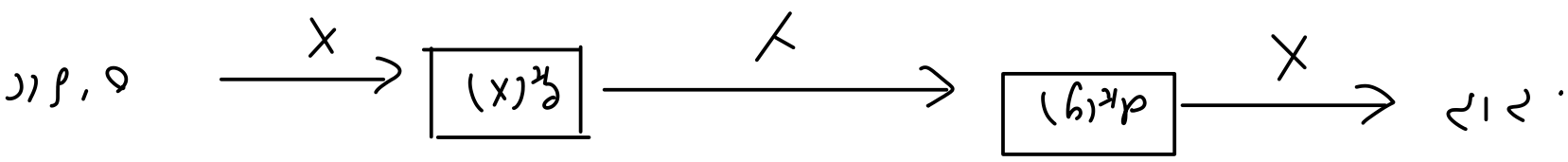
$$y = e_k(x) \qquad d_k(y) = x$$



ثانيا: نظام التشفير المتماثل

المفتاح السري

المفتاح العام

$X = \{x_1, x_2, \ldots, x_n\}$ مجموعة من الرسائل الممكنة : 5 نقاط

$Y = \{y_1, \ldots, y_m\}$ مجموعة من الشفرات الممكنة؛

$K = \{k_1, \ldots, k_p\}$ مجموعة مفاتيح التشفير المستخدمة

(Morse code) . نظام مورس للشفرات : 5 نقاط

اختر الإجابة الصحيحة فيما يلي: 10 نقاط

1. يعتمد نظام التشفير المتماثل على:
   ① مفتاح عام ② مفتاح خاص ③ مفتاح سري ④ لا شيء مما سبق

2. في نظام التشفير غير المتماثل، يُستخدم المفتاح العام لـ:
   ① فك التشفير ② التشفير ③ التوقيع ④ التحقق

3. أي من التالي يُعد نظام تشفير متماثل؟
   ① RSA ② ElGamal ③ DES ④ Diffie-Hellman

4. في نظام التشفير غير المتماثل، المفتاح الخاص يُستخدم لـ:
   ① التشفير ② التحقق ③ فك التشفير ④ التوقيع

5. أي من التالي يُعد نظام تشفير غير متماثل؟
   ① DES ② AES ③ RSA ④ Blowfish

6. ما هو الهدف الرئيسي من التشفير؟
   ① ضغط البيانات ② تسريع الإرسال ③ حماية سرية المعلومات ④ تقليل حجم الملف

שאלה 3 נתונים שני המשתנים X ו-Y ופונקציית ההסתברות המשותפת $P_{XY}(x,y)$ שלהם, כפי שמוצגת בטבלה הבאה:

X \ Y	k_1	k_2	k_3
a	5	1	1
b	1	1	1

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

$P_Y(k_1) = \frac{1}{2}$ $P_Y(k_2) = P_Y(k_3) = \frac{1}{4}$.

א. חשבו את פונקציית ההסתברות המותנית $P_{Y|X}(y|x)$ של Y בהינתן X.

ב. חשבו את פונקציית ההסתברות השולית $P_Y(y)$ של המשתנה Y.

$$P_Y(y) = \sum_{x \in X} P(X=x) P(Y=y|X=x)$$

ג. חשבו את התוחלת $E(Y)$ של המשתנה Y.

ד. חשבו את $P(X=x|Y=y)$ עבור $x=a$ ו-$y=k_1$.

$$P(Y=s) = P(H=h_1)P(X=\underbrace{\lambda_{h_1}(s)}_{a}) + P(H=h_2)P(X=\underbrace{\lambda_{h_2}(s)}_{\phi}) + P(H=h_3)P_X\underbrace{(\lambda_{h_3}(s))}_{\phi}$$

$$= P_H(h_1)\ P(X=a) = \frac{1}{2}\cdot\frac{1}{4} = \frac{1}{8}.$$

H \ X	a	b
h_1	S	T
h_2	T	U
h_3	U	V

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

$P_H(h_1) = \frac{1}{2}$ $\quad P_H(h_2) = P_H(h_3) = \frac{1}{4}$.

$$P(Y=y) = \sum_{h\in\{h_1,h_2,h_3\}} P(H=h)\cdot P(X=\lambda_h(y))$$

$\lambda_{h_1}(U) = \phi$ $\quad \lambda_{h_2}(U) = b$ $\quad \lambda_{h_3}(T) = \phi$ $\quad \lambda_{h_3}(S) = \phi$

$\lambda_{h_1}(V) = \phi$ $\quad \lambda_{h_2}(V) = \phi$ $\quad \lambda_{h_3}(U) = a$ $\quad \lambda_{h_3}(V) = b$

H \ X	a	b
h_1	S	T
h_2	T	U
h_3	U	V

$\varepsilon_{h_1}(a) = S$ $\quad \varepsilon_{h_1}(b) = T$

$\varepsilon_{h_2}(a) = T$ $\quad \varepsilon_{h_2}(b) = U$

$\varepsilon_{h_3}(a) = U$ $\quad \varepsilon_{h_3}(b) = V$

$\lambda_{h_1}(S) = a$ $\quad \lambda_{h_2}(S) = \phi$.

$\lambda_{h_1}(T) = b$ $\quad \lambda_{h_2}(T) = a$

(18 נק')

נתון מסווג בייסיאני תמים עם מרחב המצבים

$X = \{a,b\}$

ומרחב ההשערות H הבא:

$H = \{h_1, h_2, h_3\}$

כך ש-h_1 הוא המסווג הבייסיאני האופטימלי.

$Y = \{S, T, U, V\}$

H \ X	a	b
h_1	S	T
h_2	T	U
h_3	U	V

$\varepsilon_{h_1}(a) = S$ $\quad \varepsilon_{h_1}(b) = T$

$\varepsilon_{h_2}(a) = T$ $\quad \varepsilon_{h_2}(b) = U$

$\varepsilon_{h_3}(a) = U$ $\quad \varepsilon_{h_3}(b) = V$

$\lambda_{h_1}(S) = a$ $\quad \lambda_{h_2}(S) = \phi$.

$\lambda_{h_1}(T) = b$ $\quad \lambda_{h_2}(T) = a$

K \ X	a	b
k_1	S	T
k_2	T	U
k_3	U	V

$$P_X(a) = \frac{1}{4} \qquad P_X(b) = \frac{3}{4}$$

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

$$P(Y=y) = \sum_{k \in \{k_1,k_2,k_3\}} P(K=k) \cdot P(X = d_k(y))$$

$$P(Y=T) = P_K(k_1) P_X(\overbrace{d_{k_1}(T)}^{b}) + P_K(k_2) P_X(\overbrace{d_{k_2}(T)}^{a}) + P_K(k_3) P_X(\overbrace{d_{k_3}(T)}^{\phi})$$

$$= P_K(k_1) P_X(b) + P_K(k_2) P_X(a)$$

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

$$P(Y=U) = P_K(k_1) P_X(\overbrace{d_{k_1}(U)}^{\phi}) + P_K(k_2) P_X(\overbrace{d_{k_2}(U)}^{b}) + P_K(k_3) P_X(\overbrace{d_{k_3}(U)}^{a})$$

$$= P_K(k_2) P_X(b) + P_K(k_3) P_X(a) = \frac{1}{4} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{4}.$$

$$P(Y=V) = P_K(k_1) P_X(\overbrace{d_{k_1}(V)}^{\phi}) + P_K(k_2) P_X(\overbrace{d_{k_2}(V)}^{\phi}) + P_K(k_3) P_X(\overbrace{d_{k_3}(V)}^{b})$$

$$= P_K(k_3) P_X(b) = \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16}$$

$$\boxed{P_Y(S) = \frac{1}{8}, \quad P_Y(T) = \frac{7}{16} \qquad P_Y(U) = \frac{1}{4}, \quad P_Y(V) = \frac{3}{16}}$$

$$P_Y(S) + P_Y(T) + P_Y(U) + P_Y(V) = \frac{2}{16} + \frac{7}{16} + \frac{4}{16} + \frac{3}{16} = 1. \ \text{☺}$$

$P(Y=S \mid X=a)$.

$$P(Y=S \mid X=a) = \sum_{\substack{k \in (k_1,k_2,k_3) \\ a = d_k(S)}} P(K=k)$$

$$= P(K=k_1) = \frac{1}{2}.$$

K \ X	a	b
k_1	S	T
k_2	T	U
k_3	U	V

$$P(Y=S \mid X=b) = \sum_{\substack{k\in(k_1,k_2,k_3)\\ d_k(b)=T}} P_k(k) = P_k(k_1) = \frac{1}{3}$$

$$P(Y=U \mid X=a) = \sum_{\substack{k\in(k_1,k_2,k_3)\\ a=d_k(U)}} P_k(k) = P(k=k_3) = \frac{1}{4}$$

הוכחה של סודיות מושלמת

נתון הצפנה כלשהי מעל X והתפלגות כלשהי Y

הוכיחו שלמערכת יש סודיות מושלמת אם ורק אם מתקיים

$$P(X=x \mid Y=y) = P(X=x) \qquad (1)$$

לכל $x\in X$, ולכל $y\in Y$.

הוכחה: אם לקריפטו-מערכת יש סודיות מושלמת אז

$$P(Y=y \mid X=x) = P(Y=y) \qquad (2)$$

הוכחה: נתון שלמערכת יש סודיות מושלמת. ע״פ הגדרה, לכל x ולכל y מתקיים (1)

$$P(X=x \mid Y=y) = P(X=x)$$

כמו כן, לפי הגדרת הסתברות מותנית: $P(A \mid B) = \frac{P(A\cap B)}{P(B)}$

לכן

$$P(X=x \mid Y=y) = \frac{P(X=x \cap Y=y)}{P(Y=y)}$$

לפי זה נציב במשוואה (1):

$$\frac{P(X=x \cap Y=y)}{P(Y=y)} = P(X=x)$$

נכפיל את שני האגפים ב-$P(Y=y)$:

$$P(X=x \cap Y=y) = P(X=x)\,P(Y=y)$$

נחלק את שני האגפים ב-$P(X=x)$:

$$\frac{P(X=x \cap Y=y)}{P(X=x)} = P(Y=y)$$

ולפי הגדרה:

$$\frac{P(X=x \cap Y=y)}{P(X=x)} = P(Y=y \mid X=x)$$

לכן:

$$P(Y=y \mid X=x) = P(Y=y)$$

מ.ש.ל.

$$P(Y=V)=\sum_{x}\left(\lambda_{h_1}(V)\right)P_{L_2}(h_1)+P_X\left(\lambda_{L_2}(V)\right)P_{L_2}(h_2)+P_X\left(\lambda_{L_3}(V)\right)P_{L_2}(h_3)$$

$$=P_X(a)P_{L_2}(h_1)+P_X(c)P_{L_2}(h_2)=\frac{3}{5}\cdot\frac{1}{6}+\frac{1}{3}\cdot\frac{2}{5}=\frac{7}{30}$$

$$P(Y=\xi)=\sum_{x}\left(\lambda_{h_1}(z)\right)P_{L_2}(h_1)+P_X\left(\lambda_{L_2}(z)\right)P_{L_2}(h_2)+P_X\left(\lambda_{L_3}(z)\right)P_{L_2}(h_3)$$

$$=P_X(a)P_{L_2}(h_2)+P_X(c)P_{L_2}(h_3)=\frac{3}{5}\cdot\frac{1}{3}+\frac{2}{5}\cdot\frac{1}{2}=\frac{2}{5}$$

$$P(Y=W)=1-P_Y(U)-P_Y(V)=1-\frac{1}{15}-\frac{7}{30}-\frac{2}{5}=\frac{9}{30}=\frac{3}{10}$$

X / h_3	Z	W
h_2	V	Z
h_1	U	V
h	c	a

$$P(X=c\mid Y=Z)$$ מה הסיכוי ש

שאלה 1/3/15 ב. מבחן א – לכלכלה ב' | תשובות בעמוד הבא

שאלה 1 (40 נקודות) משקל ממוצע של תינוקות שנולדו בבית חולים מסוים הוא 3.5 ק"ג. סטיית התקן של משקל התינוקות היא 0.5 ק"ג. נניח כי משקל התינוקות מתפלג נורמלית.

א. מהו הסיכוי שתינוק שנולד בבית החולים ישקול יותר מ-4 ק"ג?

ב. מהו הסיכוי ששני תינוקות שנולדו בבית החולים ישקלו יחד יותר מ-8 ק"ג?

ג. מהו הסיכוי ששלושה תינוקות שנולדו בבית החולים ישקלו יחד יותר מ-10.5 ק"ג?

ד. מהו הסיכוי שמתוך 100 תינוקות שנולדו בבית החולים, יותר מ-20 יישקלו פחות מ-3 ק"ג?

ה. מהו הסיכוי שמתוך 100 תינוקות שנולדו בבית החולים, בדיוק 20 ישקלו פחות מ-3 ק"ג?

ו. מהו הסיכוי שמתוך 100 תינוקות שנולדו בבית החולים, בין 20 ל-30 ישקלו פחות מ-3 ק"ג?

שאלה 2 (40 נקודות) נתונים שני משתנים מקריים X ו-Y בעלי פונקציית ההסתברות המשותפת הבאה:

X / h_3	Z	W
h_2	V	Z
h_1	U	V
h	c	a

$$P_X(c)=\frac{2}{5}\qquad P_X(a)=\frac{3}{5}$$

$$P_{L_2}(h_1)=\frac{1}{6}\qquad P_{L_2}(h_2)=\frac{1}{3}$$

$$P_{L_2}(h_3)=\frac{1}{2}$$

X / h_3	Z	W
h_2	V	Z
h_1	U	V
h	c	a

$$P_Y$$ חשבו את פונקציית ההסתברות השולית של Y.

ג) $P(X=c \mid Y=z)$

k	c	X
k_1	U	V
k_2	V	Z
k_3	z	w

$$P(Y=z \mid X=c) = \frac{\sum_{k_1,k_2,k_3} P_k(k)}{\partial_k(z)=c}$$

$$= P_k(k_3) = \frac{1}{2}.$$

$$P(B \mid A) = \frac{P(A \mid B)\,P(B)}{P(A)}$$

$$P(X=c \mid Y=z) = \frac{P(Y=z \mid X=c)\,P(X=c)}{P(Y=z)} = \frac{\frac{1}{2}\cdot\frac{2}{5}}{\frac{2}{5}} = \frac{1}{2}$$

ד) $c, x \in X$ כך ש $y \in Y$ עבורם $P(X=x \mid Y=y) = P(X=x)$ (המשך בעמוד הבא)

ה) $P(X=c) = \frac{2}{5}$ לכל c ו $P(X=c \mid Y=z) = \frac{1}{2}$ לכל c, z כך ש $P(X=c) \neq 0$ ו $P(Y=z) \neq 0$.

$$P(X=c \mid Y=z) = \frac{P(Y=z \mid X=c)\,P(X=c)}{P(Y=z)} = \frac{\left(\frac{1}{2}\right)\left(\frac{2}{5}\right)}{\left(\frac{2}{5}\right)} = \frac{1}{2}$$

משפט שאנון (Shannon's law)

נתון צופן (P,C,K,E,D) שבו $|P|=|C|=|K|$ ומפתח נבחר אחיד.
צופן כזה הוא מושלם אם ורק אם $\forall x\in P, y\in C$ מתקיים $P(X=x)=P(X=x|Y=y)$.

הוכחה:

$\Leftarrow$ נניח שהצופן מושלם. אז $\forall x\in P, y\in C$ מתקיים $P(X=x)=P(X=x|Y=y)$.

$\Rightarrow$ נניח שהצופן מושלם. נחשב $P(Y=y)$:

$$P(Y=y)=\sum_{k\in K} P(K=k)\,P(X=D_k(y))$$

לכל $x\in P$ נגדיר $C(x)=\{k\in K : \exists y\in C,\ E_k(x)=y\}$.

טענה: $|C(x)|=|C|$ לכל $x\in P$.

הוכחה: נניח בשלילה ש-$|C(x)|<|C|$. אז קיים $y\in C$ כך ש-$y\notin C(x)$. לכן $P(X=x|Y=y)=0$ כי אין מפתח שמצפין את x ל-y. אבל $P(X=x)>0$ (כי x מופיע בטקסט גלוי), בסתירה לכך שהצופן מושלם. $\square$

מכאן נובע ש-$|K|\geq|C|$. אבל $|K|=|C|$, לכן $|C(x)|=|K|$ לכל x.

מכאן נובע שלכל $x\in P$ ולכל $y\in C$ קיים מפתח יחיד k כך ש-$E_k(x)=y$.

לכן:

$$P(Y=y)=\sum_{k\in K} P(K=k)\,P(X=D_k(y))=\frac{1}{|K|}\sum_{k\in K} P(X=D_k(y))$$

$$=\frac{1}{|K|}\sum_{x\in P} P(X=x)=\frac{1}{|K|}\cdot 1=\frac{1}{|K|}$$

כאשר המעבר האחרון נובע מכך שכל x מופיע בסכום בדיוק פעם אחת (עבור המפתח היחיד k כך ש-$E_k(x)=y$).

מצד שני, $P(Y=y)=\frac{1}{|K|}$ לכל y, כלומר Y מתפלגת אחיד.

$$P(X=x|Y=y)=\frac{P(X=x)\,P(Y=y|X=x)}{P(Y=y)}$$

$$=\frac{P(X=x)\cdot\sum_{k:E_k(x)=y} P(K=k)}{\frac{1}{|K|}}$$

$$=P(X=x)\cdot|K|\cdot\frac{1}{|K|}=P(X=x)$$

כלומר $P(X=x)=P(X=x|Y=y)$ לכל x,y, כנדרש. $\square$

דוגמה: נניח $P=\{0,1,2,\dots,25\}$ ונגדיר $E_k(x)=x+k \bmod 26$.

כלל הצפנה: $e_k(x)=x+k \bmod 26$.

כלל הפענוח: $d_k(y)=y-k \bmod 26$.

נניח שהמפתח k נבחר אחיד מתוך $\{0,1,2,\dots,25\}$.

נניח שהטקסט הגלוי הוא $x=23$ ($=$ "X").

נניח $k=9$.

$$e_k(x)=e_9(23)=23+9 \bmod 26=32 \bmod 26=6$$

$$\Longrightarrow y=6 \longrightarrow \text{"G"}$$

$$d_k(y)=d_9(6)=6-9 \bmod 26=-3 \bmod 26=23 \longrightarrow \text{"X"}$$

כלומר, אם הטקסט הגלוי הוא "X" והמפתח הוא 9, אז הטקסט המוצפן הוא "G".

חישוב $P(Y=y)$:

$$P(Y=y)=\sum_{k\in K} P(K=k)\,P(X=D_k(y))$$

$$=\frac{1}{26}\sum_{k\in K} P(X=D_k(y))$$

$$=\frac{1}{26}\left[P(X=D_0(y))+P(X=D_1(y))+\dots+P(X=D_{25}(y))\right]$$

$$=\frac{1}{26}\left[P(X=y)+P(X=y-1)+\dots+P(X=y-25)\right]$$

$$=\frac{1}{26}\sum_{k\in K} P(X=y-k)$$

$$=\frac{1}{26}\cdot 1=\frac{1}{26}$$

כאשר המעבר האחרון נובע מכך שכל x מופיע בסכום בדיוק פעם אחת (עבור המפתח היחיד k כך ש-$E_k(x)=y$).

מכאן נובע ש-$P(Y=y)=\frac{1}{26}$ לכל y, כלומר Y מתפלגת אחיד.

חישוב $P(X=x|Y=y)$:

$$P(X=x|Y=y)=\sum_{k:E_k(x)=y} P(K=k)$$

$$=\sum_{k:E_k(x)=y}\frac{1}{26}$$

$$=\frac{1}{26}\cdot|\{k : E_k(x)=y\}|$$

$$=\frac{1}{26}\cdot 1=\frac{1}{26}$$

כאשר המעבר האחרון נובע מכך שיש בדיוק מפתח אחד k כך ש-$E_k(x)=y$.

מכאן נובע ש-$P(X=x|Y=y)=\frac{1}{26}$ לכל x,y.

מסקנה: $P(X=x)=P(X=x|Y=y)=\frac{1}{26}$ לכל x,y, כלומר הצופן מושלם.

$x = d_k(y)$,(1 נכון) אם ורק אם

$k = y - x \bmod 26$ $\Leftarrow$ $x = y - k \bmod 26$ $\Leftarrow$

לכן גם אם k נבחר באופן אחיד

$$P(Y=y \mid X=x) = \sum_{k \in (0,\dots,25)} P(k = y-x)$$

נסמן $k = y - x$ ונקבל שכל איבר בסכום הוא

$$P(Y=y \mid X=x) = P(k = y-x) = \frac{1}{26} \quad (5)$$

לכן, בלי תלות ב-x

$$P(Y=y) = \frac{1}{26} = P(Y=y \mid X=x)$$

כלומר, X ו-Y הם משתנים