$(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ אזי $D:\mathcal{K} imes\mathcal{C} o\mathcal{M}$ ותהא $E:\mathcal{K} imes\mathcal{M} o\mathcal{C}$ קבוצות סופיות תהא קבוצת $\mathcal{M},\mathcal{K},\mathcal{C}\subseteq\{0,1\}^*$ אזי המקיימת

 $D\left(k,E\left(k,m
ight)
ight)=m$ מתקיים $m\in\mathcal{M}$ ולכל ולכל $k\in\mathcal{K}$

 \mathcal{K} אזי איי סימטרית בהצפנה סימטרית: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ הצפנה סימטרית

 \mathcal{M} אזי אינת הימטרית הצפנה הימטרית: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ הצפנה הימטרית אזי

 \mathcal{C} אזי אופנה סימטרית האצפנות בהצפנה סימטרית: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ מרחב הקידודים/ההצפנות

E אזי אינת סימטרית הצפנה סימטרית: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ הצפנה סימטרית:

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

D אזי סימטרית פענוח סימטרית: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ הצפנה סימטרית

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

. ידועים. על, $\mathcal{K}, \mathcal{M}, \mathcal{C}$ כי ונניח והלאה מכאן בעזרת בעזרת הצפנה הצפנה הצפנה מכאן והלאה מכאן והלאה מימטרית הערה:

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

כך $E,D:\{0\dots n\} imes \mathbb{Z}_n^{\leq m} o \mathbb{Z}_n^{\leq m}$ נגדיר $n,m\in\mathbb{N}_+$ יהיו יהיו הצפנת קיטר: יהיו

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

טענה: יהיו $n,m\in\mathbb{N}_+$ אזי הצפנת קיסר הינה הצפנה סימטרית.

כך $E,D:[n!] imes\mathbb{Z}_{n-1}^{\leq m} o \mathbb{Z}_{n-1}^{\leq m}$ הפיכות שונות נגדיר $f_1,\dots,f_{n!}:[n] o [n]$ ותהיינה $n,m\in\mathbb{N}ackslash\{0,1\}$ הצפנת הצבה: יהיו

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

. שענה: יהיו $n,m\in\mathbb{N}\setminus\{0,1\}$ הינה הצפנת הינה $f_1,\dots,f_{n!}:[n] o [n]$ ותהיינה $n,m\in\mathbb{N}\setminus\{0,1\}$ היהיו $m'\in\mathcal{M}$ ותהא $m'\in\mathcal{M}$ ותהא $m'\in\mathcal{K}$ ותהא ותהא ותהיינה ותהא ותהיינה ותהי

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

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

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

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

מתקיים מוחה ולכל אורך שווה ולכל $c\in\mathcal{C}$ מתקיים ממטרית בעלת חוסר הבחנה מושלם: הצפנה סימטרית עבורה לכל $a,b\in\mathcal{M}$ עבורה לכל $a,b\in\mathcal{M}$ עבורה אורך שווה ולכל $\mathcal{P}_{k\leftarrow\mathcal{K}}\left(E_{k}\left(a\right)=c\right)=\mathbb{P}_{k\leftarrow\mathcal{K}}\left(E_{k}\left(b\right)=c\right)$

.(בעלת חוסר הבחנה בעלת הושלמת) בעלת בעלת הואינ ((E,D)) בעלת אזי בעלת הבחנה משפט: תהא הצפנה סימטרית אזי

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

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

. משפט: יהי $\mathbb{N} \in \mathbb{N}$ אזי הצפנת פנקס חד־פעמי הינה הצפנה סימטרית בעלת סודיות מושלמת.

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

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

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

```
\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| אזי \left\{0,1\right\}^{*} אזי היינה X,Y התפלגויות על
בעל כוח \mathcal{A} בעל לכל יריב X,Y מעל X,Y אזי התפלגויות t:\mathbb{N}\to\hat{\mathbb{N}} ותהא arepsilon\geq 0 ותהא arepsilon\geq 0 ותהא
                                                                                                                                                                             \Delta_{\mathcal{A}}\left(X,Y\right)\leq \varepsilon חישוב t מתקיים
                                                                                       Xpprox_{t,arepsilon}Y תהא \hat{\mathbb{N}}	o\hat{\mathbb{N}} ותהיינה X,Y התפלגויות בנ"ל אזיarepsilon 	o \hat{\mathbb{N}} תהא
f\left(X
ight)\left(c
ight)= באשר \{0,1\}^* באשר התפלגות על f\left(X
ight)\left(c
ight)=+ ותהא ותהא \{0,1\}^* באשר אזי ווא התפלגות על \{0,1\}^* באשר
                                                                                                                                                                                                      .\mathbb{P}_{x \leftarrow X} \left( f \left( x \right) = c \right)
בעלי m,m'\in\mathcal{M} בעלת סודיות חישובית: יהי arepsilon\geq 0 ותהא ותהא לarepsilon=\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 t:\mathbb{N}	o\hat{\mathbb{N}} תהא arepsilon\geq 0 יהי (PRG): גנרטור פסודאו אקראי
                                                                                                                                                             G(\{0,1\}^n) \approx_{t \in U_\ell}בזמן פולינומי עבורה
                                                                              . טענה: אם ענרטור פסודאו אקראי. באשר \ell>n באשר לכל לכל אזי לכל \mathcal{P}=\mathcal{NP} אזי לכל
E,D:\left\{0,1
ight\}^n	imes נגדיר פסודאו אקראי (t,arepsilon) נגדיר G:\left\{0,1
ight\}^n	o\{0,1
ight\}^\ell ויהי ויהי ויהי n,\ell\in\mathbb{N} נגדיר אקראי
                                                                                                                                                                                                  כד \{0,1\}^{\ell} \to \{0,1\}^{\ell}
                                                                                                                                                                                    .E_{k}\left( m\right) =m\oplus G\left( k\right) \bullet
                                                                                                                                                                                        .D_{k}\left( c\right) =c\oplus G\left( k\right)  \bullet
טענה: יהיו פנקס חד־פעמי פנקס חד־פעמי אקראי (t,arepsilon) גנרטור פסודאו גנרטור אנרטור איז G:\{0,1\}^n 	o \{0,1\}^\ell יהי n,\ell \in \mathbb{N} יהי
                                                                                                                                                             E\left(\left\{0,1\right\}^{n},m\right)pprox_{t,arepsilon}U_{\ell} אזי m\in\left\{0,1\right\}^{\ell}
משפט: יהיו n,\ell\in\mathbb{N} אזי הצפנת פסודאו אקראי הינה הינה הינה הינה הינה הינה הינה משפט: יהיו היהי ויהי G:\{0,1\}^n	o\{0,1\}^\ell
                                                                                                                                                                                        (t-\ell,2\varepsilon) סודיות חישובית
f(X)pprox_{t-\mathsf{Size}(f),arepsilon} אזיf:\{0,1\}^*	o\{0,1\}^* ותהא Xpprox_{t,arepsilon}Y התפלגויות עבורן X התפלגויות עבורן X התפלגויות עבורן אזייt:\mathbb{N}	o\hat{\mathbb{N}} היהי
                                                                                                                                                                                                                              f(Y)
                    X pprox_{t,arepsilon+\delta} Z אזי אזי איזי אזי אוכן X pprox_{t,arepsilon} X pprox_{t,arepsilon+\delta} וכן ההיינה t: \mathbb{N} 	o \hat{\mathbb{N}} ותהיינה arepsilon X pprox_{t,arepsilon+\delta} X התפלגויות עבורן
             Xpprox_{\min(t,s),arepsilon+\delta}Z אזי אזי Ypprox_{s,\delta}Z וכן Xpprox_{t,arepsilon}Y התפלגויות עבורן Xpprox_{t,\varepsilon}Y ותהיינה X ותהיינה X ותהיינה X ותהיינה X ווהי X אזי X ווהי X ווהי X אזי X ווהי X ווהי X אזי X ווהי X ווהי X ווהי X אזי X ווהי X ווהי X אזי X ווהי X ווחי X
(E,D) אזי הצפנה סימטרית בעלת סודיות חישובית למספר הודעות: יהי n\in\mathbb{N}_+ יהי יהי אזי 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
לכל s_j=igoplus_{i=1}^Lc_is_{j-i} אזי s_0,\ldots,s_{L-1} ויהיו c_L=1 באשר באשר c\in\{0,1\}^L יהי והי L\in\mathbb{N}_+ יהי לניארי (LFRS): יהי
                                                                                                                                                                                                                              .j \ge L
```

משפט: תהא (E,D) הצפנה סימטרית אזי (E,D) בעלת חוסר הבחנה מושלם \Longrightarrow (הא (E,D) במצחת במשחק חוסר ההבחנה).

 \mathcal{A} יריב: משפחת מעגלים בוליאניים

.Size $(\mathcal{A})=\mathcal{O}\left(t\left(n\right)
ight)$ עבורו \mathcal{A} אזי יריב בעל כוח חישוב: תהא $t:\mathbb{N} o\hat{\mathbb{N}}$ אזי יריב בעל כוח

 $\hat{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ סימון:

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 \mathcal{A} lost