$17 \cdot 23 \equiv 1 \pmod{26}$

$17^{-1} \equiv 23 \pmod{26}$

$-5 \equiv 21 \pmod{26}$

$12^{-1} \equiv \quad \pmod{26}$ $-5+26$

$2x + 5y \equiv 8 \pmod{26}$

$4x + 3y \equiv 2$

$$\begin{bmatrix} 2 & 5 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 8 \\ 2 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 3 & -5 \\ -4 & 2 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & -5 \\ -4 & 2 \end{bmatrix} \begin{bmatrix} 8 \\ 2 \end{bmatrix} \pmod{26}$$

$$A = \begin{bmatrix} 2 & 5 \\ 4 & 3 \end{bmatrix}$$

$\det A = 2 \cdot 3 - 4 \cdot 5 = -14$

$\equiv 12 \pmod{26}$

$$A^{-1} = \begin{bmatrix} 3 & -5 \\ -4 & 2 \end{bmatrix} (\det A)^{-1}$$

$$= \begin{bmatrix} 3 & 21 \\ 22 & 2 \end{bmatrix}$$

$$\tilde{A} = \begin{bmatrix} 3 & -5 \\ -4 & 2 \end{bmatrix}$$

$$A\tilde{A} = \begin{bmatrix} 2 & 5 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 3 & -5 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -14 & 0 \\ 0 & -14 \end{bmatrix}$$

$$\begin{bmatrix} -14 & 0 \\ 0 & -14 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 3\cdot 8 - 5\cdot 2 \\ -4\cdot 8 + 7\cdot 2 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ -28 \end{bmatrix}$$

$$-14x \equiv 14 \pmod{26}$$
$$-14y \equiv -28 \pmod{26}$$

$$12x \equiv 14 \pmod{26} \Rightarrow 6x \equiv 7 \pmod{13}$$
$$12y \equiv 24 \pmod{26}$$

$$\Rightarrow x \equiv 12 \text{ OR } 25 \pmod{26}$$
$$y \equiv 2 \text{ OR } 15 \pmod{26}$$

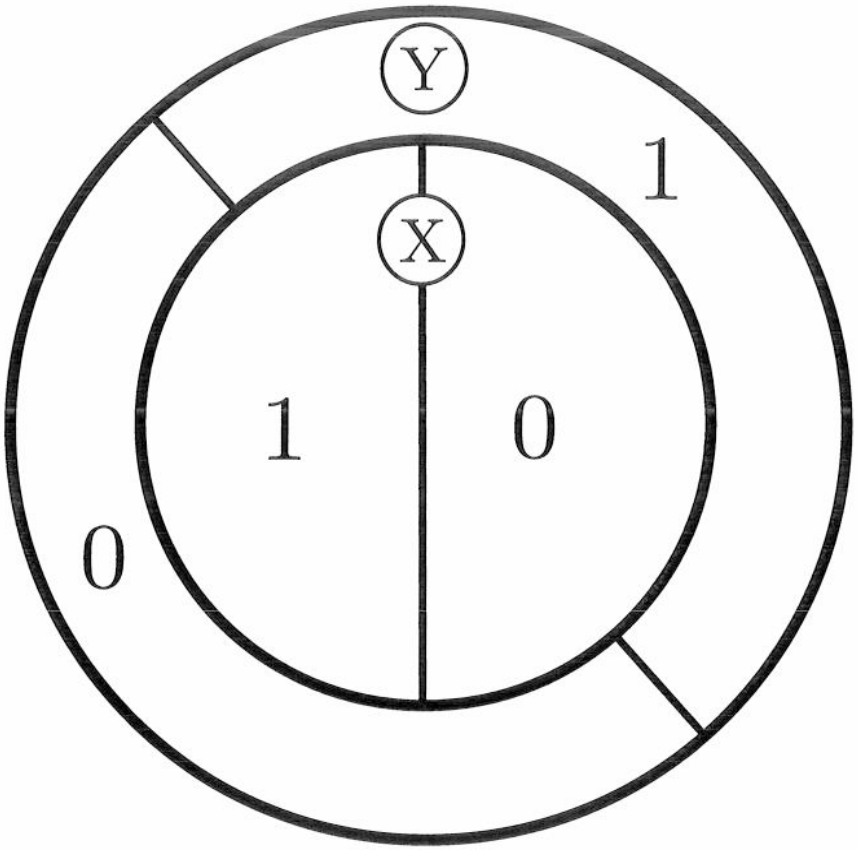
$$(x, y) \equiv (12, 2), (12, 15), (25, 2), (25, 15) \pmod{26}$$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \pmod{29} \text{ OR } \pmod{26}$$

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (\det A)^{-1} \pmod{29} \text{ OR } \pmod{26}$$

Example:

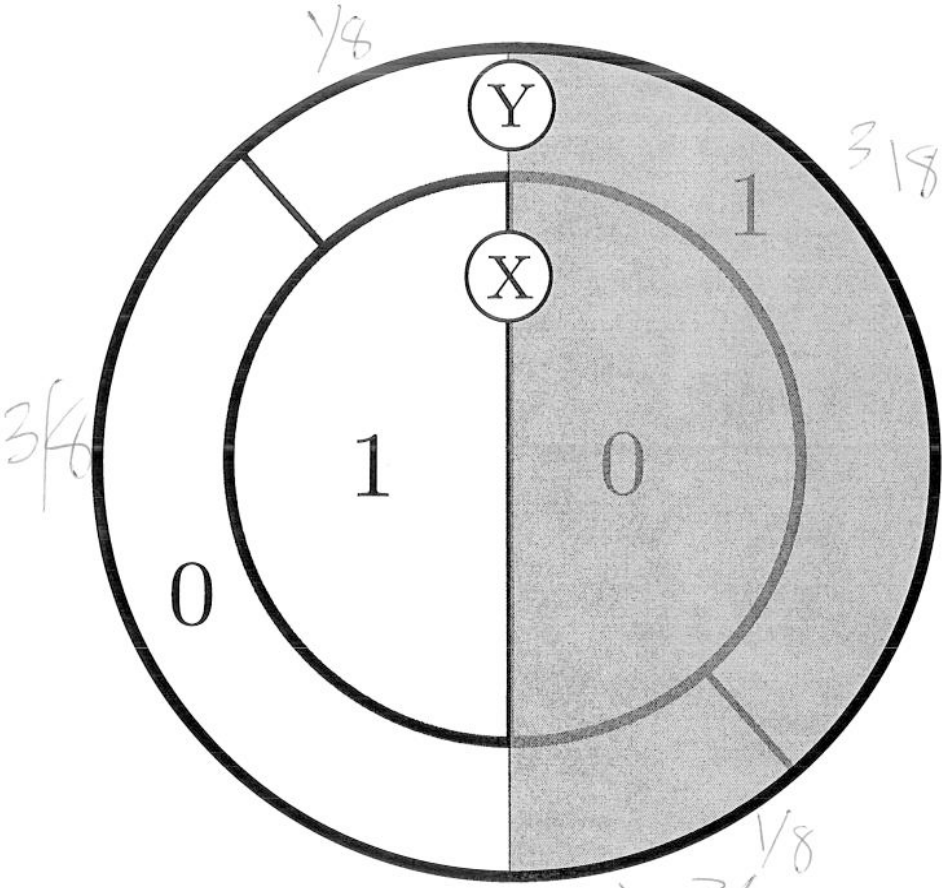
~~Cyphertext is mod 26~~



P(Y=0 & X=1) = 3/8

P(Y=0 | X=1) =

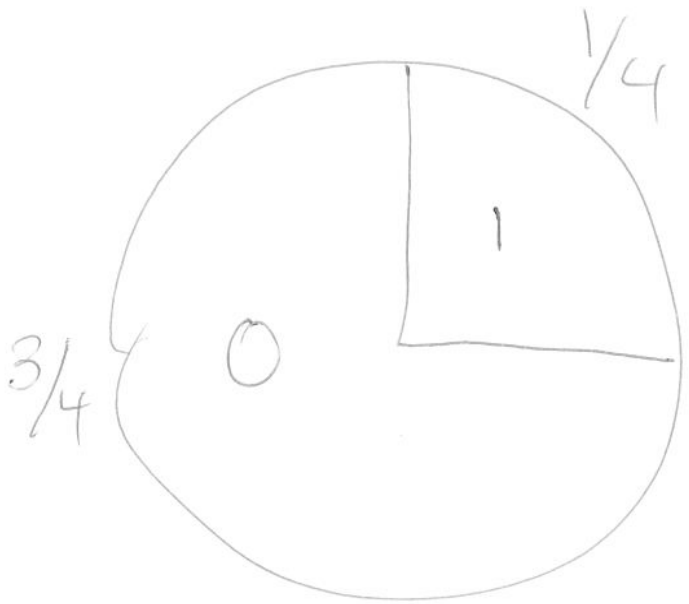
"given"

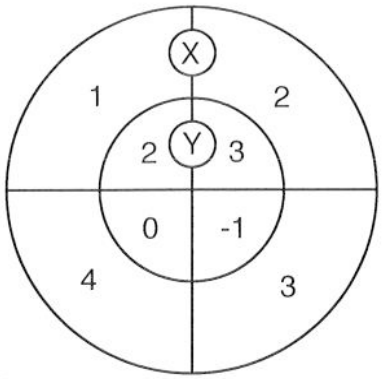


$P(Y=0 \,\&\, X=1) = 3/8$

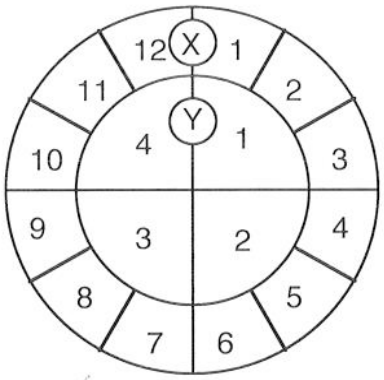
$$P(Y=0 \mid X=1) = \frac{P(Y=0 \,\&\, X=1)}{P(X=1)} = \frac{3/8}{1/2} = 3/4$$

$P(X=1) = 1/2$



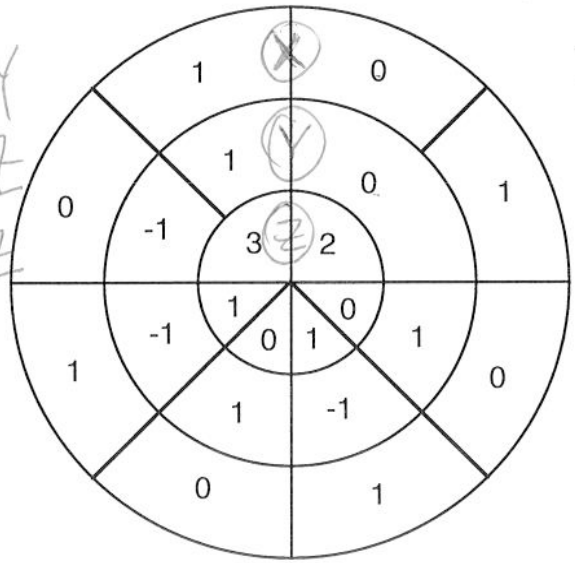


X is dependent on Y
Y is dependent on X



Y is dependent on X
X is not dependent on Y

Z is dependent on X & Y
Y is dependent on X & Z
X is not dependent on Y & Z



Z is not dependent on X
Z is not dependent on Y
Y is not dependent on X
Y is not dependent on Z
X is not dependent on Y
X is not dependent on Z

X is dependent on Y if X is a function of Y

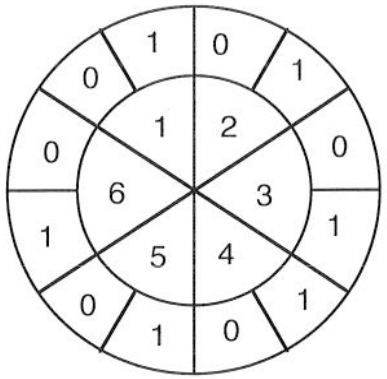
that is, knowing the value of Y determines the value of X

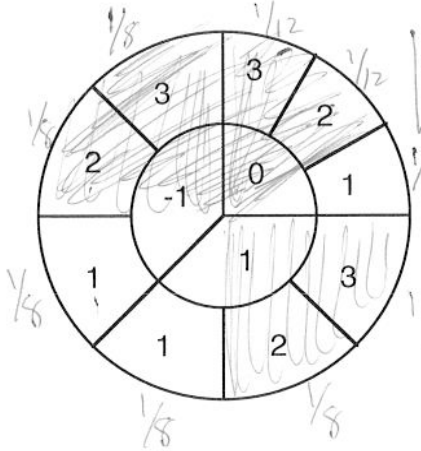
X is independent of Y if $P(X = a|Y = b) = P(X = a)$

or $P(X = a \text{ and } Y = b) = P(X = a)P(Y = b)$

or knowing the value of Y does not change the probabilities of X

If X is independent of Y, then Y is independent of X.





$$P(Y=0|X=1) = \frac{P(Y=0 \,\&\, X=1)}{P(X=1)} = \frac{1/12}{1/12 + 1/8 + 1/8} = \frac{1/12}{1/12 + 3/12} = 1/4$$