$D_k(c)=D\left(k,c
ight)$ אזי $c\in\mathcal{C}$ איזי אוני סימטרית יהי $k\in\mathcal{K}$ היהי סימטרית הצפנה סימטרית יהי

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

בופן קיסר: $D: \mathbb{Z}_n imes \mathbb{Z}_n^{\leq m} o \mathbb{Z}_n^{\leq m}$ נגדיר $n,m \in \mathbb{N}_+$ יהיו צופן קיסר:

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

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

צופן הצבה: יהיו $m,m\in\mathbb{N}\setminus\{0,1\}$ ותהיינה [n] אותהיינה [n] הפיכות שונות נגדיר ותהיינה $n,m\in\mathbb{N}\setminus\{0,1\}$ בך

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

טענה: יהיו צופן הצבה הינה הצפנה סימטרית. $f_1,\dots,f_{n!}:[n] o [n]$ ותהיינה $n,m\in\mathbb{N}\setminus\{0,1\}$ יהיו איי צופן ויז'נר: יהיו $n,m\in\mathbb{N}\setminus\{0,1\}$ נגדיר $m,m\in\mathbb{N}$ גגדיר $m,m\in\mathbb{N}$ כך דו יוז'נר: יהיו $m,m\in\mathbb{N}$

- $i \in [|x|]$ 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 ותהא ותהא $\mu:\mathcal{M}\to[0,1]$ הצפנה סימטרית הא $c=E_{k'}\left(m'\right)$

```
 \begin{array}{c|c} \text{function GenericAttack}(\left(E,D\right),\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 הא $\mu:\Omega
ightarrow\left[0,1
ight]$ סימון: תהא Ω קבוצה סופית תהא

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

 $c\in\mathcal{C}$ 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 מושלמת: הצפנה סימטרית מושלמת: $\mathbb{P}_{m\leftarrow\mu}\left(m=a\right)=\mathbb{P}_{(m,k)\leftarrow(\mu,\mathcal{K})}\left(m=a\mid c=E_k\left(m\right)\right)$ מתקיים

מתקיים מושלם: הצפנה חוסר $a,b\in\mathcal{M}$ אבורה לכל עבורה חוסר הצפנה מושלם: הצפנה מושלם: הצפנה חוסר הבחנה מושלם:

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

משפט: תהא ((E,D)) בעלת חוסר הבחנה מושלם). בעלת סודיות מושלמת סימטרית אזי ((E,D)) בעלת הבחנה משפט: תהא

בום פנקט חד־פעמי: יהי $E,D:\{0,1\}^n imes\{0,1\}^n o\{0,1\}^n$ נגדיר צופן פנקט חד־פעמי: יהי והי ת

- $E_k(m) = m \oplus k \bullet$
 - $D_k(c) = c \oplus k \bullet$

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

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

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

```
\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
      \vdash return \mathcal{A} won
     return \mathcal{A} lost
  (E,D) משפט: תהא (E,D) הצפנה סימטרית אזי ו(E,D) בעלת חוסר הבחנה מושלם)\Longleftrightarrow (הא
                                                                                                                                    \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| אזי \left\{0,1\right\}^{*} אזי \left\{0,1\right\}^{*} אזי ותהיינה X,Y התפלגויות על
התפלגויות בלתי ניתנות להבחנה (בנ"ל): יהי arepsilon \geq 0 ותהא t: \mathbb{N} 	o \hat{\mathbb{N}} אזי התפלגויות להבחנה (בנ"ל): יהי arepsilon \geq 0 ותהא arepsilon \geq 0 אזי התפלגויות בלתי ניתנות להבחנה (בנ"ל): יהי
                                                                                                                                     \Delta_A(X,Y) < \varepsilon חישוב מתקיים
                                                                   X pprox_{t,arepsilon} Y תהא בנ"ל אזי t: \mathbb{N} 	o \hat{\mathbb{N}} תהא בנ"ל אזי יהי arepsilon \geq 0 תהא
                         באשר f\left(X\right) אזי איזי f\left(X\right) אזי אזי f:\left\{0,1\right\}^{*} 	o \left\{0,1\right\}^{*} ותהא \left\{0,1\right\}^{*} ותהא איזי ותהא איזי לימון: תהא
                                                                                                                                      f(X)(c) = \mathbb{P}_{x \leftarrow X} (f(x) = c)
בעלי m,m'\in\mathcal{M} בעלת סודיות בעלת סימטרית בעלת t:\mathbb{N}\to\hat{\mathbb{N}} ותהא ותהא arepsilon\geq 0 אזי הצפנה הימטרית בעלת סודיות חישובית: יהי
                                                                                                                   .E\left(\mathcal{K},m
ight)pprox_{t,arepsilon}E\left(\mathcal{K},m'
ight) אורך שווה מתקיים
              (\infty,0) בעלת סודיות חישובית (E,D) בעלת סודיות מושלמת) בעלת סודיות חישובית סטענה: תהא
                                                                                                                          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 וויהי t:\mathbb{N}	o\hat{\mathbb{N}} תהא arepsilon\geq 0 ניתנת לחישוב (PRG) גנרטור פסודאו אקראי
                                                                                                                         G(\{0,1\}^n) \approx_{t,\varepsilon} U_\ell בזמן פולינומי עבורה
                                                            . טענה: אם גנרטור פסודאו אקראי. באשר \ell>n באשר לכל אזי לכל \mathcal{P}=\mathcal{NP} אזי אקראי.
                                נגדיר (t,arepsilon) גנרטור פסודאו אקראי ויהי G:\{0,1\}^n	o\{0,1\}^\ell נגדיר ויהי ויהי n,\ell\in\mathbb{N} נגדיר
                                                                                                                            כך E, D: \{0,1\}^n \times \{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)  \bullet
m\in\{0,1\}^\ell טענה: יהיו צופן פנקס חד־פעמי חישובי ויהי G:\{0,1\}^n	o\{0,1\}^\ell גנרטור פסודאו אקראי G:\{0,1\}^n	o\{0,1\}^\ell יהי
                                                                                                                                           E\left(\left\{0,1\right\}^{n},m\right)\approx_{t,\varepsilon}U_{\ell} אזי
משפט: יהיו n,\ell\in\mathbb{N} ויהי G:\{0,1\}^n	o\{0,1\}^\ell גנרטור פסודאו אקראי איז צופן פנקס חד־פעמי חישובי הינה בעלת סודיות משפט: יהיו
                                                                                                                                                       (t-\ell,2\varepsilon) חישובית
                         טענה: יהי f:\{0,1\}^*	o \{0,1\}^* תהא Xpprox_{t,arepsilon}Y התפלגויות עבורן X:\mathbb{N}	o \hat{\mathbb{N}} תהא t:\mathbb{N}	o \hat{\mathbb{N}}
                                                                                                                                                f(X) \approx_{t-\operatorname{Size}(f),\varepsilon} 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}} אזי arepsilon
         Xpprox_{\min(t,s),arepsilon+\delta}Z אזי Ypprox_{s,\delta}Z וכן Xpprox_{t,arepsilon}Y התפלגויות עבורן Xpprox_{t,\varepsilon}Y ותהיינה x,y,z ותהיינה x,y,z ותהיינה x,y,z ויהי x,z
```

(E,D) אזי הצפנה סימטרית בעלת סודיות חישובית למספר הודעות: יהי $n\in\mathbb{N}_+$ יהי $n\in\mathbb{N}_+$ אזי הצפנה סימטרית הצפנה סימטרית מספר הודעות:

טענה: יהי $\mathbb{N} = \mathbb{N} \setminus \{0,1\}$ יהי לא קיימת הצפנה אזי לא קיימת הצפנה חישובית למספר הודעות. $\epsilon > 0$ יהי ותהא $\epsilon > 0$ יהי

 $E\left(\mathcal{K},x
ight)pprox_{t,arepsilon}E\left(\mathcal{K},y
ight)$ מתקיים $i\in\left[n
ight]$ לכל ו $|x_{i}|=|y_{i}|$ באשר $x,y\in\mathcal{M}^{n}$

game IndistinguishabilityGame($(E, D), \mathcal{W}, \mathcal{A}$):

 \mathcal{A} chooses messages $m_0, m_1 \in \mathcal{M}$

```
D:\mathcal{L}	imes\mathcal{C}	o\mathcal{M} ותהא E:\mathcal{L}	imes\mathcal{M}	o\mathcal{C} תהא G:\mathcal{K}	o(\mathbb{N}	o\mathcal{L}) תהא קבוצות סופיות תהא קבוצות סופיות תהא
                                                                                                  (\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{L}, E, D, G) באשר שלמות שלמות שלמות באשר באשר
                                                                                    \mathcal{L} אזי סינכרוני אזי (\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{L}, E, D, G) מרחב הצפנים: יהי
                                                                                    G אופן זרם סינכרוני אזי (\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G) אופן זרם סינכרוני אזי
ותהא E:\mathcal{L}	imes\mathcal{M}	o\mathcal{C} תהא G:\mathcal{K}	o(\mathcal{L}	o\mathcal{L}) ותהא קבוצות סופיות תהא \mathcal{M},\mathcal{K},\mathcal{C},\mathcal{L} תהיינה \mathcal{M},\mathcal{K},\mathcal{C},\mathcal{L} קבוצות סופיות אינכרוני עצמית/אסינכרוני:
                                                                         (\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{L}, E, D, G) אזי שלמות שלמות באשר E, D באשר D: \mathcal{L} \times \mathcal{C} \to \mathcal{M}
                                                                                  \mathcal{L} מרחב הצפנים: יהי (\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G) צופן זרם אסינכרוני אזי
                                                                                  G אופן זרם אסינכרוני אזי (\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G) אופן זרם אסינכרוני אזי
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 יהי ויהי (LFRS): אוגר הזזה בעל משוב ליניארי
                                                                                                                                                                         .j \geq L
                                      טענה: יהי צפנים בצופן זרם אסינכרוני. LFRS אזי c_L=1 באשר בc\in \{0,1\}^L יהי L\in \mathbb{N}_+ יהי יהי
                                                                                                                         אזי k \in \left\{0,1\right\}^{256} יהי :RC4 גנרטור צפנים
function RC4(k):
      (j,i) \leftarrow 0
      S \leftarrow \mathrm{Id}_{\{0...255\}}
     for i \leftarrow [0 \dots 255] do
          j \leftarrow (j + S_i + k_i) \mod 256
         (S_i, S_j) \leftarrow (S_j, S_i)
     end
     return function RC4Inner(S):
          i \leftarrow (i+1) \mod 256
          j \leftarrow (j + S_i) \mod 256
          (S_i, S_j) \leftarrow (S_j, S_i)
          r \leftarrow (S_i + S_j) \mod 256
           return S_r
                                                                                                           טענה: RC4 הינו גנרטור צפנים בצופן זרם אסינכרוני.
\mathcal A משפט: יהי arepsilon \geq 0 תהא (t,arepsilon) ותהא (t,arepsilon) הצפנה סימטרית אזי ((t,arepsilon) בעלת סודיות חישובית (t,arepsilon) ותהא
                                                                            בעל כוח חישוב t מתקיים arepsilon \leq rac{1}{2} + arepsilon מנצחת במשחק חוסר ההבחנה) \mathbb{P}(z)
                              משחק חוסר ההבחנה תחת התקפת גלוי־נבחר (Chosen plaintext attack): יהי \mathcal{M},\mathcal{A} ויהיו שחקנים אזי
game CPA((E, D), W, A):
     \mathcal{W} samples key k \leftarrow \mathcal{K}
     for i \in [1 \dots n] do
           \mathcal{A} chooses message x_i \in \mathcal{M}
          \mathcal{W} sends E_k(x_i) to \mathcal{A}
     end
      \mathcal{A} chooses messages m_0, m_1 \in \mathcal{M}
     \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
      \vdash return \mathcal{A} won
     return \mathcal{A} lost
```

משפט: יהי (t,ε) יהי (t,ε) תחת התקפת גלוי־נבחר אזי (t,ε) הצפנה סימטרית בעלת סודיות ((t,ε) תחת התקפת גלוי־נבחר אזי (t,ε) בעלת סודיות חישובית ((t,ε)) למספר הודעות. צופן רנדומלי גנרי: יהי (t,ε) תהא (t,ε) למספר הודעות. (t,ε) הפיכה אזי נגדיר (t,ε) תהא (t,ε) תהא (t,ε) למספר הודעות. (t,ε) הפיכה אזי נגדיר (t,ε) ותהא (t,ε) תהא (t,ε) למספר הודעות. (t,ε) הפיכה אזי נגדיר (t,ε) ותהא (t,ε) תהא (t,ε) למספר הודעות. (t,ε) הפיכה אזי נגדיר (t,ε) (t,ε) תחת התקפת גלוי־נבחר אזי (t,ε) למספר הודעות. (t,ε) למספר הודעות חישובית (t,ε) למספר הודעות חישובית (t,ε) למספר הודעות חישובית (t,ε) למספר הודעות חישובית (t,ε) למספר הודעות (t,ε) למספר

הצפנה סימטרית בעלת סודיות תחת התקפת גלוי־נבחר: יהי $n\in\mathbb{N}$ אזי הצפנה סימטרית בעלת סודיות תחת התקפת גלוי־נבחר: יהי

.
 $\mathbb{P}\left($ מנצחת מנצחת ממחק חוסר ההבחנה מנצחת לוי־נבחר
) $\mathcal{A}\right) \leq \frac{1}{2} + \varepsilon$ מתקיים מתקיים t

```
x \leftarrow \{0,1\}^n עבור E(m) = (r, F(r \oplus m)) \bullet
```

 $.D((r,c)) = r \oplus F^{-1}(c) \bullet$

משפט: יהי (t,ε) תחת התקפת גלוי־נבחר אזי צופן רנדומלי אוי אוי אקראית אזי התקפת גלוי־נבחר $F:\{0,1\}^n o \{0,1\}^n$ תחת התקפת גלוי־נבחר באשר $\varepsilon=\mathcal{O}\left(\frac{t(n)}{2^n}\right)$

 $k\in\{0,1\}^n$ משפחת תמורות: יהי $F:\{0,1\}^n imes \{0,1\}^n o \{0,1\}^n o \{0,1\}^n$ אזי פונקציה $n\in\mathbb{N}$ אזי פונקציה $F:\{0,1\}^n o \{0,1\}^n o \{0,1\}^n$ חשיבה בזמן poly (n) יהי $n\in\mathbb{N}$ אזי פונקציה $F:\{0,1\}^n o \{0,1\}^n o \{0,1\}^n$ חשיבה בזמן המקיימת

- $.k \in \left\{0,1\right\}^n$ הפיכה לכל F_k
- $k \in \left\{0,1\right\}^n$ לכל $\operatorname{poly}\left(n\right)$ בזמן חשיבה F_k^{-1}
- $\|\mathbb{P}_{k\leftarrow\{0,1\}^n}\left(\mathcal{A}^{F_k(\cdot)}\left(1^n
 ight)=1
 ight)-\mathbb{P}_{f\leftarrow(\{0,1\}^n o\{0,1\}^n)}\left(\mathcal{A}^{f(\cdot)}\left(1^n
 ight)=1
 ight)ig|\leq arepsilon$ משמעות הביטוי $\mathcal{A}^{f(\cdot)}$ היא שלמעגל \mathcal{A} יש אורקל לחישוב f.

משפחת תמורות פסודאו אקראיות (PRP): יהי $n\in\mathbb{N}$ אזי משפחת פונקציות פסודאו אקראיות אשר הינה משפחת תמורות. משחק חוסר ההבחנה עבור משפחת פונקציות פסודאו אקראיות: יהי $n\in\mathbb{N}$ תהא $n\in\mathbb{N}$ תהא $f:\{0,1\}^n imes\{0,1\}^n imes\{0,1\}^n$ ויהיו $f:\{0,1\}^n$ שחקנים אזי

```
\begin{array}{c|c} \mathbf{game} \ \mathsf{PRF}\left(\left(E,D\right),\mathcal{W},\mathcal{A}\right) \text{:} \\ & \mathcal{W} \ \mathsf{samples} \ \mathsf{key} \ k \leftarrow \mathcal{K} \\ & \mathcal{W} \ \mathsf{samples} \ \mathsf{bit} \ b \leftarrow \{0,1\} \\ & \mathbf{if} \ b = 0 \ \mathbf{then} \\ & \mid \ R \leftarrow F_k \\ & \mathbf{else} \\ & \mid \ R \leftarrow (\{0,1\}^n \rightarrow \{0,1\}^n) \\ & \mathbf{for} \ i \in [1 \dots m] \ \mathbf{do} \\ & \mid \ \mathcal{A} \ \mathsf{chooses} \ \mathsf{message} \ x_i \in \mathcal{M} \\ & \mid \ \mathcal{W} \ \mathsf{sends} \ E_k(x_i) \ \mathsf{to} \ \mathcal{A} \\ & \mathbf{end} \\ & \mathcal{A} \ \mathsf{prints} \ \mathsf{a} \ \mathsf{bit} \ b' \\ & \mathbf{if} \ b' = b \ \mathbf{then} \\ & \mid \ \mathbf{return} \ \mathcal{A} \ \mathsf{won} \\ & \mathbf{return} \ \mathcal{A} \ \mathsf{lost} \\ \end{array}
```

 \mathcal{A} טענה: יהי $\mathbb{R} \in \mathbb{N}$ ותהא (t, ε) ותהא $f: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ אזי ותהא $n \in \mathbb{N}$ אזי וותהא $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ אזי וותהא $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ מענה: יהי $f: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות פסודאו אקראיות: יהי $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות פסודאו אקראיות: יהי $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות פסודאו אקראיות: יהי $f: \{0,1\}^n \to \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות פסודאו אקראיות: יהי $f: \{0,1\}^n \to \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות פסודאו אקראיות: יהי $f: \{0,1\}^n \to \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות פסודאו אקראיות: יהי $f: \{0,1\}^n \to \{0,1\}^n \to \{0,1\}^n \to \{0,1\}^n$

```
\begin{array}{c|c} \mathbf{game} \ \mathsf{PRP}\left(\left(E,D\right),\mathcal{W},\mathcal{A}\right) \text{:} \\ & \mathcal{W} \ \mathsf{samples} \ \mathsf{key} \ k \leftarrow \mathcal{K} \\ & \mathcal{W} \ \mathsf{samples} \ \mathsf{bit} \ b \leftarrow \{0,1\} \\ & \mathbf{if} \ b = 0 \ \mathbf{then} \\ & \mid \ R \leftarrow F_k \\ & \mathbf{else} \\ & \mid \ R \leftarrow S\left(\{0,1\}^n\right) \\ & \mathbf{for} \ i \in [1 \dots m] \ \mathbf{do} \\ & \mid \ \mathcal{A} \ \mathsf{chooses} \ \mathsf{message} \ x_i \in \mathcal{M} \\ & \mid \ \mathcal{W} \ \mathsf{sends} \ E_k(x_i) \ \mathsf{to} \ \mathcal{A} \\ & \mathbf{end} \\ & \mathcal{A} \ \mathsf{prints} \ \mathsf{a} \ \mathsf{bit} \ b' \\ & \mathbf{if} \ b' = b \ \mathbf{then} \\ & \mid \ \mathbf{return} \ \mathcal{A} \ \mathsf{won} \\ & \mathbf{return} \ \mathcal{A} \ \mathsf{lost} \\ \end{array}
```

 (t, ε) טענה: יהי $n \in \mathbb{N}$ ותהא $n \in \mathbb{N}$ ותהא $n \in \mathbb{N}$ משפחת תמורות אזי ($t \in \mathbb{N}$ משפחת תמורות פסודאו אקראיות ($t \in \mathbb{N}$) משפחת ענה: יהי $t \in \mathbb{N}$ ותהא $t \in \mathbb{N}$ מנצחת במשחק חוסר ההבחנה עבור משפחת תמורות פסודאו אקראיות) $t \in \mathbb{N}$ יריב $t \in \mathbb{N}$ מנצחת במשחק חוסר ההבחנה עבור משפחת תמורות פסודאו אקראיות) בעל כוח חישוב $t \in \mathbb{N}$ מנצחי $t \in \mathbb{N}$ אזי נגדיר $t \in \mathbb{N}$ אזי נגדיר $t \in \mathbb{N}$ ותהא $t \in \mathbb{N}$ ותהא $t \in \mathbb{N}$ ותהא $t \in \mathbb{N}$ מנגדיר $t \in \mathbb{N}$ אזי נגדיר $t \in \mathbb{N}$ מכך $t \in \mathbb{N}$ כך $t \in \mathbb{N}$ מנגדיר $t \in \mathbb{N}$ מותהא $t \in \mathbb{N}$ מנגדיר $t \in \mathbb{N}$ מותהא $t \in \mathbb{N}$ מנגדיר $t \in \mathbb{N}$ מנגדיר $t \in \mathbb{N}$ מנגדיר $t \in \mathbb{N}$ מותהא $t \in \mathbb{N}$ מותהא t

- $.r \leftarrow \left\{0,1\right\}^n$ עבור $E_k\left(m\right) = \left(r, F_k\left(r \oplus m\right)\right)$
 - $.D\left((r,c) \right) = r \oplus F_k^{-1}\left(c \right) \bullet$

משפט: יהי (t,arepsilon) אזי צופן פסודאו רנדומלי $F:\{0,1\}^n imes\{0,1\}^n o \{0,1\}^n o (t,arepsilon)$ אזי צופן פסודאו רנדומלי הינו בעל סודיות $n\in\mathbb{N}$ תחת התקפת גלוי־נבחר.

 $(\mathcal{M},\mathsf{MAC})$ אזי איזי MAC : $\{0,1\}^n \times \mathcal{M} \to \{0,1\}^\ell$ א קבוצה ותהא $\ell < n$ באשר איזי $n,\ell \in \mathbb{N}$ אזי אימות מסרים: יהיו $\ell \in \mathbb{N}$ איזי $\ell \in \mathbb{N}$ אזי $\ell \in \mathbb{N}$ אזי מרחב ההודעות בקוד אימות מסרים: יהי $\ell \in \mathbb{N}$ קוד אימות מסרים אזי $\ell \in \mathbb{N}$

 $k \in \left\{0,1\right\}^n$ אזי מסרים אימות מסרים: יהי (\mathcal{M},MAC) קוד אימות מסרים אזי

.MAC אימות מסרים אימות (\mathcal{M},MAC) אלגוריתם אימות בקוד אימות מסרים: יהי

משחק איוף אימות מסרים ויהיו \mathcal{W},\mathcal{A} שחקנים אזי (\mathcal{M},MAC) איזי יהי שחקנים אזי שחקנים אזי

 $\begin{array}{l} \mathbf{game} \ \, \mathbf{ExistentialForgeryCPA((\mathcal{M},k,\mathsf{MAC})}\,,\mathcal{W},\mathcal{A}) \text{:} \\ | \ \, \mathcal{W} \ \, \mathbf{samples} \ \, \mathbf{key} \ \, k \leftarrow \{0,1\}^n \end{array}$

 $\mathcal{A}^{\mathsf{MAC}_k(\cdot)}$ prints (m,t) if $(m \in \mathcal{M}) \wedge (\mathsf{MAC}_k(m) = t) \wedge (\mathcal{A} \text{ didn't query } m)$ then \mid return \mathcal{A} won

return A lost

קוד אימות מסרים בעל חסינות זיוף אימות תחת התקפת גלוי־נבחר: קוד אימות מסרים בעל חסינות זיוף אימות תחת התקפת גלוי־נבחר: קוד אימות מסרים בעל חסינות זיוף אימות תחת התקפת גלוי־נבחר) $\mathbb{P}(M,\mathsf{MAC})$

סענה: אינה אזי (\mathcal{M},MAC) ויהי אינה אינה אינה אינה (\mathcal{M},MAC) אינה אינה אינה אינה אינה אינה ($(\mathcal{M},\mathsf{MAC})$) ויהי ווהי אינה ($(\mathcal{M},\mathsf{MAC})$) אימות התקפת אימות ($(\mathcal{M},\mathcal{MAC})$) תחת התקפת אלוי־נבחר.

 $\left(t,arepsilon+2^{-\ell}
ight)$ איזי איוף אימות זיוף אימות פונקציות פסודאו אקראיות איזי איזי איזי איזי איזי איזיף אימות פונקציות פסודאו אקראיות איזי איזי איזי איזי $\left(\left\{0,1
ight\}^{\ell},F
ight)$ איזי איזי איזיף אימות פונקציות פסודאו אקראיות איזיי איזיי איזיף אימות פסודאו אקראיות פסודאו אקראיות איזיי אי

 $\mathsf{MAC}_k\left(M_1\dots M_\ell
ight) = egin{pmatrix} r \\ E_k(r,M_1,1,\ell) \\ \vdots \\ E_k(r,M_\ell,\ell,\ell) \end{pmatrix}$ אזי $n\cdot\ell+rac{n}{3}$ אזי משפחת פונקציות פסודאו אקראיות מגודל $n\cdot\ell+rac{n}{3}$ אזי $n\cdot\ell+rac{n}{3}$ הינה בעלת חסינות זיוף אימות תחת התקפת גלוי־נבחר.