 7 & 8 \end{bmatrix} & \det\begin{bmatrix} 15 & 4 \\ 7 & 0 \end{bmatrix} \\ -\det\begin{bmatrix} 7 & 8 \\ 0 & 8 \end{bmatrix} & \det\begin{bmatrix} 3 & 8 \\ 7 & 8 \end{bmatrix} & -\det\begin{bmatrix} 3 & 7 \\ 7 & 0 \end{bmatrix} \\ \det\begin{bmatrix} 7 & 8 \\ 4 & 23 \end{bmatrix} & -\det\begin{bmatrix} 3 & 8 \\ 15 & 23 \end{bmatrix} & \det\begin{bmatrix} 3 & 7 \\ 15 & 4 \end{bmatrix} \end{bmatrix}^T = \begin{bmatrix} 6 & 22 & 25 \\ 15 & 20 & 25 \\ 24 & 23 & 11 \end{bmatrix}$$

$$MM^{-1} = \frac{1}{\det}\cdot\text{adj}(MM) \bmod 26 = \boxed{\begin{bmatrix} 2 & 16 & 17 \\ 5 & 24 & 17 \\ 8 & 25 & 21 \end{bmatrix}}$$

5. Shift cipher, frequency analysis (refer to 9-2 of Bach's notes)

The idea is to count the most frequently occurring letter in the ciphertext and try to match with the most frequently occurring letter in the English alphabet.

http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html



In the English alphabet: this is the letter E!

Given ciphertext: LCLLEWLJAZLNNZMVYIYLHRMHZA

The letter L occurs 6 times in this 26 character string. much more frequent than any other letter.

Let's say $\underset{11}{L}$ in ciphertext = $\underset{4}{E}$ in plaintext. (our "best guess")

Then: solve $e_k(x) = x + k \bmod 26$ for k

$11 = 4 + k \bmod 26 \implies \boxed{k = 7}$

Determine the plaintext:

Recall the decryption function $d_k(y) = y - k \bmod 26$

Plug in ciphertext for y and use our guess for k. (math not shown)

$$d_k(y) = y - 7 \bmod 26$$

We recover the plaintext: $\boxed{\text{EVEEXPECTSEGGSFORBREAKFAST}}$