(2) נתון: ΔABC שווה שוקיים, $AB=AC$.

(3) נתון: ΔABC שווה שוקיים, $AB=AC$.
CD חוצה את $\angle C$, $D\in AB$.

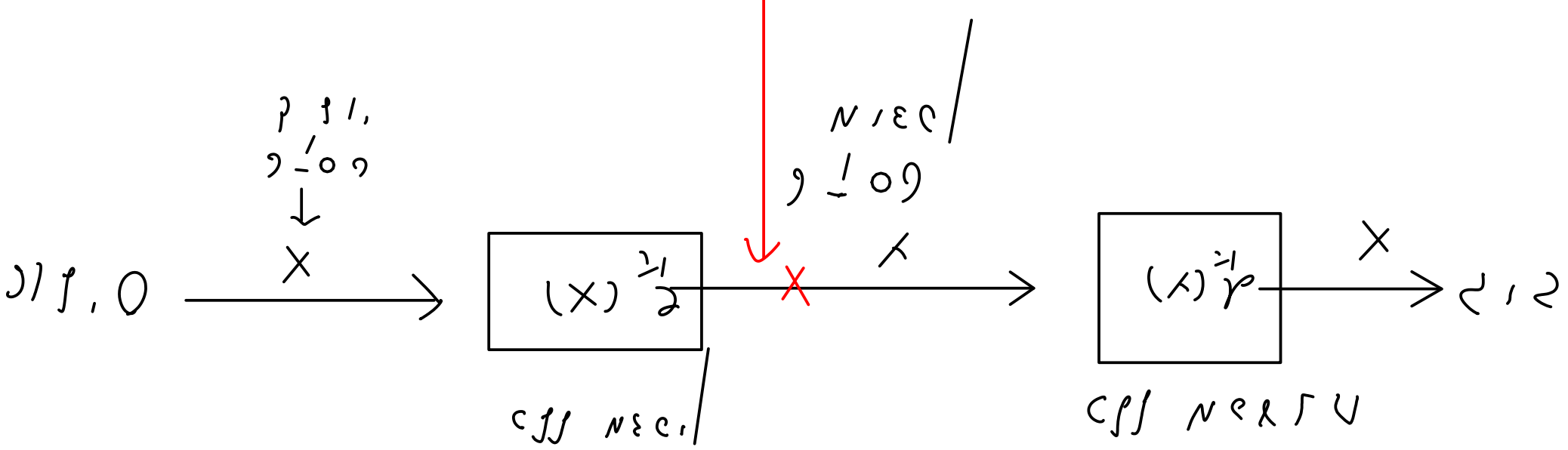
(4) נתון: ΔABC שווה שוקיים, $AB=AC$.
BD חוצה את $\angle B$, $D\in AC$.

(1) נתון: ΔABC שווה שוקיים, $AB=AC$.
BD חוצה את $\angle B$, $D\in AC$.
$AD=DC$

(2) ΔABC שווה שוקיים, $AB=AC$.
BD חוצה את $\angle B$, $D\in AC$.
$AD=DC$

(3) ΔABC שווה שוקיים, $AB=AC$.
CD חוצה את $\angle C$, $D\in AB$.
$AD=DB$

(4) ΔABC שווה שוקיים, $AB=AC$.
BD חוצה את $\angle B$, $D\in AC$.
$AD=DC$



טבלה 6.2 תדירות הופעת אותיות בטקסט רנדומי

	אות	תדירות
1.	e	$p = 0.127$
2.	t, a, o, i, n, s, h, r	$0.06 \lessapprox p \lessapprox 0.09$
3.	d, l	$p \approx 0.04$
4.	c, u, m, w, f, g, y, p, b	$0.015 \lessapprox p \lessapprox 0.028$
5.	v, k, j, x, q, z	$p < 0.01$

.

.

טבלה 6.1 פיזורים תדירותיים של האותיות של האלפבית

אות	תדירות
a	0.082
b	0.015
c	0.028
d	0.043
e	0.127
f	0.022
g	0.02
h	0.061
i	0.07
j	0.002
k	0.008
l	0.04
m	0.024

אות	תדירות
n	0.067
o	0.075
p	0.019
q	0.001
r	0.06
s	0.063
t	0.091
u	0.028
v	0.01
w	0.023
x	0.001
y	0.02
z	0.001

אותיות ידוע כי אינן תורמות את התורמי האמצעית ביותר אינני אלו הוא לא ידוע את המסרים. כיצד הוא

ברות לפניה אותה. בשאו את המפתח בבקשה.

KARSROHVUKARPFSZFERXERFKREKAFSKARSROHVUKARURTVEKARVSR

ניתן כי אינך שלחת הודעה מוצפנת כדאי ואותיות יש/ את ההודעה. המפתח מוצפן הוא

ב' אלגוריתם של אוילר למציאת מעגל אוילר בגרף קשיר, שבו כל הקודקודים הם בדרגה זוגית. נתאר את האלגוריתם עבור גרף קשיר $G=(V,E)$ שבו $V=\{1,2,\ldots,n\}$.

$E_k(i,j)$ = מספר הקשתות מ־i ל־j שטרם נמחקו.

$E_k(i)$ = $\sum_j E_k(i,j)$ — דרגת i בגרף שנותר.

$E_{ir}(i)$ = $\sum_j E_{ir}(i,j)$ — דרגת i בגרף המקורי.

$E_{ir}(x)=ax+b \pmod 7$:נגדיר את הפונקציה הלינארית הבאה

$$\begin{cases} E_k(4)=12 \Rightarrow a(4)+b=12 \\ E_k(19)=10 \Rightarrow a(19)+b=10 \end{cases}$$

$$\left(\begin{array}{cc|c} 4 & 1 & 12 \\ 19 & 1 & 10 \end{array}\right) \xrightarrow{R_2-R_1} \left(\begin{array}{cc|c} 4 & 1 & 12 \\ 15 & 0 & -2 \end{array}\right) \bmod 26 = \left(\begin{array}{cc|c} 4 & 1 & 12 \\ \underline{15} & 0 & 19 \end{array}\right)$$

$$\xrightarrow{R_2 \to 15^{-1}R_2 = 7R_2} \left(\begin{array}{cc|c} 4 & 1 & 12 \\ 1 & 0 & 133 \end{array}\right) \bmod 26 = \left(\begin{array}{cc|c} 4 & 1 & 12 \\ 1 & 0 & 3 \end{array}\right) \xrightarrow{R_1 \to R_1 - 4R_2} \left(\begin{array}{cc|c} 0 & 1 & 5 \\ 1 & 0 & 3 \end{array}\right)$$

$\Rightarrow a=3,\ b=5.$

$gcd(a,26)=gcd(3,26)=1$:נוודא ש־a הפיך מודולו 26 (כלומר a^{-1} קיים מודולו 26)

$gcd(a,26)=1$ ⟸ $\exists a^{-1} \bmod 26$ מכאן שקיים פתרון יחיד למשוואה $ax=b \pmod{26}$, כלומר a^{-1} קיים מודולו 26 אם ורק אם a ו־26 זרים.

$a^{-1}=\tilde{a}\ (y-b)$ מקיים $a_k(y)$

$gcd(a,26)=1$ -ו $a,b \in \mathbb{Z}_{26}$ יהיו המספרים שלפי סעיף א' מקיימים $E_{ir}(x)=ax+b$.

$y=$ KARSRROHVUKARPFSZFERXERFKREKAFSKARSRROHVUKARURTVEKARVSR

A	6	N	0
B	0	O	2
C	0	P	1
D	0	Q	0
E	4	R	14
F	4	S	5
G	0	T	1
H	2	U	3
I	0	V	4
J	0	W	0
K	7	X	1
L	0	Y	0
M	0	Z	1

שאלה 2 מתוך 6 נקודות

נתון שהמפתח הוא מספר בן שני בתים, כלומר $K \in \{0,1,\ldots,65535\}$. נתון גם שהמפתח K נבחר באופן אחיד מבין כל המפתחות האפשריים. נתון שהטקסט המוצפן y הוא פלט של הצפנת ויז'נר עם המפתח K הלא־ידוע. נתון שהטקסט הגלוי x שהוצפן הוא משפט בעברית שנכתב בכתב מלא, ללא ניקוד וללא סימני פיסוק, ושכל האותיות בו הן אותיות גדולות.

א. (3 נקודות) חשבו את ההסתברות המותנית $P(K=k \mid y)$ עבור כל $k \in \{0,1,\ldots,65535\}$.

ב. (3 נקודות) מצאו את המפתח K.

רמז: ניתן להניח שהמפתח K הוא מספר בן שני בתים שבו שני הבתים הם אותיות בעברית.

שלב 3: בונים הכלל מפענח המתאים:

$$d_k(y) = a^{-1}(y-b) = 3^{-1}(y-5) = 9(y-5) = 9y - 45 \mod 26$$

$$-45 \mod 26 = 7$$

$$\Rightarrow \boxed{d_k(y) = 9y + 7}$$

שלב 4: ננסה לפענח את y:

$$d_k(10) = 9(10)+7 \mod 26 = 97 \mod 26 = 19$$

טקסט מוצפן → $y \in C$

מספרים ב-$\mathbb{Z}_{26}$ → $y \in \mathbb{Z}_{26}$

$y \in C$	K	A	R	S	R	R	O	H	V	U	K	A	R	P	F	S	Z	F	E	R
$y \in \mathbb{Z}_{26}$	10	0	17	18	17	17	14	7	21	20	10	0	17	15	5	18	25	5	4	17
$x = d_k(y) \in \mathbb{Z}_{26}$	19	7	4	13	4	4	3	18	14	5	19	7	4	12	0	13	24	0	17	4
$x \in P$	t	h	e	n	e	e	d	s	o	t	t	h	e	m	a	n	y	a	r	e

$y \in C$	X	E	R	F	K	R	E	K	A	F	S	K	A	R	S	R	R	O	H
$y \in \mathbb{Z}_{26}$	23	4	17	5	10	17	4	10	0	5	18	10	0	17	18	17	17	14	7
$x = d_k(y) \in \mathbb{Z}_{26}$	6	17	4	0	19	4	17	19	7	0	13	19	7	4	13	4	4	3	18
$x \in P$	g	r	e	a	t	e	r	t	h	a	n	t	h	e	n	e	e	d	s

$y \in C$	V	U	K	A	R	U	R	T	V	E	K	A	R	V	S	R
$y \in \mathbb{Z}_{26}$	21	20	10	0	17	20	17	19	21	4	10	0	17	21	18	17
$x = d_k(y) \in \mathbb{Z}_{26}$	14	5	19	7	4	5	4	22	14	17	19	7	4	14	13	4
$x \in P$	o	f	t	h	e	f	e	w	o	r	t	h	e	o	n	e

the needs of the many are greater than the needs of the few or the one.

הגדרה של צופן היל:

$$e_k(x_1, x_2 \dots x_m) = (x_1 \dots x_m)k \qquad k \in \mathbb{Z}_{26}^{m\times m}$$

$$d_k(y_1, y_2 \dots y_m) = (y_1 \dots y_m)k^{-1}$$

קריפטואנליזה של צופן היל

משפט: נתון טקסט גלוי X וטקסט Y שהוצפן ע"י צופן היל.

נניח שהמפתח הוא $k \in \mathbb{Z}_{26}^{m\times m}$.

יהי $X = (x_1, x_2 \dots x_m)$ קטע של טקסט גלוי

ויהי $Y = (y_1, y_2 \dots y_m)$ הטקסט המוצפן של X המתאים.

אזי, המשוואה נתונה ע"י $Y = Xk$

נניח שנתונים m זוגות של טקסט גלוי כאלה ונסמן אותם:

$$X_1 = (x_{11}, x_{12} \dots x_{1m})$$

$$X_2 = (x_{21}\ x_{22}\ \cdots\ x_{2m})$$

$$\vdots$$

$$X_m = (x_{m1}\ x_{m2}\ \cdots\ x_{mm})$$

יהי $\hat{X} \in \mathbb{Z}_{26}^{m\times m}$ שמוגדר

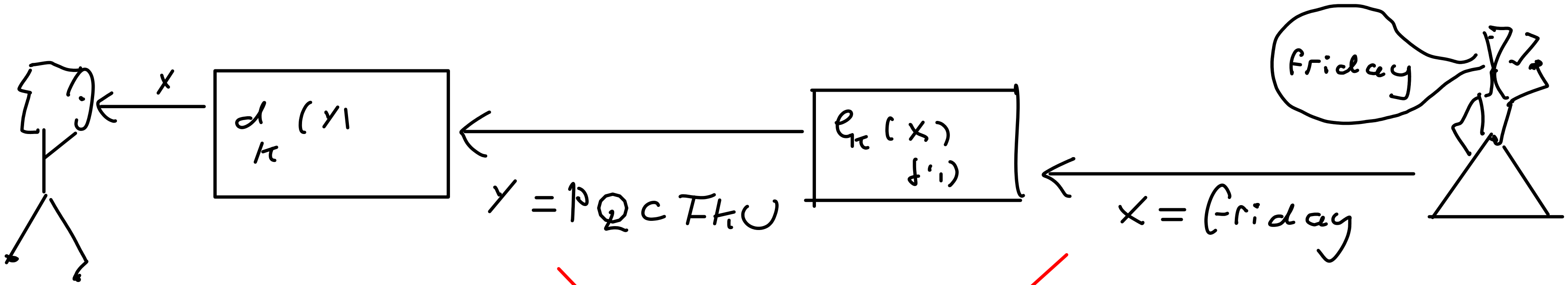
$$\hat{X} = \begin{pmatrix} — X_1 — \\ — X_2 — \\ \vdots \\ — X_m — \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ & & & \\ x_{m1} & x_{m2} & \cdots & x_{mm} \end{pmatrix}$$

אזי המפתח ניתן ע״י הנוסחה:

$$\hat{X}^{-1}\hat{Y} = \hat{X}^{-1}\hat{X}K \implies \hat{X}^{-1}\hat{Y} = K$$

כאשר $\hat{Y}$ הטקסט המוצפן של $\hat{X}$.

<u>דוגמה</u> אליס שולחת את ההודעה הבאה לבוב:



אוסקר השיג את הטקסט המוצפן Y
וגם הטקסט גלוי X.

מהו המפתח של הצופן שאוסקר מחשב? (נתון כי הסדר של
המפתח הוא 2x2)

<u>פתרון</u> <u>שלב 0</u>

תרגיל 1

$x \in P$	5	12	8	3	0	24
$y \in \mathbb{Z}_{26}^*$	15	16	2	5	10	20

$x \in P$ | f | r | $:$ | d | e | y

$y \in \mathbb{Z}_{26}^*$ | 15 | 16 | 2 | 5 | 10 | 20

$y \in C$ | P | Q | C | E | H | U

$x \in \mathbb{Z}_{26}^*$ | 5 | 12 | 8 | 3 | 0 | 24

תרגיל 2 סעיף א

$$X_1 = (5 \quad 12) \longrightarrow Y_1 = (15 \quad 16)$$

$$X_2 = (8 \quad 3) \longrightarrow Y_2 = (2 \quad 5)$$

$$\begin{pmatrix} 5 & 12 \\ 8 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = K$$

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 8 & 3 \end{pmatrix} K$$

$$\hat{Y} = \hat{X} K \quad \Longrightarrow \quad \hat{X}^{-1} \hat{Y} = K$$

תרגיל 2 סעיף ב

$$\hat{Y} = \begin{pmatrix} -Y_1 - \\ -Y_2 - \end{pmatrix} = \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}.$$

$$\hat{X} = \begin{pmatrix} -X_1 - \\ -X_2 - \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 8 & 3 \end{pmatrix}$$

תרגיל 3

$$|\hat{X}| = \begin{vmatrix} 5 & 12 \\ 8 & 3 \end{vmatrix} \mod 26 = -121 \mod 26 = 9$$

$$\hat{X}^{-1} = |\hat{X}|^{-1} \, adj(\hat{X})$$

תרגיל 4 סעיף א

$\hat{Y}$ של $\mathbb{Z}_{26}$ (2) הוכיחו כי $\hat{X}$ הפיכה אם ורק אם $\gcd(|\hat{X}|, 26) = 1$.

תרגיל 4 סעיף ב

הוכיחו כי $\hat{X}$ הפיכה אם ורק אם $\hat{Y}$ הפיכה.

תרגיל 4 סעיף ג

הוכיחו כי אם $\hat{X}$ הפיכה אז $\hat{Y}$ הפיכה.

תרגיל 4 סעיף ד

הוכיחו כי אם $\hat{Y}$ הפיכה אז $\hat{X}$ הפיכה.

$|\hat{X}|^{-1} \bmod 26 = 9^{-1} \bmod 26 = 3.$

$(-1)^{1+1}$

$$adj(\hat{X}) = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}^t \qquad C_{11} = 3 \quad C_{12} = -8 \quad C_{21} = -17 \quad C_{22} = 5$$

$\hat{X} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$ $\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$ $\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$ $\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix}^t = \begin{pmatrix} 3 & -17 \\ -8 & 5 \end{pmatrix}$$

$$\Rightarrow \hat{X}^{-1} = |\hat{X}|^{-1} adj(\hat{X}) = 3\begin{pmatrix} 3 & -17 \\ -8 & 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 9 & -51 \\ -24 & 15 \end{pmatrix} \bmod 26 = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}$$

$$K = \hat{X}^{-1}\hat{Y} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 137 & 147 \\ 60 & 77 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 & 17 \\ 8 & 25 \end{pmatrix}$$

גבוה

$\cdot K = \begin{pmatrix} 7 & 17 \\ 8 & 25 \end{pmatrix}$ וזה מטריצה הפיכה מעל $\mathbb{Z}_{26}$

מעולה אז נמשיך:

כלומר $Y_1 = X_1 K$?

$$(15 \quad 16) = (5 \quad 17)\begin{pmatrix} 7 & 17 \\ 8 & 25 \end{pmatrix}$$

$$(15 \quad 16) = (35+136 \quad 85+425) \bmod 26$$

$$= (15 \quad 16) \checkmark$$

$$P_{X_1}(x_1) = P(X_1 = x_1).$$

ונסמן x_1 את ערכי ה-X_1 האפשריים ו $P_{X_1}(x_1)$ מוגדרת P_{X_1} עבור x_1 שעבורם X_1 מקבל ערך חיובי.

$Y(x)$ מתאים X וקטור מקרי שרכיביו הם פונקציות מרכיבי X ו y מתאים x כך ש $y = Y(x)$.

כלומר, y_1 מתאים x_1 אם $y_1 = Y_1(x_1, x_2, \ldots, x_n)$ וכך הלאה עבור $y_2, \ldots, y_n$.

$$X = (X_1, X_2, \ldots X_n) \xrightarrow{\text{ערך של } X} Y(x) = \{g_{x_1}(x_1), g_{x_2}(x_2), \ldots g_{x_n}(x_n)\}$$

$x \in X$ מערכים של המרחב שבו הוקטור מקבל ערכים.

מרחב מדגם / מרחב הסתברות

מרחב מדגם (מרחב מדגם בדיד)

מרחב מדגם Ω של ניסוי מקרי הוא קבוצה $\Omega = \{x_1, x_2, \ldots, x_n\}$ כך שכל תוצאה אפשרית של הניסוי מתאימה לאיבר יחיד ב Ω.

1- $\mathcal{A} = \{A_1, A_2, \ldots A_n\}$ מרחב המאורעות של מרחב מדגם בדיד הוא קבוצת כל תתי הקבוצות של Ω.

– פונקציית ההסתברות של מרחב מדגם בדיד היא $P_X(x)$

$$P_X(x) = P(X = x)$$

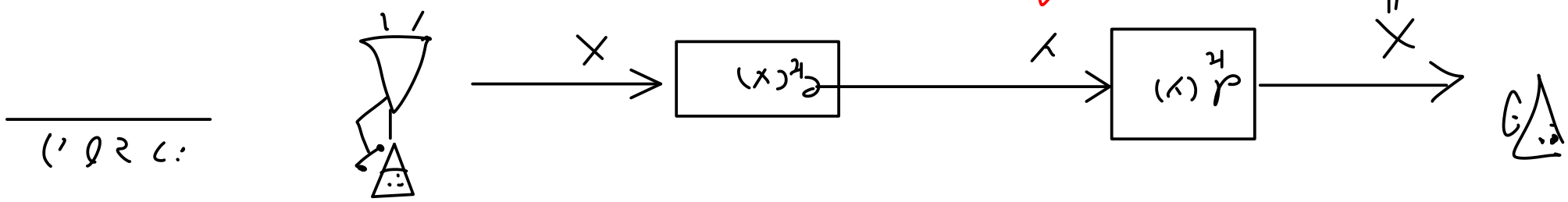
לדוגמה: $P_X(e) = 0.127$ - כאשר e מייצג את האות 'e' בשפה האנגלית.

$Q_{k_1}(X=\alpha) = 1$

$Q_{k_2}(b) = 3$

$Q_{k_3}(\alpha) = 3.$

k	X	α	b
k_1	1	2	
k_2	2	3	
k_3	3	q	



$$P(Y=y) = \sum_{k \in K} P(K=k) \cdot P(X = d_k(y))$$

דוגמה

נתון הקוד $\{00, 01, 10, 11\}$ מעל $\{0,1\}$ ונתון $p = 0.1$.

$X = x$ נשלח ומתקבל $Y = y$ (בשידור מעל ערוץ סימטרי חסר זכרון).

$$P(Y=y \mid X=x) = \sum_{k \in K,\ x = d_k(y)} P(K=k).$$

לכן המסנצ'ת יהיו צפנים, הקבוצת טקסט גלוי היא:

$$X = \{a, b\}$$

הקבוצת המפתחות היא:

$$K = \{k_1, k_2, k_3\}$$

הקבוצת טקסט מוצפן:

$$Y = \{1, 2, 3, 4\}$$

נתונה פונקצית ההסתברות:

$$P_X(a) = \frac{1}{4}, \quad P_X(b) = \frac{3}{4}.$$

ונתונה פונקצית ההסתברות של K:

$$P_K(k_1) = \frac{1}{2}, \quad P_K(k_2) = \frac{1}{4}, \quad P_K(k_3) = \frac{1}{4}.$$

חשבו את פונק"ת ההסתברות של Y.

פתרון

נוסחת ההסתברות השלמה

$$P_y(y) = \sum_{\omega \in \Omega} P(x = d_\omega(y)) \, P_\omega(\omega)$$

$$P_y(1) = \sum_{\omega \in \Omega} P_x(x = d_\omega(1)) \, P_\omega(\omega)$$

$$= P_x(x = d_{\omega_1}(1)) P_\omega(\omega_1) + P_x(x = d_{\omega_2}(1)) P_\omega(\omega_2) + P_x(x = d_{\omega_3}(1)) P_\omega(\omega_3)$$

$P(x=a)$ $P(x=\phi)$ $P(x=\phi)$

ω \ x	a	b
ω_1	1	2
ω_2	2	3
ω_3	3	4

$d_{\omega_1}(1) = a \Rightarrow P(x = d_{\omega_1}(1)) = P(x=a) = \frac{1}{4}$

$d_{\omega_2}(1) = \phi \Rightarrow P(x = d_{\omega_2}(1)) = P(\phi) = 0$

$d_{\omega_3}(1) = \phi \Rightarrow P(x = d_{\omega_3}(1)) = P(\phi) = 0.$

$$P_y(y=1) = P_x(a) P_\omega(\omega_1) + P_x(\phi) P_\omega(\omega_2) + P_x(\phi) P_\omega(\omega_3)$$

$$= \frac{1}{4} \cdot \frac{1}{2} + 0 \cdot \frac{1}{4} + 0 \cdot \frac{1}{4} = \frac{1}{8}$$

$P_y(1) = \frac{1}{8}$ $P_y(2) = ?$ $P_y(3) = ?$ $P_y(4) = ?$

π \ X	a	b
π_1	1	2
π_2	2	3
π_3	3	4

$d_{\pi_1}(2) = b$ $\quad$ $d_{\pi_1}(3) = \phi$

$d_{\pi_2}(2) = a$ $\quad$ $d_{\pi_2}(3) = b$

$d_{\pi_3}(2) = \phi$ $\quad$ $d_{\pi_3}(3) = a$

$$P_y(2) = P(x = d_{\pi_1}(2))\, p_\pi(\pi_1) + P(x = d_{\pi_2}(2))\, p_\pi(\pi_2) + P(x = d_{\pi_3}(2))\, p_\pi(\pi_3)$$

$$= P(x = b)\, p_\pi(\pi_1) + P(x = a)\, p_\pi(\pi_2) + P(x = \phi)\, p_\pi(\pi_3)$$

$$= \frac{3}{4}\cdot\frac{1}{2} + \frac{1}{4}\cdot\frac{1}{4} + 0\cdot\frac{1}{4} = \frac{7}{16}$$

$$P_y(3) = P(x = d_{\pi_1}(3))\, p_\pi(\pi_1) + P(x = d_{\pi_2}(3))\, p_\pi(\pi_2) + P(x = d_{\pi_3}(3))\, p_\pi(\pi_3)$$

$$= P(x = \phi)\, p_\pi(\pi_1) + P(x = b)\, p_\pi(\pi_2) + P(x = a)\, p_\pi(\pi_3)$$

$$= 0\cdot\frac{1}{2} + \frac{3}{4}\cdot\frac{1}{4} + \frac{1}{4}\cdot\frac{1}{4} = \frac{1}{4}.$$

$P_y(4) = 1 - \frac{1}{4} - \frac{7}{16} - \frac{1}{8} = \frac{3}{16}$. , $P_y(3) = \frac{1}{4}$, $P_y(2) = \frac{7}{16}$, $P_y(1) = \frac{1}{8}$ $\quad$ $\therefore \Lambda$