קריפטולוגיה מודרנית

דף עזר למבחן

מבוסס על דף עזר שנכתב על־ידי גיא שקד בשנת 2011.

הצפנת DES

$R_i = L_{i-1} \oplus F\left(R_{i-1}, K_i\right)$,$L_i = R_{i-1}$
:F-function

$$\begin{aligned} input\left(32bits\right) &\rightarrow S_E\left(48bits\right) \oplus subkey\left(48bits\right) \\ &\rightarrow S-boxes \rightarrow P \rightarrow output\left(32bits\right) \end{aligned}$$

<u>תכונת ההשלמה</u> - אם $C = E_K\left(P\right)$ אז $\bar{C} = E_{\bar{K}}\left(\bar{P}\right)$.
התקפה: מבקשים זוגות $C_1 = E_K\left(P\right), C_2 = E_K\left(\bar{P}\right)$, מנסים ערכי K' (שאינם משלימים): אם $E_{K'}\left(P\right) = C_1$ אז יתכן $K = K'$, ואם $E_{K'}\left(P\right) = \overline{C_2}$ אז יתכן $K = \bar{K'}$.

צפני בלוקים - אופני תפעול

כל בלוק מוצפן בנפרד - ECB

$$C_i = E_K\left(M_i\right),\ M_i = D_K\left(C_i\right)$$

לפני ההצפנה כל בלוק מקוסר עם ההצפנה של הבלוק הקודם - CBC

$$C_i = E_K\left(M_i \oplus C_{i-1}\right),\ M_i = D_K\left(C_i\right) \oplus C_{i-1}$$

מחשבים מחרוזת פסאודו־אקראית שתקוסר עם הכתב הגלוי - OFB

$$V_i = E_K\left(v_{i-1}\right),\ C_i = M_i \oplus V_i,\ M_i = C_i \oplus V_i$$

CFB - $C_i = M_i \oplus E_K\left(C_{i-1}\right),\ M_i = C_i \oplus E_K\left(C_i - 1\right)$

צופן מושלם

צופן יקרא מושלם אם לכל M, C מתקיים $p\left(M|C\right) = p\left(M\right)$.
הגדרות שקולות: $\forall M, C:\ p\left(C\right) = p\left(C|M\right)$,

$$\forall M, C:\ p\left(C|M\right) = \sum_{K|E_K(M)=C} p\left(K\right)$$

לכן צופן הוא מושלם אמ"מ לכל C הסכום הנ"ל לא תלוי ב־M.
צופן מושלם מקיים בהכרח - $|K| \geq |M|$

מרחק היחידות

$$N = \frac{\text{key length in bits}}{D} = \frac{H\left(K\right)}{H\left(C\right) - H\left(P\right)}$$

מרחק היחידות הוא האורך של M, C ביחס ל־K שיאפשר זיהוי וודאי של המפתח K בהנתן M, C.
H הוא מדד לאנטרופיה הממוצעת בייצוג של אות. D הוא מדד ליתירות הייצוג, ומוגדר $D \triangleq H\left(C\right) - H\left(P\right)$. באנגלית דרושים 1.5 ביטים לכל אות, לכן בייצוג $ASCII$ למשל - $D_{ASCII} = 8 - 1.5$.

פרדוקס יום ההולדת

כדי למצוא התנגשות בהסתברות גדולה מחצי, בפונקציה בעלת טווח בגודל m מספיק להגריל $1.17 \cdot \sqrt{m}$ קלטים שונים. (עובד גם בהגרלה מ־2 קבוצות שונות.)

חבורות

חבורה $\{G, \cdot\}$ מקיימת -
- סגירות - $\alpha, \beta \in G \Rightarrow \alpha \cdot \beta \in G$
- קיום יחידה - $e \in G$ כך ש־$e \cdot \alpha = \alpha \cdot e = \alpha\ \forall \alpha \in G$
- קיום הפכי - $\alpha \in G \Rightarrow \alpha^{-1} \in G,\ \alpha\alpha^{-1} = \alpha^{-1}\alpha = e$
- אסוציאטיביות $\alpha, \beta, \gamma \in G \Rightarrow \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

תכונות

$G' \subseteq G$ תת חבורה אמ"מ $G' \neq \emptyset$ (ואז $e \in G'$) ומתקיימת סגירות.
סדר של איבר מחלק את סדר החבורה.
אם מתקיים $a^s = e$ אז $order\left(a, G\right)|s$.

פונקציית אויילר

$\varphi\left(n\right) = |\mathbb{Z}_n^*| = |\{i \in \mathbb{Z}_n \mid \gcd\left(i, n\right) = 1\}|$
עבור $n = \prod_i p_i^{e_i}$:
$\varphi\left(n\right) = \prod_i \left(p_i^{e_i - 1}\left(p_i - 1\right)\right) = n \cdot \prod_i \left(1 - \frac{1}{p_i}\right)$
p, q ראשוניים, a, b, n שלמים. מתקיים -
$\varphi\left(p\right) = p - 1$
$\varphi\left(p^a\right) = \left(p - 1\right)p^{a-1} = p^a - p^{a-1}$
$\varphi\left(pq\right) = \left(p - 1\right)\left(q - 1\right)$
$\gcd\left(a, b\right) = 1 \Longrightarrow \varphi\left(ab\right) = \varphi\left(a\right)\varphi\left(b\right)$
$\sum_{d|n} \varphi\left(d\right) = n$
$a^p \equiv a \pmod{p}$ (המשפט הקטן של פרמה.)
$\gcd\left(a, n\right) = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 \left(\mathrm{mod} n\right)$

משפט השאריות הסיני

$\mathbb{Z}_{pq}^* \cong \left(\mathbb{Z}_p^* \times \mathbb{Z}_q^*\right)$ וניתן לחשב את המעבר בין החבורות בקלות.
באופן שקול: קיים הומומורפיזם $h : \mathbb{Z}_{pq}^* \rightarrow \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.
ההומומורפיזם מוגדר כך: $h(u) = \left(u \pmod{p}, u \pmod{q}\right)$.
<u>אלגוריתם</u> (למעבר מאגף ימין לשמאל). מחשבים a, b כך ש־

$$\begin{aligned} a &\equiv 1 \pmod{p} \qquad a \equiv 0 \pmod{q} \\ b &\equiv 0 \pmod{p} \qquad b \equiv 1 \pmod{q} \end{aligned}$$

על ידי - $a = q \cdot \left(q^{-1} \pmod{p}\right)$ ו־$b = p \cdot \left(p^{-1} \pmod{q}\right)$.
ואז - $(s, t) \longrightarrow a \cdot s + b \cdot t$.

חבורות מהצורה $\mathbb{Z}_n^*$

לאיבר a יש הופכי ב־$\mathbb{Z}_n^*$ אמ"ם $gcd(a, n) = 1$.
$order(a, \mathbb{Z}_n^*)|\varphi(n)$, ואם n ראשוני אז מתקיים $order(a, \mathbb{Z}_n^*)|\left(n - 1\right)$.
כאשר n ראשוני ו־$d \mid \left(n - 1\right)$, מספר האיברים מסדר d ב־$\mathbb{Z}_p^*$ הוא $\varphi\left(d\right)$. בפרט מספר היוצרים הוא $\varphi\left(\varphi\left(p\right)\right) = \varphi\left(p - 1\right)$.
<u>משפט וילסון</u> - $1 \cdot 2 \cdot 3 \cdots (p-1) \equiv -1 \pmod{p}$.

שאריות ריבועיות ($p \neq 2$)

יש $\frac{\varphi(p)}{2} = \frac{p-1}{2}$ שאריות ריבועיות ב־$\mathbb{Z}_p^*$
<u>קריטריון אויילר</u> - $a \in \mathbb{Z}_p^*$ שארית ריבועית אמ"מ $a^{\frac{p-1}{2}} \equiv_{(p)} 1$.
<u>עבור $n = pq$</u> - אם $a \in \mathbb{Z}_n^*$ שארית ריבועית אז יש לו 4 שורשים ריבועיים.
לכן - יש בדיוק $\frac{\varphi(n)}{4}$ שאריות ריבועיות ב־$\mathbb{Z}_n^*$.

חישוב שורש מודולו p

- $p = 4k + 3$ - $\sqrt{a} = a^{\frac{p+1}{4}}$
- $p = 4k + 1$ - אלגוריתם הסתברותי -
  - מוצאים באקראי b שאיננו שארית ריבועית.
  - מאתחלים - $0 \rightarrow t, 2k \rightarrow i$
  - כל עוד i זוגי -
    - $t \rightarrow \frac{t}{2}$,$i \rightarrow \frac{i}{2}$
    - אם $a^i b^t \equiv -1$ אז $t + 2k \rightarrow t$.
  - החזר $a^{\frac{i+1}{2}} \cdot b^{\frac{t}{2}}$.

סימן לג'נדר

$$\left(\frac{a}{p}\right) \triangleq \begin{cases} +1 & a \text{ is a quadratic residue mod } p \\ -1 & a \text{ is a quadratic non-residue mod } p \end{cases}$$

ע"פ אויילר - $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
לכל c מתקיים - $\left(\frac{c^2}{p}\right) = \left(\frac{1}{p}\right) = 1$

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & p=4k+1\\ -1 & p=4k+3\end{cases}$$
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$
$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$
אם p,q ראשוניים אי זוגיים - $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

סימן יעקובי

$n=p_1\cdot p_2\cdots p_k$ אי־זוגי. a זר ל־n. סימן יעקובי מוגדר -
$$\left(\frac{a}{n}\right)\triangleq\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$
a הוא שארית ריבועית מודולו n אמ"מ $\left(\frac{a}{p_i}\right)=1$ לכל i. לכן - אם $\left(\frac{a}{n}\right)=-1$ נדע בוודאות ש־a הוא לא שארית ריבועית. אבל $\left(\frac{a}{n}\right)=1$ לא מבטיח ש־a הוא שארית ריבועית.

1 הוא שארית ריבועית לכל n. בפרט - $1=\left(\frac{c^2}{n}\right)=\left(\frac{1}{n}\right)$.
$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$$
$$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$$
$$\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$
$$\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$
אם m,n זרים ואי זוגיים - $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$
חישוב יעיל דורש $O\left(\log^2 n\right)$ פעולות מודולריות.

תורת המספרים

a,b זרים $\Leftrightarrow\exists x,y\mid ax+by=1$
a,b זרים ו־$a\mid bc\Leftarrow a\mid c$
$m|\alpha a+\beta b\forall\alpha,\beta\in\mathbb{Z}\Leftarrow m\mid a,\ m\mid b$
$\gcd(a,b)=\min\{ax+by>0\mid x,y\in\mathbb{Z}\}$
$\operatorname{lcm}(a,b)=\min\{c>0|a\mid c,\ b\mid c\}$
$m\mid\gcd(a,b)\Leftarrow m|a,\ m|b$
$\gcd(ma,mb)=|m|\cdot\gcd(a,b)$

אלגוריתם אוקלידס מוצא gcd, וניתן להשתמש בו למציאת הופכי מודולרי. סיבוכיות $O(\log n)$.
ל־a קיים הופכי $\bmod n\Leftrightarrow\gcd(a,n)=1$.

הצפנת RSA

p,q ראשוניים גדולים, $n=pq$.
e זר ל־$\varphi(n)$. $d=e^{-1}\pmod{\varphi(n)}$.
(n,e) מפתח פומבי, d סודי.
הצפנה $C\leftarrow M^e\pmod n$. **פענוח** $M\leftarrow C^d\pmod n$.
תכונות:
תכונת הכפל - $E(m_1\cdot m_2)=E(m_1)\cdot E(m_2)$ הצפנה משמרת
סימן יעקובי - $\left(\frac{m}{n}\right)=\left(\frac{m^e}{n}\right)$
ביטים קשים (hardcore) - lsb, half
שורש יחידה לא טרוויאלי ($\alpha^2=1,\alpha\neq\pm1$) מאפשר פירוק לגורמים ראשוניים.
הוצאת שורש מודולרי מאפשרת פירוק לגורמים ראשוניים:
אם $a^2=b^2$ אז $\gcd(a-b,n)$ ו־$\frac{n}{\gcd(a-b,n)}$ הגורמים הראשוניים.

חתימות RSA

- תהליך החתימה: $S=D_A(m)\equiv M^{d_A}$.
- ווידוא חתימה: $M\stackrel{?}{=}E_A(S)\equiv S^{e_A}$.

הוכחה באפס ידע

מושלם - פלט הסימולטור בעל התפלגות זהה לפלט "אמיתי".
חישובי - לא ניתן להבחין (חישובית) בין התפלגות פלט הסימולטור והתפלגות הפלט של מוכיח אמיתי, כלומר יתכן הבדל זניח ביניהם.
אם משתמשים ב־Bit-commitment בפרוטוקול ZK, חייבים להבטיח כבילה מושלמת כי המוכיח לא מוגבל חישובית. לכן הסודיות חישובית ולכן הפרוטוקול יהיה ZK חישובי ולא מושלם.
אפס־ידע **חישובית**: Graph 3-Colorability.

קריפטאנליזה דיפרנציאלית

תכונה בת n שלבים היא - $\Omega=(\Omega_P,\Omega_\Lambda,\Omega_T)$ כך ש:

- Ω_P - m ביטים, הפרש הקלט (לפני הצפנה)
- Ω_T - m ביטים, הפרש הפלט (אחרי הצפנה)
- $\Omega_\Lambda=(\Lambda_1,\Lambda_2,\dots\Lambda_n)$ שלבי הביניים. כל אחד מהם:
  - $\Lambda_i=\left(\Lambda_I^i,\Lambda_O^i\right)$ (קלט ופלט של השלב, בני $\frac{m}{2}$ ביט)

ומתקיים -
- Λ_I^1 - החצי הימני של Ω_P
- Λ_I^2 - (החצי השמאלי של Ω_P)$\oplus\Lambda_O^1$
- Λ_I^n - החצי הימני של Ω_T
- Λ_I^{n-1} - (החצי השמאלי של Ω_T)$\oplus\Lambda_O^n$
- לכל $2\leq i\leq n-1$ מתקיים - $\Lambda_O^i=\lambda_I^{i-1}\oplus\lambda_I^{i+1}$

זוג נכון ביחס לתכונה Ω ומפתח K הוא זוג קלטים שההפרש ביניהם הוא Ω_P וכן כל ההפרשים בשלבי הביניים מתאימים למתואר בתכונה.
הסתברות של תכונה היא ההסתברות שזוג קלטים שמתאים ל־Ω_P הוא זוג נכון (ביחס לכל המפתחות).
דיפרנציאל הוא קבוצת כל התכונות שיש להן Ω_P, Ω_T זהים ומספר שלבים זהה. הסתברות של דיפרנציאל הוא סכום הסתברויות התכונות.
התכונה האיטרטיבית $\Omega_P=(19\ 60\ 00\ 00_x,\ 00\ 00\ 00\ 00)$ נכתבת גם $\Omega_P=(\psi,0)$. תכונה בת שני שלבים, בהסתברות $\frac{1}{234}$. $\Omega_T=(0,\psi)$ כך שניתן להרכיב אותה על עצמה. שרשור של התכונה ל־17־16 שלבים מניבה תכונה בעלת הסתברות של $2^{-62},2^{-63}$ בהתאמה.
הערה: כדי לקבל אותו פלט של F שני קלטים צריכים להבדל לפחות ב־3 S-boxes.
התקפת $0R$ דורשת $2\cdot p^{-1}$ זוגות קלטים (p - הסתברות התכונה) מהם ישארו 2 זוגות נכונים.

שיתוף סוד

סכימת שיתוף סוד:
- n שחקנים, כל אחד מקבל שתף (Share).
- שיתוף פעולה של קבוצות שהוגדרו מראש מאפשר לשחזר הסוד.
- כל קבוצה שלא הוגדרה מראש לא יכולה ללמוד דבר על הסוד.

סכימת סף (k,n) קבוצה יכולה לשחזר את הסוד רק אם גודלה לפחות k.

פונקציות תמצות

- ריפוד מרקל־דמגרד: בהנתן הודעה M מרפדים את M בשביל שאורכה יהיה כפולה של אורך הבלוק. בריפוד כוללים את האורך הסופי של ההודעה.
- מבנה מרקל־דמגרד: $h_i=H(h_{i-1},M_i)$ כאשר $h_0=IV$ ו $h(M_1\cdots M_n)=h_n$.

התחייבות הדדית

כבילה מושלמת: המתחייב שולח $g^r\bmod p$ (r זוגי\אי־זוגי בהתאם ל־S). המתחייב לא יכול לרמות (לחשוף ערך אחר), אבל המקבל יכול לחשב את S.
התחייבות מושלמת: שולח $g^Sh^r\bmod p$ (g,h יוצרים של חבורה של איברים מסדר $q\mid p-1$). המקבל לא יכול לחשב את S אבל המתחייב יכול לחשוף S,r אחרים.
הטלת מטבע (ביט) משותף: כל אחד מתחייב על ביט ושולח, אח"כ חושפים הביטים והמטבע יהיה $b=b_A\oplus b_B$.
OT: B לומד ביט בהסתברות $1/2$, A לא יודע אם B למד את הביט.
OT_1^2: B לומד אחד משני סודות לבחירתו. A לא יודע איזה סוד B למד.
יישומים: bit commitment, הוכחות אפס ידע לא אינטראקטיביות.