```
המפיימת (\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} המקיימת המפנה סימטרית: תהיינה
                                                                     D\left(k,E\left(k,m
ight)
ight)=m מתקיים m\in\mathcal{M} ולכל ולכל k\in\mathcal{K}
                                                        \mathcal{K} אזי אזי סימטרית בהצפנה סימטרית: תהא (\mathcal{K},\mathcal{M},\mathcal{C},E,D) הבפנה סימטרית אזי
                                                        \mathcal{M} אזי איי סימטרית בהצפנה סימטרית: תהא (\mathcal{K},\mathcal{M},\mathcal{C},E,D) הצפנה סימטרית אזי
                                             \mathcal{K} מרחב הקידודים/ההצפנות בהצפנה סימטרית: תהא (\mathcal{K},\mathcal{M},\mathcal{C},E,D) הצפנה סימטרית אזי
                                                                   E אזי אינת הצפנה סימטרית: תהא (\mathcal{K},\mathcal{M},\mathcal{C},E,D) האינת הצפנה סימטרית: תהא
                                                                   D אזי סימטרית פענוח סימטרית: תהא (\mathcal{K},\mathcal{M},\mathcal{C},E,D) הצפנה סימטרית
                                                       . ידועים \mathcal{K}, \mathcal{M}, \mathcal{C} יכ ונניח (E,D) הערה: מכאן והלאה נסמן הצפנה סימטרית בעזרת
                                                                                                  \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 קיסר: יהיו n,m\in\mathbb{N}_+
                                                                                               i \in [|m|] לכל (E(k,m))_i = (m_i + k) \% n
                                                                                                   i \in [|c|] לכל (D(k,c))_i = (c_i - k) \% n
                                                                                . אזי הצפנת קיסר הינה הצפנה סימטרית n,m\in\mathbb{N}_+ יהיו
     כך E,D:[n!]	imes\mathbb{Z}_{n-1}^{\leq m}	o \mathbb{Z}_{n-1}^{\leq m} הצפנת הצבה: יהיו n,m\in\mathbb{N}ackslash\{0,1\} ותהיינה n,m\in\mathbb{N}ackslash\{0,1\}
                                                                                                      i \in [|m|] לכל (E(k,m))_i = f_k(m_i)
                                                                                                        i \in [|c|] לכל (D(k,c))_i = f_k^{-1}(c_i)
              טענה: יהינה הצפנת הצבה הינה n,m\in\mathbb{N}\setminus\{0,1\} הפיכות שונות אזי הצפנת הצבה הינה הצפנה סימטרית. יהיו
```

טענה: הינה הצפנת הצבה הינה הצפנת שונות אזי הצפנת הצבה הינה $n,m\in\mathbb{N}\setminus\{0,1\}$ ותהיינה $m,m\in\mathbb{N}\setminus\{0,1\}$ האינה המקפה גנרית: תהא $m'\in\mathcal{M}$ הצפנה סימטרית תהא $m'\in\mathcal{M}$ התפלגות שכיחויות המילים יהי $m'\in\mathcal{M}$ ותהא $m'\in\mathcal{M}$ נגדיר $m'\in\mathcal{M}$ האינה מימטרית תהא $m'\in\mathcal{M}$ ותהא שכיחויות המילים יהי $m'\in\mathcal{M}$ ותהא $m'\in\mathcal{M}$ ותהא מימטרית תהא וונה מימטרית תהא בינה מימטרית תהא וונה מימטרית תהא וונה מימטרית תהא מימטרית תה

```
 \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 התפלגות התפלגות ותהא $\mu:\Omega o [0,1]$ התפלגות חופית סופית סופית אזי $\mathbb{P}_{a\leftarrow\Omega}\left(a
ight)=rac{1}{|\Omega|}$ אזי חופית חופית אזי $\mathbb{P}_{a\leftarrow\Omega}\left(a
ight)$

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

מתקיים מושלם: הצפנה חוסר הבחנה אלכל מושלם: הצפנה חוסר הבחנה אלכל מושלם: הצפנה חוסר הבחנה חוסר הבחנה מושלם: הצפנה מושלם: הצפנה מושלם: הצפנה הבחנה מושלם: הצפנה הבחנה מושלם: הצפנה מושלם: הצוב מושלם: הצפנה מושלם: הצפנה מושלם: הצפנה מושלם: הצפנה מושלם:

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

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

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

- $E(k,m) = m \oplus k \bullet$
 - $.D(k,c) = c \oplus k \bullet$

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

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

טענה: יהי \mathbb{N}_+ אזי הצפנת קיסר n הינה הצפנה סימטרית בעלת סודיות מושלמת.

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

```
\begin{array}{l|l} \mathbf{game} \  \, \mathbf{IndistinguishabilityGame} \, ((E,D)\,,\mathcal{W},\mathcal{A}) \text{:} \\ & \mathcal{A} \  \, \mathbf{chooses} \  \, \mathbf{messages} \  \, m_0, m_1 \in \mathcal{M} \\ & \mathcal{W} \  \, \mathbf{samples} \  \, \mathbf{key} \  \, k \leftarrow \mathcal{K} \\ & \mathcal{W} \  \, \mathbf{samples} \  \, \mathbf{bit} \  \, b \leftarrow \{0,1\} \\ & \mathcal{W} \  \, \mathbf{sends} \  \, E(k,m_b) \  \, \mathbf{to} \  \, \mathcal{A} \\ & \mathcal{A} \  \, \mathbf{prints} \  \, \mathbf{a} \  \, \mathbf{bit} \  \, b' \\ & \mathbf{if} \  \, b' = b \  \, \mathbf{then} \\ & | \  \, \mathbf{return} \  \, \mathcal{A} \  \, \mathbf{won} \\ & \mathbf{return} \  \, \mathcal{A} \  \, \mathbf{lost} \end{array}
```

.($\mathbb{P}(B,D)$ מנצחת במשחק חוסר ההבחנה מושלם) בעלת חוסר הבחנה בעלת אזי בעלת אזי ((E,D) מנצחת במשחק הצפנה סימטרית אזי ((E,D)