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.

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

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

הצפנת קיסר: יהיו $n,m\in\mathbb{N}_+$ נגדיר $E,D:\{0\ldots n\}\times\mathbb{Z}_n^{\le m}\to\mathbb{Z}_n^{\le m}$ כך

- $(E(k,m))_i=(m_i+k)\%n$ לכל $i\in[|m|]$.
- $(D(k,c))_i=(c_i-k)\%n$ לכל $i\in[|c|]$.

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

הצפנת 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

- $(E(k,m))_i=f_k(m_i)$ לכל $i\in[|m|]$.
- $(D(k,c))_i=f_k^{-1}(c_i)$ לכל $i\in[|c|]$.

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

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 ותהא $\mu:\Omega\to[0,1]$ 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 $\mu:\mathcal{M}\to[0,1]$ ולכל $a\in\mathcal{M}$ 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).

הצפנת 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 הצפנת 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 הצפנת קיסר n הינה הצפנה סימטרית בעלת סודיות מושלמת.

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

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

$\mathcal{A}$ 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

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