2a $521x + 233y = 1$

$521 = 233(2) + 55$
$233 = 55(4) + 13$
$55 = 13(4) + 3$
$13 = 3(4) + 1$

$1 = 13 - 3(4)$
$= 13 - (55 - 13\cdot 4)\cdot 4$
$= 13 - (55\cdot 4 - 13\cdot 16) = 13\cdot 17 - 55\cdot 4$
$= (233 - 55\cdot 4)\cdot 17 - 55\cdot 4$
$= 233\cdot 17 - 55\cdot 68 - 55\cdot 4$
$= 233\cdot 17 - 55(68 - 4)$
$= 233\cdot 17 - 55\cdot 72$
$= 233\cdot 17 - (521 - 233\cdot 2)\cdot 72$
$233\cdot 17 - 521\cdot 72 + 233\cdot 144$
$1 = 521\cdot -72 + 233\cdot 161$
$x = -72 \quad y = 161$

b. find $521^{-1} \bmod 233 \Rightarrow 55^{-1} \bmod 233$

$\gcd(521, 233) = 1$ so $521^{-1} \bmod 233$ exists

$233 = 55(4) + 13 \qquad p_0 = 0$
$55 = 13(4) + 3 \qquad p_1 = 1$
$13 = 3(4) + 1 \qquad p_2 = 0 - 1(4) \bmod 233 = -4 \bmod 233$
$p_3 = 1 - (-4(4)) \bmod 233 = 1 + 16 \bmod 233 = 17 \bmod 233$
$p_4 = -4 - (17\cdot 4) \bmod 233 = -72 \bmod 233$

So $521^{-1} \bmod 233$ is $-72 \bmod 233$

Find $233^{-1} \bmod 521$

$521 = 233(2) + 55 \qquad p_0 = 0$
$233 = 55(4) + 13 \qquad p_1 = 1$
$55 = 13(4) + 3 \qquad p_2 = 0 - 1(2) \bmod 521 = -2$
$13 = 3(4) + 1 \qquad p_3 = 1 - (-2(4)) \bmod 521 = 1 + 8 \bmod 521 = 9 \bmod 521$
$p_4 = -2 - 9(4) \bmod 521 = -38 \bmod 521$
$p_5 = 9 - (-38)(4) \bmod 521 = 161 \bmod 521$

So $233^{-1} \bmod 521$ is $161 \bmod 521$

3. $K_1 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \quad K_2 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \quad K_3 = (7,2)$

$K_i \cdot K_2 = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \qquad x = (5,8) \quad y = (2,4)$

$(5,8)K + 2(1,1) = (2,4) \bmod 11$

$K = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 5a+c & 5b+d \\ a & b \end{pmatrix}$

$(5,8)\begin{pmatrix} 5a+c & 5b+d \\ a & b \end{pmatrix} + (2,2) = (2,4)$

$(5,8)\begin{pmatrix} 5a+c & 5b+d \\ a & b \end{pmatrix} = (0,2)$

$(5(5a+c) + 8a) \bmod 11 = 0 \bmod 11$
$5(5b+d) + 8b) \bmod 11 = 2 \bmod 11$
$25a + 5c + 8a = (33a + 5c) \bmod 11 = 0 \bmod 11$
$0a + 5c \qquad a = 0 \to \text{any}$
$c = 11 \qquad c = 11$
$(0 + 55) \bmod 11 = 0 \bmod 11$

$25b + 5d + 8b$
$(33b + 5d) \bmod 11 = 2 \bmod 11$
$b = 0 \to \text{any}$
$5d \bmod 11 = 2 \bmod 11 \qquad 33 + 2 = 35$
$d = 7 \qquad 11\cdot 3 + 2 = 5\cdot 7$
$35 \bmod 11 = 2 \bmod 11$
$\begin{pmatrix} 0 & 0 \\ 11 & 7 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 11 & 7 \end{pmatrix} = K_3$

$x\begin{pmatrix} 16 & 12 \\ 1 & 1 \end{pmatrix} + 2(1,1) = y \pmod{11}$

$x\begin{pmatrix} 5 & 1 \\ 1 & 1 \end{pmatrix} + 2(1,1) = y$

b. $K = \begin{pmatrix} 5 & 1 \\ 1 & 1 \end{pmatrix}$

$K^{-1} = \frac{1}{\det(K)} \cdot K^{*} = \begin{pmatrix} 3 & 8 \\ 8 & 4 \end{pmatrix}$

$b = -2(1,1) = (-2,-2)$

$y\begin{pmatrix} 3 & 8 \\ 8 & 4 \end{pmatrix} + (-2,-2) = x$

4a. Shift cipher

Since the text is repeated a's, the ciphertext will consist of one letter some amount of distance away from a. The eavesdropper will know it's one letter repeated but won't be able to know the letter or the key because it could be any character

b. Affine cipher

Same with shift cipher, since all letters are a the ciphertext will be one character that is scaled and shifted from a. So "2" won't know the key or letter

c. Hill cipher

All values in cipher matrix is the same and since $a = 0$ the matrix will be 0 mod 26 so the "2" will be more likely to guess the character but not the key

0 0 0
0 1 1 , , , ,

d. Vigenere Cipher

The ciphertext will be the key as $a = 0$, so the "2" can deduce that the ciphertext is random numbers but if it repeats for m characters then "2" can deduce that it's the same character and if they start at a, the key will not change but with any big character value the mod 26 will make the key different.

5. $z_{i+3} \sum_{j=0}^{2} c_j z_{i+j} \pmod 3 \quad c_j \in \{0,1,2\}$

$1, 0, 1, *, 2, 0, *, 1$

$z_{i+3} = c_0 z_{i+0} + c_1 z_{i+1} + c_2 z_{i+2}$

$\boxed{z_3} = c_0 z_0 + c_1 z_1 + c_2 z_2 = 0(1) + 0(1) + 2(1) = \boxed{2 \pmod 3}$

$z_4 = c_0 z_1 + c_1 z_2 + c_2 z_3 = 0(0) + 1(1) + 2(2) = 5 \pmod 3 = 2 \bmod (3)$

$z_5 = 0$

$\boxed{z_6} = c_0 z_3 + c_1 z_4 + c_2 z_5 = 0(2) + 1(2) + 0(2) = \boxed{2 \bmod (3)}$

8. $a: \frac{2}{3} \quad b: \frac{1}{6} \quad c: \frac{1}{6} \quad m = 3$

ABCBABBBACAA
1 1 1 1 1 1

Shift by 1,2,3 looking for overlaps

1 has 3 overlap

2 has 4 overlap

3 has 2 overlap

So I expect key length to be 2

by looking at every other letter,

AGABAA BBBBCA

even odd

Due to $\frac{2}{3}$ for A, in even A decrypts A

$\frac{4}{6} = \frac{2}{3}$

In odd sequence, B decrypts A because

$\frac{4}{6} = \frac{2}{3}$

key is $\boxed{AB}$