# CSCI-4116
# Assignment 4

Anas Alhadi

B00895875

February 10, 2025

## Question 1a

Given a matrix $A$, it's inverse $A^{-1} = (det\ A)^{-1} \times adj\ A$

We first check if $A$ is invertible modulo 2, by finding its determinant and verifying that it is relativley prime to 2.

### det A:

I am using row reduction and fixing $i = 3$. Since $j = 2$ and $j = 3$ both result in 0 i'll be omitting their calculation step. So:

$$det\ A = (-1)^{3+1} \times 1 \times det\ A_{3,1}$$

$$det\ A = 1 \times (0 - 1) = -1$$

We thus have it that $det\ A = -1$ which is congruent to $1 (\text{mod } 2)$ and has an inverse $(det\ A)^{-1} = 1$ in modulo 2. So $A$ is invertible

## adj A

The adjoint matrix of $A$ is the transpose of the matrix of A's cofactors. So we first find the the matrix of cofactors $C$ then transpose it.

$$\begin{aligned}
C_{1,1} &= (-1)^{1+1} \times det\ A_{1,1} = & 1 \times (0-0) = & \quad 0 \\
C_{1,2} &= (-1)^{1+2} \times det\ A_{1,2} = & -1 \times (0-0) = & \quad 0 \\
C_{1,3} &= (-1)^{1+3} \times det\ A_{1,3} = & 1 \times (0-1) = & \quad -1 \\
C_{2,1} &= (-1)^{2+1} \times det\ A_{2,1} = & -1 \times (0-0) = & \quad 0 \\
C_{2,2} &= (-1)^{2+2} \times det\ A_{2,2} = & 1 \times (0-1) = & \quad -1 \\
C_{2,3} &= (-1)^{2+3} \times det\ A_{2,3} = & -1 \times (0-1) = & \quad 1 \\
C_{3,1} &= (-1)^{3+1} \times det\ A_{3,1} = & 1 \times (0-1) = & \quad -1 \\
C_{3,2} &= (-1)^{3+2} \times det\ A_{3,2} = & -1 \times (0-1) = & \quad 1 \\
C_{3,3} &= (-1)^{3+3} \times det\ A_{3,3} = & 1 \times (1-1) = & \quad 0
\end{aligned}$$

Giving us the matrix:

$$C = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix}$$

And an adjoint matrix:

$$adj\ A = C^T = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 1 \\ -1 & 1 & 0 \end{pmatrix}$$

## $\mathbf{A^{-1}}$

$$A^{-1} = 1 \times adj\ A \pmod 2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

# Question 1b

Again I am using row reduction, and fixing $i = 1$.

$$\begin{aligned}(-1)^{1+1} \times 1 \times det\ A_{1,1} &= \quad 1 \times (6-1) &&= 5\\ (-1)^{1+2} \times 2 \times det\ A_{1,2} &= \quad -1 \times (4-3) &&= -2\\ (-1)^{1+3} \times 3 \times det\ A_{1,3} &= \quad 3 \times (2-9) &&= -21\end{aligned}$$

$$det\ A = 5 - 2 - 21 = -18$$

# Question 2a

Recall that a matrix $M$ is invirtable in modulo $p$ iff $gcd(det\ M, p) = 1$, thus to find the primes where $M$ is not invirtable, we need to find the prime factors of the $det\ M$

## det M

I am using column reduction with $j = 1$

$$\begin{aligned}(-1)^{1+1} \times 1 \times det\ M_{1,1} &= \quad 1 \times (980-350) = &&630\\ (-1)^{1+2} \times 1 \times det\ M_{1,2} &= \quad -1 \times (392-56) = &&-336\\ (-1)^{1+3} \times 1 \times det\ M_{1,3} &= \quad 1 \times (50-20) = &&30\end{aligned}$$

$$det\ M = 630 - 336 + 30 = 324$$

The prime factors of 324 are 2 and 3. Thus $M$ is not invertible in $p \in \{2, 3\}$.

# Question 2b

Just like in Question 2a, we need to find the inverse of the det of M in modulo 101. Then multiply it with the adjoint matrix of M.

## Inverse of det M

We can use the Euclidean algorithm to find the inverse. First observe that $324 \equiv 21 (\text{mod } 101)$, Thus we find the inverse of 21 in modulo 101

**Euclidean Alg Steps:**

$101 = 21(4) + (17)$
$21 = 17(1) + (4)$
$17 = 4(4) + 1$

Now moving backwards:

$1 = 17 + 4(-1)$
$4 = 21 + 17(-1)$
$17 = 101 + 21(-4)$

Subsituting the $2^{nd}$ and $3^{rd}$ equations into the first:

$1 = (101 + 21(-4)) + 21(-4) + (101 + 21(-4))(-4)$ $1 = 101(6) + 21(-24)$

Thus:

$$1 \equiv 21 \times -24 (\text{mod } 101)$$

$$1 \equiv 21 \times 77 (\text{mod } 101)$$

And the inverse of the determinant of M, $(det\ M)^{-1} = 77$

## Adjoint matrix of M

Again, we now repeat the exact same steps taken in Question 1a to find the cofactor matrix of A but this time on M. This gives us the cofactor matrix $C$

$$C = \begin{pmatrix} 630 & -171 & 9 \\ -336 & 192 & -12 \\ 30 & -21 & 3 \end{pmatrix}$$

$$adj\ M = C^T = \begin{pmatrix} 630 & -336 & 30 \\ -171 & 192 & -21 \\ 9 & -12 & 3 \end{pmatrix}$$

### Inverse of M

$$
\begin{aligned}
M^{-1} &= (det\ M)^{-1} \times adj\ M \pmod{101} \\
&= 77 \times \begin{pmatrix} 630 & -336 & 30 \\ -171 & 192 & -21 \\ 9 & -12 & 3 \end{pmatrix} \pmod{101} \\
&= \begin{pmatrix} 48510 & -25872 & 2310 \\ -13167 & 14784 & -1617 \\ 693 & -924 & 231 \end{pmatrix} \pmod{101} \\
&\equiv \begin{pmatrix} 30 & 85 & 88 \\ 64 & 38 & 100 \\ 87 & 86 & 29 \end{pmatrix}
\end{aligned}
$$

## Question 3

$$
\begin{aligned}
\mathcal{E}: &\quad (\mathbb{Z}/2\mathbb{Z})^3 \to (\mathbb{Z}/2\mathbb{Z})^3 \\
s.t &\quad \mathcal{E}(v) \mapsto Av + b \pmod 2
\end{aligned}
$$

Where:

$$
A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
$$

$$
b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}
$$

## Question 4

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$b = \begin{pmatrix} 18 \\ 2 \\ 11 \end{pmatrix}$$

## Question 5

The corresponding key stream is:
$z = 1010011\ 1010011\ 1010011$

Resulting in:
$\mathcal{E}_k(w) = 0100000\ 0100010\ 0000010$