CS152-Homework3

Hongchen Cao 2019533114

2020.9.25

1

Count the number of pairs, we find that
num(”TX”)=4
num(”LM”)=3
If $d_k(”TX”) = ”TH”$ and $d_k(”LM”) = ”IN”$, we have $K = \begin{bmatrix} 4 & 11 \\ 13 & 9 \end{bmatrix}$
Thus, the plaintext=”thekingwasinhiscountinghousecountingouthismoneythequeuewasintheparloureating breadandhoneyz”

2

Pr($\mathbf{Y}$=y)=$\frac{1}{n}$

Pr($\mathbf{Y{=}y}|\mathbf{X{=}x}$)=$\frac{1}{n}$

Pr($\mathbf{X}$=x|$\mathbf{Y}$=y)=$\frac{Pr(\mathbf{Y}=y|\mathbf{X}=x)}{Pr(\mathbf{Y}=y)} = \frac{\frac{1}{n} \cdot Pr(\mathbf{X}=x)}{\frac{1}{n}} = Pr(\mathbf{X}=x)$

Thus, perfect secrecy.

3

Pr($\mathbf{Y}$=1)=$\frac{\alpha}{3}$
Pr($\mathbf{Y}$=2)=$\frac{\alpha}{3}$
Pr($\mathbf{Y}$=3)=$\frac{\alpha}{3}$
Pr($\mathbf{Y}$=4)=$\frac{\beta}{2}$
Pr($\mathbf{Y}$=5)=$\frac{\beta}{2}$
Then,
Pr($\mathbf{X}$=a|$\mathbf{Y}$=1)=$\frac{Pr(K_1)}{Pr(\mathbf{Y}=1)} \cdot Pr(\mathbf{X}=a) = \frac{\frac{\alpha}{3}}{\frac{\alpha}{3}} \cdot Pr(\mathbf{X}=a) = Pr(\mathbf{X}=a)$
Pr($\mathbf{X}$=a|$\mathbf{Y}$=2)=$\frac{Pr(K_2)}{Pr(\mathbf{Y}=2)} \cdot Pr(\mathbf{X}=a) = \frac{\frac{\alpha}{3}}{\frac{\alpha}{3}} \cdot Pr(\mathbf{X}=a) = Pr(\mathbf{X}=a)$
Pr($\mathbf{X}$=a|$\mathbf{Y}$=3)=$\frac{Pr(K_3)}{Pr(\mathbf{Y}=3)} \cdot Pr(\mathbf{X}=a) = \frac{\frac{\alpha}{3}}{\frac{\alpha}{3}} \cdot Pr(\mathbf{X}=a) = Pr(\mathbf{X}=a)$
Pr($\mathbf{X}$=a|$\mathbf{Y}$=4)=$\frac{Pr(K_4)}{Pr(\mathbf{Y}=4)} \cdot Pr(\mathbf{X}=a) = \frac{\frac{\beta}{2}}{\frac{\beta}{2}} \cdot Pr(\mathbf{X}=a) = Pr(\mathbf{X}=a)$
Pr($\mathbf{X}$=a|$\mathbf{Y}$=5)=$\frac{Pr(K_5)}{Pr(\mathbf{Y}=5)} \cdot Pr(\mathbf{X}=a) = \frac{\frac{\beta}{2}}{\frac{\beta}{2}} \cdot Pr(\mathbf{X}=a) = Pr(\mathbf{X}=a)$
Pr($\mathbf{X}$=b|$\mathbf{Y}$=1)=$\frac{Pr(K_3)}{Pr(\mathbf{Y}=1)} \cdot Pr(\mathbf{X}=b) = \frac{\frac{\alpha}{3}}{\frac{\alpha}{3}} \cdot Pr(\mathbf{X}=b) = Pr(\mathbf{X}=b)$
Pr($\mathbf{X}$=b|$\mathbf{Y}$=2)=$\frac{Pr(K_1)}{Pr(\mathbf{Y}=2)} \cdot Pr(\mathbf{X}=b) = \frac{\frac{\alpha}{3}}{\frac{\alpha}{3}} \cdot Pr(\mathbf{X}=b) = Pr(\mathbf{X}=b)$
Pr($\mathbf{X}$=b|$\mathbf{Y}$=3)=$\frac{Pr(K_2)}{Pr(\mathbf{Y}=3)} \cdot Pr(\mathbf{X}=b) = \frac{\frac{\alpha}{3}}{\frac{\alpha}{3}} \cdot Pr(\mathbf{X}=b) = Pr(\mathbf{X}=b)$
Pr($\mathbf{X}$=b|$\mathbf{Y}$=4)=$\frac{Pr(K_5)}{Pr(\mathbf{Y}=4)} \cdot Pr(\mathbf{X}=b) = \frac{\frac{\beta}{2}}{\frac{\beta}{2}} \cdot Pr(\mathbf{X}=b) = Pr(\mathbf{X}=b)$
Pr($\mathbf{X}$=b|$\mathbf{Y}$=5)=$\frac{Pr(K_4)}{Pr(\mathbf{Y}=5)} \cdot Pr(\mathbf{X}=b) = \frac{\frac{\beta}{2}}{\frac{\beta}{2}} \cdot Pr(\mathbf{X}=b) = Pr(\mathbf{X}=b)$
Thus, $\forall x \in P$, $y \in C$, we have $Pr(\mathbf{X}=x|\mathbf{Y}=y) = Pr(\mathbf{X}=x)$
So, perfect secrecy.

4

4.1

	000	001	010	011	100	101	110	111
K_1=000	000	001	010	011	100	101	110	111
K_2=001	001	000	011	010	101	100	111	110
K_3=010	010	011	000	001	110	111	100	101
K_4=011	011	010	001	000	111	110	101	100
K_5=100	100	101	110	111	000	001	010	011
K_6=101	101	100	111	110	001	000	011	010
K_7=110	110	111	100	101	010	011	000	001
K_8=111	111	110	101	100	011	010	001	000

4.2

First proof the size of matrix is $2^n \times 2^n$.

Both plaintext and key have n bits, so from the definition we know that matrix must have 2^n rows and 2^n cols.

Then we proof the matrix follows the definition of Latin square.

Let A be the matrix, $\forall i, j, k \in [1, n]$ and $j \neq k$, we have $A_{ij} \neq A_{ik}$ because $in\, i^{th} row$, $p_j \neq p_k$ and both p_j, p_k encrypted by K_i.

The situation in every col of the matrix is same, which means $\forall i, j, k \in [1, n]$ and $j \neq k$, we have $A_{ji} \neq A_{ki}$.

Thus, we have proved that the encryption matrix of a OTP is a Latin square of order 2^n.