```
הצפנה סימטרית: תהיינה \mathcal{K} \times \mathcal{C} \to \mathcal{M} אזי חופיות תהא \mathcal{K} \times \mathcal{C} \to \mathcal{M} אזי \mathcal{K} \times \mathcal{C} \to \mathcal{M} המקיימת \mathcal{K} \times \mathcal{C} \to \mathcal{K} ולכל \mathcal{K} \in \mathcal{K} מרחב המפתחות בהצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \to \mathcal{K} הצפנה סימטרית אזי \mathcal{K} \times \mathcal{K}. מרחב הקידודים/ההצפנות בהצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \to \mathcal{K} הצפנה סימטרית אזי \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} הצפנה סימטרית: תהא \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K}
```

L(m) = E(h,m) איניים פוני סיבוט יונ. יווא (K,Nt,C,E,D) ווצפנוז סיבוט יונ אוL(m) = E(h,m) איניים פוני L(m) = E(h,m) איניים פוני L(m) = E(h,m)

 $E_k\left(m
ight)=E\left(k,m
ight)$  אזי  $m\in\mathcal{M}$  ויהי אויה אויה אויהעפנה סימטרית הצפנה סימטרית הא הצפנה  $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$  איזי

D אזי סימטרית אזי ( $\mathcal{K},\mathcal{M},\mathcal{C},E,D$ ) אהא חימטרית: פונקציית פענוח הימטרית: תהא

 $D_k\left(c
ight)=D\left(k,c
ight)$  אזי  $c\in\mathcal{C}$  ווהי א ויהי הי אצפנה סימטרית הצפנה  $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$  אחי

. ידועים. מכאן והלאה נסמן הצפנה סימטרית בעזרת (E,D) הערה: מכאן הצפנה סימטרית הצפנה הצפנה מכאן והלאה נסמן הצפנה מימטרית בעזרת

 $\mathbb{Z}_n^{\leq m} = igcup_{i=0}^m \mathbb{Z}_n^i$  נגדיר  $n,m \in \mathbb{N}_+$  יהיו סימון: יהיו

עופן קיסר: יהיו  $m,m\in\mathbb{N}_+$  נגדיר  $n,m\in\mathbb{N}_+$  כך צופן קיסר: יהיו

- $i \in [|x|]$  לכל  $(E_k(x))_i = (x_i + k) \% n$
- $i \in [|c|]$  לכל  $(D_k(c))_i = (c_i k) \% n$

טענה: יהיו אזי צופן אזי אוי אופן  $n,m\in\mathbb{N}_+$  יהיו יהיו

בך  $E,D:[n!] imes\mathbb{Z}_{n-1}^{\leq m} o \mathbb{Z}_{n-1}^{\leq m}$  בדיר שונות נגדיר  $f_1,\dots,f_{n!}:[n] o [n]$  ותהיינה ותהיינה  $n,m\in\mathbb{N}\setminus\{0,1\}$ 

- $.i\in \left[\left|m
  ight|
  ight]$  לכל  $\left(E_{k}\left(x
  ight)
  ight)_{i}=f_{k}\left(x_{i}
  ight)$
- $.i\in\left[\left|c\right|
  ight]$  לכל  $\left(D_{k}\left(c
  ight)
  ight)_{i}=f_{k}^{-1}\left(c_{i}
  ight)$

. טענה: הינה הצפנה הינה הצפנה אזי אופן שונות הפיכות הפיכות  $n,m\in\mathbb{N}\setminus\{0,1\}$  יהיי טענה: יהיו היינה  $n,m\in\mathbb{N}\setminus\{0,1\}$ 

בום  $E,D:\mathbb{Z}_n^m imes\mathbb{Z}_n^m o\mathbb{Z}_n^m$  נגדיר  $n,m\in\mathbb{N}_+$  יהיו צופן ויז'נר: יהיו

- $i \in [|x|]$  לכל  $(E_k(x))_i = (x_i + k_i) \% n$
- $i \in [|c|]$  לכל  $(D_k(c))_i = (c_i k_i) \% n$

נגדיר  $m'\in\mathcal{M}$  ותהא  $k'\in\mathcal{K}$  ותהא המילים שכיחויות המילים שכיחויות המילים ווהא  $\mu:\mathcal{M}\to[0,1]$  ותהא התקפה נגדיר ווהא  $c=E_{k'}\left(m'\right)$ 

```
 \begin{split} & \text{function GenericAttack}((E,D)\,,\mu,c) \text{:} \\ & \quad \ell \leftarrow \mathcal{M} \\ & \quad p \leftarrow [0,1] \\ & \quad \text{for } k \leftarrow \mathcal{K} \text{ do} \\ & \quad \mid \quad m \leftarrow D(k,c) \\ & \quad \mid \quad \text{if } \mu(m) > p \text{ then } (\ell,p) \leftarrow (m,\mu(m)) \\ & \quad \text{end} \\ & \quad \text{return } \ell \end{split}
```

 $\mathbb{P}_{a\leftarrow\mu}\left(a
ight)=\mu\left(a
ight)$  אזי התפלגות הא  $\mu:\Omega
ightarrow\left[0,1
ight]$  תהא קבוצה סופית תהא

 $\mathbb{P}_{a\leftarrow\Omega}\left(a
ight)=rac{1}{\left|\Omega
ight|}$  אימון: תהא  $\Omega$  קבוצה סופית אי

 $c\in\mathcal{C}$  ולכל  $\mu:\mathcal{M} o [0,1]$  אבורה לכל התפלגות עבורה פימטרית. הצפנה סימטרית בעלת מודיות מושלמת: הצפנה סימטרית עבורה לכל התפלגות  $\mu:\mathcal{M} o [0,1]$  אבורה לכל התפלגות בעלת סודיות מושלמת: הצפנה סימטרית  $\mathbb{P}_{m\leftarrow\mu}$   $(m=a)=\mathbb{P}_{(m,k)\leftarrow(\mu,\mathcal{K})}$   $(m=a\mid c=E_k(m))$  מתקיים

מתקיים  $c\in\mathcal{C}$  ולכל  $a,b\in\mathcal{M}$  ולכל עבורה לכל עבורה אצפנה סימטרית הצפנה חוסר הבחנה מושלם: הצפנה הצפנה הצפנה הימטרית בעלת חוסר הבחנה מושלם:

 $\mathbb{P}_{k \leftarrow \mathcal{K}} \left( E_k \left( a \right) = c \right) = \mathbb{P}_{k \leftarrow \mathcal{K}} \left( E_k \left( b \right) = c \right)$ 

.(בעלת חוסר הבחנה הבחנה מושלם). בעלת סודיות מושלמת) בעלת הבחנה מימטרית אזי הבחנה מושלם ((E,D)) בעלת הצפנה סימטרית אזי

בום פנקס חד־פעמי: יהי  $n\in\mathbb{N}$  נגדיר  $E,D:\left\{0,1
ight\}^n imes\left\{0,1
ight\}^n$  כך צופן פנקס חד־פעמי: יהי

- $.E_k(m) = m \oplus k \bullet$ 
  - $.D_{k}\left( c\right) =c\oplus k$  •

משפט: יהי אזי צופן פנקס חד־פעמי הינה הצפנה סימטרית צופן פנקס אזי צופן פנקס משפט: יהי  $n\in\mathbb{N}$ 

 $|\mathcal{M}| \leq |\mathcal{K}|$  משפט שאנון: תהא (E,D) הצפנה סימטרית בעלת סודיות מושלמת אזי

. טענה: יהי בעלת סודיות מושלמת הינה הצפנה הינה אזי צופן קיסר  $m\in\mathbb{N}_+$  יהי יהי

משחק חוסר ההבחנה: יהיו  $\mathcal{W},\mathcal{A}$  שחקנים אזי

```
game IndistinguishabilityGame((E, D), W, A):
         \mathcal{A} chooses messages m_0, m_1 \in \mathcal{M}
          \mathcal{W} samples key k \leftarrow \mathcal{K}
          \mathcal{W} samples bit b \leftarrow \{0, 1\}
          \mathcal{W} sends E(k, m_b) to \mathcal{A}
          \mathcal{A} prints a bit b'
          if b' = b then
           return \mathcal{A} won
          return A lost
    (E,D) מעצחת במשחק חוסר ההבחנה מושלם) בעלת חוסר הבחנה בעלת אזי בעלת אזי ((E,D) בעלת בעלת הבחנה) משפט: תהא
                                                                                                                                                                                                                               \mathcal{A} יריב: משפחת מעגלים בוליאניים
                                                                                                                                                                                                                                                            \hat{\mathbb{N}} = \mathbb{N} \cup \{\infty\} סימון:
                                                                                                                       .Size (\mathcal{A})=\mathcal{O}\left(t\left(n
ight)
ight) עבורו \mathcal{A} אזי יריב בעל כוח חישוב: תהא \hat{\mathbb{N}}
                      \Delta_{\mathcal{A}}\left(X,Y
ight)=\left|\mathbb{P}_{x\leftarrow X}\left(\mathcal{A}\left(x
ight)=1
ight)-\mathbb{P}_{y\leftarrow Y}\left(\mathcal{A}\left(y
ight)=1
ight)
ight| איי \{0,1\}^* איי איינה X,Y התפלגויות על
התפלגויות בלתי ניתנות להבחנה (בנ"ל): יהי arepsilon \geq 0 ותהא t: \mathbb{N} 	o \hat{\mathbb{N}} אזי התפלגויות איי עבורן לכל יריב \mathcal{A} בעל כוח arepsilon \geq 0 בעל כוח
                                                                                                                                                                                                                                 \Delta_{\mathcal{A}}(X,Y) \leq \varepsilon חישוב t מתקיים
                                                                                                                  X pprox_{t,arepsilon} Y תהא בנ"ל אזי t: \mathbb{N} 	o \hat{\mathbb{N}} תהא בנ"ל אזי יהי ותהיינה t: \mathbb{N} 	o \hat{\mathbb{N}}
f\left(X
ight)\left(c
ight)= באשר \{0,1\}^* באשר התפלגות על f:\{0,1\}^* 	o \{0,1\}^* ותהא ותהא \{0,1\}^* 	o \{0,1\}^* אזי התפלגות על
                                                                                                                                                                                                                                                                  \mathbb{P}_{x \leftarrow X} \left( f \left( x \right) = c \right)
בעלי m,m'\in\mathcal{M} בימטרית בעלת סודיות חישובית: יהי arepsilon\geq 0 ותהא ותהא arepsilon=\mathbb{N} אזי הצפנה סימטרית בעלת סודיות חישובית: יהי arepsilon\geq 0 ותהא
                                                                                                                                                                                                   E(\mathcal{K},m) \approx_{t,\varepsilon} E(\mathcal{K},m') אורך שווה מתקיים
                         (\infty,0) בעלת סודיות חישובית ((E,D)) בעלת סודיות מושלמת) בעלת סודיות חישובית ((E,D)).
                                                                                                                                                                                                               U_n = U\left(\left\{0,1\right\}^n\right) אזי n \in \mathbb{N} סימון: יהי
ניתנת לחישוב G:\{0,1\}^n	o\{0,1\}^\ell אזי \ell>n באשר בשר \ell,n\in\mathbb{N} ויהיו וויהין t:\mathbb{N}	o\hat{\mathbb{N}} תהא arepsilon\geq 0 ניתנת לחישוב ויהי
                                                                                                                                                                                                             G(\{0,1\}^n) \approx_{t,\varepsilon} U_{\ell} בזמן פולינומי עבורה
                                                                                                       . טענה: אם גנרטור פסודאו אקראי. באשר \ell > n באשר אזי לכל \mathcal{P} = \mathcal{NP} טענה: אם
E,D:\{0,1\}^n	imes נגדיר (t,arepsilon) נגדיר פסודאו אקראי (t,arepsilon) צופן פנקט חד־פעמי חישובי: יהיו t,\ell\in\mathbb{N} ויהי ויהי ויהי
                                                                                                                                                                                                                                                             כד \{0,1\}^{\ell} \to \{0,1\}^{\ell}
                                                                                                                                                                                                                                            .E_k(m) = m \oplus G(k) \bullet
                                                                                                                                                                                                                                                 .D_{k}\left( c\right) =c\oplus G\left( k\right)  •
m\in \left\{0,1
ight\}^\ell טענה: יהיו צופן פנקס חד־פעמי חישובי ויהי G: \left\{0,1
ight\}^n 	o \left\{0,1
ight\}^\ell אנרטור פסודאו אקראי מענה: יהיו אופן פנקס חד־פעמי חישובי ויהי
                                                                                                                                                                                                                                            E\left(\left\{0,1\right\}^{n},m\right)\approx_{t\in}U_{\ell} אזי
משפט: יהיו n,\ell\in\mathbb{N} ויהי הינה בעלת חישובי הינה בעלת פסודאו אקראי G:\{0,1\}^n	o\{0,1\}^\ell ויהי ויהי משפט: יהיו
f(X)pprox_{t-{	ext{Size}(f)},arepsilon} איי f:\{0,1\}^*	o\{0,1\}^* ותהא Xpprox_{t,arepsilon} איי תהיינה X,Y התפלגויות עבורן Xpprox_{t-{	ext{Size}(f)},arepsilon} איי x\in\mathbb{N}
                                                                                                                                                                                                                                                                                                  f(Y)
                          X pprox_{t,arepsilon+\delta} Z אזי אזי Y pprox_{t,\delta} Z וכן וכן X pprox_{t,\varepsilon} Y התפלגויות עבורן X pprox_{t,\varepsilon+\delta} Z אזי ותהיינה t: \mathbb{N} \to \hat{\mathbb{N}} התינה \varepsilon,\delta \geq 0
                Xpprox_{\min(t,s),arepsilon+\delta} אזי Ypprox_{s,\delta} וכן Xpprox_{t,arepsilon} ותהיינה t,s:\mathbb{N}\to\hat{\mathbb{N}} ותהיינה t,s:\mathbb{N}\to\hat{\mathbb{N}} ותהיינה t,s:\mathbb{N}\to\hat{\mathbb{N}} ותהיינה t,s:\mathbb{N}\to\hat{\mathbb{N}} ווהי t,s:\mathbb{N}\to\hat{\mathbb{N}} ווחים t,s:\mathbb{N}\to\hat{\mathbb{N} ווחים t,s:\mathbb{N}\to\hat{\mathbb{N}} ווחים t,s:\mathbb{N}\to\hat{\mathbb{N}} ווחים t,s:\mathbb
(E,D) אזי הצפנה סימטרית בעלת סודיות חישובית למספר הודעות: יהי n\in\mathbb{N}_+ יהי יהי חישובית למספר הודעות הצפנה סימטרית בעלת סודיות חישובית למספר הודעות: יהי
                                                                                                 E(\mathcal{K},x) pprox_{t,\varepsilon} E(\mathcal{K},y) מתקיים i \in [n] לכל |x_i| = |y_i| באשר x,y \in \mathcal{M}^n עבורה לכל
```

טענה: יהי  $n\in\mathbb{N}\setminus\{0,1\}$  יהי אזי לא קיימת אזי אזי לא קיימת הצפנה חישובית למספר הודעות.  $arepsilon\geq 0$  ותהא