

הצפנה סימטרית: תהייה $\mathcal{K}, \mathcal{C} \subseteq \{0, 1\}^*$ קבוצות סופיות תהא $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ ותהא $D : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$ 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 $E, D : \mathbb{Z}_n \times \mathbb{Z}_n^{\leq m} \rightarrow \mathbb{Z}_n^{\leq m}$ כך

• $i \in [|x|]$ 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.

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

• $i \in [|m|]$ לכל $(E_k(x))_i = f_k(x_i)$

• $i \in [|c|]$ לכל $(D_k(c))_i = f_k^{-1}(c_i)$

טענה: יהיו $n, m \in \mathbb{N} \setminus \{0, 1\}$ ותהייה $f_1, \dots, f_n : [n] \rightarrow [n]$ הפיכות שונות אזי צופן הצבה הינה הצפנה סימטרית.

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

• $i \in [|x|]$ לכל $(E_k(x))_i = (x_i + k_i) \% n$

• $i \in [|c|]$ לכל $(D_k(c))_i = (c_i - k_i) \% n$

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

function GenericAttack $((E, D), \mu, c)$:

```

    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 $\mu : \Omega \rightarrow [0, 1]$ 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 $\mu : \mathcal{M} \rightarrow [0, 1]$ 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 $a, b \in \mathcal{M}$ בעלי אורך שווה 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 $\iff (E, D)$ בעלת חוסר הבחנה מושלם.

צופן פנקס חד-פעמי: יהי $n \in \mathbb{N}$ נגדיר $E, D : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ 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( $(E, D), \mathcal{W}, \mathcal{A}$ ):
   $\mathcal{A}$  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 $\iff (\mathbb{P}(\mathcal{A} \text{ מנצחת במשחק חוסר ההבחנה}) = \frac{1}{2})$.

יריב: משפחת מעגלים בוליאניים \mathcal{A} .

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

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

סימון: יהי \mathcal{A} יריב ותהינה 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 $t : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ 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 $\varepsilon \geq 0$ ותהא $t : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ ותהינה X, Y התפלגויות בנ"ל אזי $X \approx_{t, \varepsilon} Y$.

סימון: תהא X התפלגות על $\{0, 1\}^*$ ותהא $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ 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 $t : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ אזי הצפנה סימטרית (E, D) עבורה לכל $m, m' \in \mathcal{M}$ בעלי אורך שווה מתקיים $E(K, m) \approx_{t, \varepsilon} E(K, m')$.

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 $\varepsilon \geq 0$ ותהא $t : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ ויהיו $\ell, n \in \mathbb{N}$ באשר $\ell > n$ אזי $G : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$ 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 $G : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$ גנרטור פסודאו אקראי (t, ε) נגדיר $E, D : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ כך

$$E_k(m) = m \oplus G(k) \quad \bullet$$

$$D_k(c) = c \oplus G(k) \quad \bullet$$

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

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

טענה: יהיו $\varepsilon, \delta \geq 0$ ותהינה $t : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ ותהינה 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 $\varepsilon \geq 0$ ותהינה $t, s : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ ותהינה 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 $\varepsilon, \delta \geq 0$ ותהינה $t, s : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ ותהינה 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 $t : \mathbb{N} \rightarrow \hat{\mathbb{N}}$ אזי הצפנה סימטרית (E, D) עבורה לכל $x, y \in \mathcal{M}^n$ באשר $|x_i| = |y_i|$ לכל $i \in [n]$ מתקיים $E(K, x) \approx_{t, \varepsilon} E(K, y)$.

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

צופן זרם סינכרוני: תהינה $\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathcal{L} \subseteq \{0, 1\}^*$ קבוצות סופיות תהא $G : \mathcal{L} \rightarrow (\mathbb{N} \rightarrow \mathcal{L})$ ותהא $E : \mathcal{L} \times \mathcal{M} \rightarrow \mathcal{C}$ ומקיימות שלמות אזי $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{L}, E, D, G)$.
אוגר הזה בעל משוב ליניארי (LFRS): יהי $L \in \mathbb{N}_+$ יהי $c \in \{0, 1\}^L$ באשר $c_L = 1$ ויהיו s_0, \dots, s_{L-1} אזי $s_j = \bigoplus_{i=1}^L c_i s_{j-i}$ לכל $j \geq L$.