הצפנה סימטרית: תהיינה $\mathcal{M},\mathcal{K},\mathcal{C}$ קבוצות סופיות תהא $E:\mathcal{K}\times\mathcal{M}\to\mathcal{C}$ ותהא $D:\mathcal{K}\times\mathcal{C}\to\mathcal{M}$ אזי $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ המקיימת

- שלמות: לכל $k\in\mathcal{K}$ ולכל $m\in\mathcal{M}$ מתקיים $D\left(k,E\left(k,m\right)\right)=m$.

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

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

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

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

סימון: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ הצפנה סימטרית יהי $k\in\mathcal{K}$ ויהי $m\in\mathcal{M}$ אזי $E_k\left(m\right)=E\left(k,m\right)$.

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

סימון: תהא $(\mathcal{K},\mathcal{M},\mathcal{C},E,D)$ הצפנה סימטרית יהי $k\in\mathcal{K}$ ויהי $c\in\mathcal{C}$ אזי $D_k\left(c\right)=D\left(k,c\right)$.

הערה: מכאן והלאה נסמן הצפנה סימטרית בעזרת (E,D) ונניח כי $\mathcal{K},\mathcal{M},\mathcal{C}$ ידועים.

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

צופן קיסר: יהיו $n,m\in\mathbb{N}_+$ נגדיר $E,D:\mathbb{Z}_n\times\mathbb{Z}_n^{\le m}\to\mathbb{Z}_n^{\le m}$ כך

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

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

צופן הצבה: יהיו $n,m\in\mathbb{N}\backslash\{0,1\}$ ותהיינה $f_1,\ldots,f_{n!}:[n]\to[n]$ הפיכות שונות נגדיר $E,D:[n!]\times\mathbb{Z}_{n-1}^{\le m}\to\mathbb{Z}_{n-1}^{\le m}$ כך

- $\left(E_k\left(x\right)\right)_i=f_k\left(x_i\right)$ לכל $i\in\left[|m|\right]$.
- $\left(D_k\left(c\right)\right)_i=f_k^{-1}\left(c_i\right)$ לכל $i\in\left[|c|\right]$.

טענה: יהיו $n,m\in\mathbb{N}\backslash\{0,1\}$ ותהיינה $f_1,\ldots,f_{n!}:[n]\to[n]$ הפיכות שונות אזי צופן הצבה הינה הצפנה סימטרית.

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

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

התקפה גנרית: תהא (E,D) הצפנה סימטרית תהא $\mu:\mathcal{M}\to[0,1]$ התפלגות שכיחויות המילים יהי $k'\in\mathcal{K}$ ותהא $m'\in\mathcal{M}$ נגדיר $c=E_{k'}\left(m'\right)$ אזי

```
function GenericAttack((E, D), μ, c):
    ℓ ← M
    p ← [0, 1]
    for k ← K do
        m ← D(k, c)
        if μ(m) > p then (ℓ, p) ← (m, μ(m))
    end
    return ℓ
```

סימון: תהא Ω קבוצה סופית תהא $\mu:\Omega\to[0,1]$ התפלגות אזי $\mathbb{P}_{a\leftarrow\mu}\left(a\right)=\mu\left(a\right)$.

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

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

הצפנה סימטרית בעלת חוסר הבחנה מושלם: הצפנה סימטרית (E,D) עבורה לכל $a,b\in\mathcal{M}$ ולכל $c\in\mathcal{C}$ מתקיים $\mathbb{P}_{k\leftarrow\mathcal{K}}\left(E_k\left(a\right)=c\right)=\mathbb{P}_{k\leftarrow\mathcal{K}}\left(E_k\left(b\right)=c\right)$.

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

צופן פנקס חד־פעמי: יהי $n\in\mathbb{N}$ נגדיר $E,D:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$ כך

- $E_k\left(m\right)=m\oplus k$.
- $D_k\left(c\right)=c\oplus k$.

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

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

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

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

```
game IndistinguishabilityGame((E, D), W, A):
    A chooses messages m_0, m_1 ∈ M
    W samples key k ← K
    W samples bit b ← {0,1}
    W sends E(k, m_b) to A
    A prints a bit b'
    if b' = b then
        return A won
    return A lost
```

משפט: תהא (E,D) הצפנה סימטרית אזי ((E,D) בעלת חוסר הבחנה מושלם)$\Longleftrightarrow$($\mathbb{P}\left(\text{מנצחת במשחק חוסר ההבחנה } \mathcal{A}\right)=\frac{1}{2}$).

יריב: משפחת מעגלים בוליאניים $\mathcal{A}$.

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

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

סימון: יהי $\mathcal{A}$ יריב ותהיינה X,Y התפלגויות על $\{0,1\}^*$ אזי $\Delta_{\mathcal{A}}\left(X,Y\right)=\left|\mathbb{P}_{x\leftarrow X}\left(\mathcal{A}\left(x\right)=1\right)-\mathbb{P}_{y\leftarrow Y}\left(\mathcal{A}\left(y\right)=1\right)\right|$.

התפלגויות בלתי ניתנות להבחנה (בנ"ל): יהי $\varepsilon\geq 0$ ותהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ אזי התפלגויות X,Y מעל $\{0,1\}^*$ עבורן לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\Delta_{\mathcal{A}}\left(X,Y\right)\leq\varepsilon$.

סימון: יהי $\varepsilon\geq 0$ תהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ ותהיינה X,Y התפלגויות בנ"ל אזי $X\approx_{t,\varepsilon}Y$.

סימון: תהא X התפלגות על $\{0,1\}^*$ ותהא $f:\{0,1\}^*\to\{0,1\}^*$ אזי $f\left(X\right)$ הינה התפלגות על $\{0,1\}^*$ באשר $f\left(X\right)\left(c\right)=\mathbb{P}_{x\leftarrow X}\left(f\left(x\right)=c\right)$.

הצפנה סימטרית בעלת סודיות חישובית: יהי $\varepsilon\geq 0$ ותהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ אזי הצפנה סימטרית (E,D) עבורה לכל $m,m'\in\mathcal{M}$ בעלי אורך שווה מתקיים $E\left(\mathcal{K},m\right)\approx_{t,\varepsilon}E\left(\mathcal{K},m'\right)$.

טענה: תהא (E,D) הצפנה סימטרית אזי ((E,D) בעלת סודיות מושלמת)$\Longleftrightarrow$((E,D) בעלת סודיות חישובית $(\infty,0)$).

סימון: יהי $n\in\mathbb{N}$ אזי $U_n=U\left(\{0,1\}^n\right)$.

גנרטור פסודו אקראי (PRG): יהי $\varepsilon\geq 0$ תהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ ויהיו $\ell,n\in\mathbb{N}$ באשר $\ell>n$ אזי $G:\{0,1\}^n\to\{0,1\}^\ell$ ניתנת לחישוב בזמן פולינומי עבורה $G\left(\{0,1\}^n\right)\approx_{t,\varepsilon}U_\ell$.

טענה: אם $\mathcal{P}=\mathcal{NP}$ אזי לכל $\ell,n\in\mathbb{N}$ באשר $\ell>n$ לא קיים גנרטור פסודו אקראי.

צופן פנקס חד־פעמי חישובי: יהיו $n,\ell\in\mathbb{N}$ ויהי $G:\{0,1\}^n\to\{0,1\}^\ell$ גנרטור פסודו אקראי (t,ε) נגדיר $E,D:\{0,1\}^n\times\{0,1\}^\ell\to\{0,1\}^\ell$ כך

- $E_k\left(m\right)=m\oplus G\left(k\right)$.
- $D_k\left(c\right)=c\oplus G\left(k\right)$.

טענה: יהיו $n,\ell\in\mathbb{N}$ יהי $G:\{0,1\}^n\to\{0,1\}^\ell$ גנרטור פסודו אקראי (t,ε) תהא E צופן פנקס חד־פעמי חישובי ויהי $m\in\{0,1\}^\ell$ אזי $E\left(\{0,1\}^n,m\right)\approx_{t,\varepsilon}U_\ell$.

משפט: יהיו $n,\ell\in\mathbb{N}$ ויהי $G:\{0,1\}^n\to\{0,1\}^\ell$ גנרטור פסודו אקראי (t,ε) אזי צופן פנקס חד־פעמי חישובי הינה בעלת סודיות חישובית $(t-\ell,2\varepsilon)$.

טענה: יהי $\varepsilon\geq 0$ תהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ תהיינה X,Y התפלגויות עבורן $X\approx_{t,\varepsilon}Y$ ותהא $f:\{0,1\}^*\to\{0,1\}^*$ אזי $f\left(X\right)\approx_{t-\text{Size}(f),\varepsilon}f\left(Y\right)$.

טענה: יהיו $\varepsilon,\delta\geq 0$ תהיינה $t:\mathbb{N}\to\hat{\mathbb{N}}$ ותהיינה X,Y,Z התפלגויות עבורן $X\approx_{t,\varepsilon}Y$ וכן $Y\approx_{t,\delta}Z$ אזי $X\approx_{t,\varepsilon+\delta}Z$.

טענה: יהיו $\varepsilon\geq 0$ תהיינה $t,s:\mathbb{N}\to\hat{\mathbb{N}}$ ותהיינה X,Y,Z התפלגויות עבורן $X\approx_{t,\varepsilon}Y$ וכן $Y\approx_{s,\varepsilon}Z$ אזי $X\approx_{\min(t,s),\varepsilon}Z$.

מסקנה: יהיו $\varepsilon,\delta\geq 0$ תהיינה $t,s:\mathbb{N}\to\hat{\mathbb{N}}$ ותהיינה X,Y,Z התפלגויות עבורן $X\approx_{t,\varepsilon}Y$ וכן $Y\approx_{s,\delta}Z$ אזי $X\approx_{\min(t,s),\varepsilon+\delta}Z$.

סימון: תהא (E,D) הצפנה סימטרית יהי $x\in\mathcal{M}^n$ ויהי $k\in\mathcal{K}$ אזי $E\left(k,x\right)=\begin{pmatrix}E(k,x_1)\\ \vdots\\ E(k,x_n)\end{pmatrix}$.

הצפנה סימטרית בעלת סודיות חישובית למספר הודעות: יהי $n\in\mathbb{N}_+$ יהי $\varepsilon\geq 0$ ותהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ אזי הצפנה סימטרית (E,D) עבורה לכל $x,y\in\mathcal{M}^n$ באשר $|x_i|=|y_i|$ לכל $i\in[n]$ מתקיים $E\left(\mathcal{K},x\right)\approx_{t,\varepsilon}E\left(\mathcal{K},y\right)$.

טענה: יהי $n\in\mathbb{N}\backslash\{0,1\}$ יהי $\varepsilon\geq 0$ ותהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ אזי לא קיימת הצפנה סימטרית בעלת סודיות חישובית למספר הודעות.

צופן זרם סינכרוני: תהיינה $\mathcal{M},\mathcal{K},\mathcal{C},\mathcal{L}$ קבוצות סופיות תהא $G:\mathcal{K}\to(\mathbb{N}\to\mathcal{L})$ תהא $E:\mathcal{L}\times\mathcal{M}\to\mathcal{C}$ ותהא $D:\mathcal{L}\times\mathcal{C}\to\mathcal{M}$ באשר E,D מקיימות שלמות אזי $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$.

מרחב הצפנים: יהי $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$ צופן זרם סינכרוני אזי $\mathcal{L}$.

גנרטור צפנים: יהי $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$ צופן זרם סינכרוני אזי G.

צופן זרם סינכרוני עצמית/אסינכרוני: תהיינה $\mathcal{M},\mathcal{K},\mathcal{C},\mathcal{L}$ קבוצות סופיות תהא $G:\mathcal{K}\to(\mathcal{L}\to\mathcal{L})$ תהא $E:\mathcal{L}\times\mathcal{M}\to\mathcal{C}$ ותהא $D:\mathcal{L}\times\mathcal{C}\to\mathcal{M}$ באשר E,D מקיימות שלמות אזי $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$.

מרחב הצפנים: יהי $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$ צופן זרם אסינכרוני אזי $\mathcal{L}$.

גנרטור צפנים: יהי $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$ צופן זרם אסינכרוני אזי G.

אוגר הזזה בעל משוב ליניארי (LFRS): יהי $L\in\mathbb{N}_+$ יהי $c\in\{0,1\}^L$ באשר $c_L=1$ ויהיו $s_0,\ldots,s_{L-1}$ אזי $s_j=\bigoplus_{i=1}^{L}c_is_{j-i}$ לכל $j\geq L$.

טענה: יהי $L\in\mathbb{N}_+$ יהי $c\in\{0,1\}^L$ באשר $c_L=1$ אזי LFRS הינו גנרטור צפנים בצופן זרם אסינכרוני.

גנרטור צפנים RC4: יהי $k\in\{0,1\}^{256}$ אזי

```
function RC4(k):
    (j, i) ← 0
    S ← Id_{0...255}
    for i ← [0...255] do
        j ← (j + S_i + k_i)  mod 256
        (S_i, S_j) ← (S_j, S_i)
    end
    return function RC4Inner(S):
        i ← (i + 1)  mod 256
        j ← (j + S_i)  mod 256
        (S_i, S_j) ← (S_j, S_i)
        r ← (S_i + S_j)  mod 256
        return S_r
```

טענה: RC4 הינו גנרטור צפנים בצופן זרם אסינכרוני.

משפט: יהי $\varepsilon\geq0$ תהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ ותהא (E,D) הצפנה סימטרית אזי $((E,D)$ בעלת סודיות חישובית $(t,\varepsilon))\Longleftrightarrow($לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\mathbb{P}\left(\mathcal{A}\text{ מנצחת במשחק חוסר ההבחנה}\right)\leq\frac{1}{2}+\varepsilon$).

משחק חוסר ההבחנה תחת התקפת גלוי־נבחר (Chosen plaintext attack): יהי $n\in\mathbb{N}$ ויהיו $\mathcal{W},\mathcal{A}$ שחקנים אזי

```
game CPA((E, D), W, A):
    W samples key k ← K
    for i ∈ [1...n] do
        A chooses message x_i ∈ M
        W sends E_k(x_i) to A
    end
    A chooses messages m_0, m_1 ∈ M
    W samples bit b ← {0, 1}
    W sends E_k(m_b) to A
    A prints a bit b'
    if b' = b then
        return A won
    return A lost
```

הצפנה סימטרית בעלת סודיות תחת התקפת גלוי־נבחר: יהי $n\in\mathbb{N}$ אזי הצפנה סימטרית (E,D) עבורה לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\mathbb{P}\left(\mathcal{A}\text{ מנצחת במשחק חוסר ההבחנה תחת התקפת גלוי־נבחר}\right)\leq\frac{1}{2}+\varepsilon$.

משפט: יהי $n\in\mathbb{N}$ יהי $\varepsilon\geq0$ תהא $t:\mathbb{N}\to\hat{\mathbb{N}}$ ותהא (E,D) הצפנה סימטרית בעלת סודיות (t,ε) תחת התקפת גלוי־נבחר אזי (E,D) בעלת סודיות חישובית (t,ε) למספר הודעות.

צופן רנדומלי גנרי: יהי $n\in\mathbb{N}$ ותהא $F:\{0,1\}^n\to\{0,1\}^n$ הפיכה אזי נגדיר $E:\varnothing\times\{0,1\}^n\to\{0,1\}^n\times\{0,1\}^n$ ונגדיר $D:\varnothing\times\left(\{0,1\}^n\times\{0,1\}^n\right)\to\{0,1\}^n$ כך

- $E(m) = (r, F(r \oplus m))$ עבור $r \leftarrow \{0,1\}^n$.
- $D((r,c)) = r \oplus F^{-1}(c)$.

משפט: יהי $n \in \mathbb{N}$ ותהא $F : \{0,1\}^n \to \{0,1\}^n$ אקראית אזי צופן רנדומלי גנרי הינו בעל סודיות (t, ε) תחת התקפת גלוי־נבחר באשר $\varepsilon = \mathcal{O}\left(\frac{t(n)}{2^n}\right)$.

משפחת תמורות: יהי $n \in \mathbb{N}$ אזי פונקציה $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ עבורה F_k תמורה לכל $k \in \{0,1\}^n$.

משפחת פונקציות פסודו אקראיות (PRF): יהי $n \in \mathbb{N}$ אזי פונקציה $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ חשיבה בזמן $\text{poly}(n)$ המקיימת

- F_k הפיכה לכל $k \in \{0,1\}^n$.
- F_k^{-1} חשיבה בזמן $\text{poly}(n)$ לכל $k \in \{0,1\}^n$.
- לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\left|\mathbb{P}_{k \leftarrow \{0,1\}^n}\left(\mathcal{A}^{F_k(\cdot)}(1^n) = 1\right) - \mathbb{P}_{f \leftarrow (\{0,1\}^n \to \{0,1\}^n)}\left(\mathcal{A}^{f(\cdot)}(1^n) = 1\right)\right| \le \varepsilon$.

הערה: משמעות הביטוי $\mathcal{A}^{f(\cdot)}$ היא שלמעגל $\mathcal{A}$ יש אורקל לחישוב f.

משפחת תמורות פסודו אקראיות (PRP): יהי $n \in \mathbb{N}$ אזי משפחת פונקציות פסודו אקראיות אשר הינה משפחת תמורות.

משחק חוסר ההבחנה עבור משפחת פונקציות פסודו אקראיות: יהי $n \in \mathbb{N}$ תהא $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ ויהיו $\mathcal{W}, \mathcal{A}$ שחקנים אזי

```
game PRF((E, D), W, A):
    W samples key k ← K
    W samples bit b ← {0,1}
    if b = 0 then
        R ← F_k
    else
        R ← ({0,1}^n → {0,1}^n)
    for i ∈ [1...m] do
        A chooses message x_i ∈ M
        W sends E_k(x_i) to A
    end
    A prints a bit b'
    if b' = b then
        return A won
    return A lost
```

טענה: יהי $n \in \mathbb{N}$ ותהא $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ אזי (F משפחת פונקציות פסודו אקראיות (t, ε))$\Longleftrightarrow$(לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\mathbb{P}$ ($\mathcal{A}$ מנצחת במשחק חוסר ההבחנה עבור משפחת פונקציות פסודו אקראיות) $\le \frac{1}{2} + \varepsilon$).

משחק חוסר ההבחנה עבור משפחת תמורות פסודו אקראיות: יהי $n \in \mathbb{N}$ תהא $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ משפחת תמורות ויהיו $\mathcal{W}, \mathcal{A}$ שחקנים אזי

```
game PRP((E, D), W, A):
    W samples key k ← K
    W samples bit b ← {0,1}
    if b = 0 then
        R ← F_k
    else
        R ← S({0,1}^n)
    for i ∈ [1...m] do
        A chooses message x_i ∈ M
        W sends E_k(x_i) to A
    end
    A prints a bit b'
    if b' = b then
        return A won
    return A lost
```

טענה: יהי $n \in \mathbb{N}$ ותהא $F : \{0,1\}^n\times\{0,1\}^n \to \{0,1\}^n$ משפחת תמורות אזי (F משפחת תמורות פסודאו אקראיות (t,ε))$\Longleftrightarrow$(לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\mathbb{P}(\mathcal{A}$ מנצחת במשחק חוסר ההבחנה עבור משפחת תמורות פסודאו אקראיות$) \le \frac{1}{2}+\varepsilon$).

צופן פסודאו רנדומלי גנרי: יהי $n \in \mathbb{N}$ ותהא $F : \{0,1\}^n\times\{0,1\}^n \to \{0,1\}^n$ אזי נגדיר $E : \{0,1\}^n\times\{0,1\}^n \to \{0,1\}^n\times\{0,1\}^n$ ונגדיר $D : \{0,1\}^n \times \left(\{0,1\}^n \times \{0,1\}^n\right) \to \{0,1\}^n$ כך

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

משפט: יהי $n \in \mathbb{N}$ ותהא $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ משפחת פונקציות פסודאו אקראיות (t,ε) אזי צופן פסודאו רנדומלי גנרי הינו בעל סודיות $\left(\Omega\left(\frac{t(n)}{n}\right), 2\varepsilon+\frac{t}{2^n}\right)$ תחת התקפת גלוי־נבחר.

קוד אימות מסרים: יהיו $n,\ell \in \mathbb{N}$ באשר $\ell < n$ תהא $\mathcal{M}$ קבוצה ותהא $\mathsf{MAC} : \{0,1\}^n \times \mathcal{M} \to \{0,1\}^\ell$ אזי $(\mathcal{M}, \mathsf{MAC})$.

מרחב ההודעות בקוד אימות מסרים: יהי $(\mathcal{M}, \mathsf{MAC})$ קוד אימות מסרים אזי $\mathcal{M}$.

קוד אימות סודי בקוד אימות מסרים: יהי $(\mathcal{M}, \mathsf{MAC})$ קוד אימות מסרים אזי $k \in \{0,1\}^n$.

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

משחק זיוף אימות תחת התקפת גלוי־נבחר: יהי $(\mathcal{M}, \mathsf{MAC})$ קוד אימות מסרים ויהיו $\mathcal{W},\mathcal{A}$ שחקנים אזי

```
game ExistentialForgeryCPA((M, k, MAC), W, A):
    W samples key k ← {0,1}^n
    A^{MAC_k(·)} prints (m, t)
    if (m ∈ M) ∧ (MAC_k(m) = t) ∧ (A didn't query m) then
        return A won
    return A lost
```

קוד אימות מסרים בעל חסינות זיוף אימות תחת התקפת גלוי־נבחר: קוד אימות מסרים $(\mathcal{M}, \mathsf{MAC})$ עבורו לכל יריב $\mathcal{A}$ בעל כוח חישוב t מתקיים $\mathbb{P}(\mathcal{A}$ מנצחת במשחק זיוף אימות תחת התקפת גלוי־נבחר$) < \varepsilon$.

טענה: יהיו $n,\ell \in \mathbb{N}$ באשר $\ell < n$ ויהי $(\mathcal{M}, \mathsf{MAC})$ קוד אימות מסרים באשר MAC פונקציה אקראית אזי $(\mathcal{M}, \mathsf{MAC})$ הינה בעלת חסינות זיוף אימות $\left(\infty, 2^{-\ell}\right)$ תחת התקפת גלוי־נבחר.

טענה: יהי $\ell \in \mathbb{N}$ ותהא F משפחת פונקציות פסודאו אקראיות (t,ε) אזי $\left(\{0,1\}^\ell, F\right)$ הינה בעלת חסינות זיוף אימות $\left(t, \varepsilon + 2^{-\ell}\right)$ תחת התקפת גלוי־נבחר.

טענה: יהיו $n,\ell \in \mathbb{N}$ ותהא E משפחת פונקציות פסודאו אקראיות מגודל $n\cdot\ell+\frac{n}{3}$ אזי $\mathsf{MAC}_k(M_1\ldots M_\ell) = \begin{pmatrix} r \\ E_k(r,M_1,1,\ell) \\ \vdots \\ E_k(r,M_\ell,\ell,\ell) \end{pmatrix}$ באשר $r \leftarrow \{0,1\}^{\frac{n}{3}}$ הינה בעלת חסינות זיוף אימות תחת התקפת גלוי־נבחר.