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 $D(k,E(k,m))=m$.

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 $E_k(m)=E(k,m)$.

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 $D_k(c)=D(k,c)$.

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 $\mathbb{Z}_n^{\leq m}=\bigcup_{i=0}^{m}\mathbb{Z}_n^i$.

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

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

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

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

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

טענה: יהיו $n,m\in\mathbb{N}\setminus\{0,1\}$ 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

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

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 $c=E_{k'}(m')$ 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 $\mathbb{P}_{a\leftarrow\mu}(a)=\mu(a)$.

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

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 $\mathbb{P}_{m\leftarrow\mu}(m=a)=\mathbb{P}_{(m,k)\leftarrow(\mu,\mathcal{K})}(m=a\mid c=E_k(m))$.

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

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

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

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 $|\mathcal{M}|\leq|\mathcal{K}|$.

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)$\iff$($\mathbb{P}(\mathcal{A}$ מנצחת במשחק חוסר ההבחנה$)=\frac{1}{2}$).

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 $\text{Size}(\mathcal{A})=\mathcal{O}(t(n))$.

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

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 $\Delta_{\mathcal{A}}(X,Y)\leq\varepsilon$.

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 $f(X)$ הינה התפלגות על $\{0,1\}^*$ באשר $f(X)(c)=\mathbb{P}_{x\leftarrow X}(f(x)=c)$.

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 $E(\mathcal{K},m)\approx_{t,\varepsilon}E(\mathcal{K},m')$.

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

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

גנרטור פסודאו 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 $G(\{0,1\}^n)\approx_{t,\varepsilon}U_\ell$.

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

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

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

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

משפט: יהיו $n,\ell\in\mathbb{N}$ ויהי $G:\{0,1\}^n\to\{0,1\}^\ell$ גנרטור פסודאו 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 $f(X)\approx_{t-\text{Size}(f),\varepsilon}f(Y)$.

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 $E(k,x)=\begin{pmatrix}E(k,x_1)\\ \vdots\\ E(k,x_n)\end{pmatrix}$.

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 $E(\mathcal{K},x)\approx_{t,\varepsilon}E(\mathcal{K},y)$.

טענה: יהי $n\in\mathbb{N}\setminus\{0,1\}$ 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 $G:\mathcal{L}\to(\mathbb{N}\to\mathcal{L})$ 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 $(\mathcal{K},\mathcal{M},\mathcal{C},\mathcal{L},E,D,G)$.

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 $j\geq L$.