יסודות הקריפטוגרפיה שיעור #4

חיזוק הצפנת *Block Cipher* נתונה:

שימוש באותו בלוק הצפנ ה אך בצורה מאובטחת יותר, למשל שימוש במפתח כפול או משולש ושיטות נוספות שיפורטו.

Iterated Ciphers:

שימוש באותו בלוק יותר מפעם אחת עם שני מפתחות שונים: $P \to E_{k_1} \to E_{k_2} \to C$. מרחב המפתחות עבר מגודל n ביטים לגודל $2n$ ביטים, כלומר זמן הפיצוח הנאיבי עולה מ-$O(2^n)$ ל-$O(2^{2n})$. בעיות: אם פונקציית ההצפנה סגורה תחת הרכבה, שימוש בשני מפתחות שונים שקולה לשימוש במפתח אחד, למשל XOR: $P \oplus k_1 \oplus k_2$ שקולה ל-$P \oplus k_3$ כאשר $k_3 = k_1 \oplus k_2$.

Meet in the middle attack:

נתון זוג x, y טקסט רגיל ומוצפן כך ש- $E_{k_2}\left(E_{k_1}(x)\right) = y$. מראש יש $2^n \cdot 2^n$ זוגות פוטנציאלים (k_1, k_2). ההתקפה תצמצם את מספר הזוגות האפשריים (לבערך 2^n). נשתמש אח"כ בזוגות נוספים כדי לצמצם את הרשימה עד לזוג יחיד.

עבור x קבוע, לכל מפתח k_1 מחשב את $z_{k_1} := E_{k_1}(x)$, ונאחסן את הזוגות (z_{k_1}, k_1) ברשימה L_1 ממויין ע"פ z_{k_1}. זמן $O(n \cdot 2^n)$ וזיכרון $O(n \cdot 2^n)$ ביטים לכל הרשימה. עבור y קבוע, כעת נעבור על כל ה-k_2 ונחשב את $t_{k_2} := D_{k_2}(y)$. נמיין את L_2 עם האיברים (t_{k_2}, k_2) לפי t_{k_2}. לגבי ה"זוג הנכון" יודעים שיתקיים $z_{k_1} = t_{k_2}$. ה"פגישה" תתקיים כנראה ביחס לזוגות מפתחות נוספים (כאילו מתקדמים מ-x צעד קדימה ומ-y צעד אחורה). נשתמש ב-(x, y) נוספים כדי להתבית על k_1, k_2 הנכונים. כיוון שהרשימות ממויינות נוכל למצוא את כל הזוגות השווים בזמן $O\big(length(L_i) \cdot time(compaing\ two\ word\ of\ n\ bits)\big) = O(2^n)$.

אינטואיציה לניתוח שיטה זו:

מחזיקים x קבוע, עוברים על כל k_1 ומסתכלים על $E_{k_1}(x) \in \{0,1\}^n$ כפונקציה של k. הנחה סבירה: כמו פונקציה אך לא תמורה אקראית. ההסתברות ש-$E_{k_1}(x) = D_{k_2}(y)$ היא $\frac{1}{2^n}$. מספר הזוגות k_1, k_2 הוא 2^l אז תוחלת מספר הזוגות שמקיימים את השוויון הנ"ל היא 2^{2l-n}, וזהו מספר ההתנגשויות שאנו מצפים למצוא בין הרשימות L_1, L_2 עבור זוג טקסט רגיל-מוצפן בודד (x, y). אם $l = n$ אז תוחלת מספר ההתנגשויות הוא $2^{2n-n} = 2^n$. עבור שני זוגות $(x_1, y_1), (x_2, y_2)$ הסיכוי לשוויון הוא $\frac{1}{2^n}$. מהנחת אי תלות, הסיכוי לשניהם הוא $\frac{1}{2^{2n}}$ (הנחה חזקה). לכן תוחלת מספר ההתנגשויות לשני זוגות $(x_1, y_1), (x_2, y_2)$ תהיה 2^{2l-2n} ולזה נקבל זוגות אפשריים בודדים של k_1, k_2 ואם ניקח עוד נתמקד עוד יותר לזוג הנכון. חשבון זה הוא היוריסטי (כלומר שקרי) אך מתברר שעובד.

Triple Cipher:

$P \to E_{k_1} \to D_{k_2} \to E_{k_3} \to C$: על גבי השיטה הקודמת נוסף שלב הצפנה E_{k_3} עם מפתח k_3. ניתן גם כאן לנסות להיפגש באמצע, אך מצד אחד יהיו שני מפתחות ומצד שני אחד, והסיבוכיות פה תהיה בהתחשב במפתח באורך $2n$.

From encryption to authentication:

- אלגוריתם אימות A
- אלגוריתם וידוא V
- מפתח אימות משותף k
- מרחב הודעות
- כל הודעה בין שני המתקשרים היא זוג $\big(m, A_k(m)\big)$ (m הודעה ב-*plaintext*)
- $A_k(m)$ הוא *authentication tag* של m

דרישות:

- קונסיסטנטיות: $V_k\big(A_k(m)\big) = accept$
- אלגוריתם האימות מסומן MAC, ו-$A_k(m)$ יסומן $MAC_k(m)$

תחת מגבלות חישוביות של היריב לזמן פולינומיאלי למשל, נרצה שהיריב לא יוכל אלא בהסתברות זניחה לבנות זוג מתאים $\big(m, MAC_k(m)\big)$ אפילו לאחר שרואה n זוגות אמיתיים. הפלט הוא קצר ככל האפשר ו-MAC אינו אלגוריתם חח"ע.

האינפורמציה שיש ליריב הוא אלגוריתם ה- MAC, אך כמובן לא המפתח. מניחים כי היריב רואה את ההודעות. בהינתן $\left(m_1, MAC_k(m_1)\right), \dots, \left(m_n, MAC_k(m_n)\right)$ המטרה של היריב למצוא זוג חדש חוקי $\left(m, MAC_k(m)\right)$ ביעילות ובהסתברות לא זניחה.

שימושי *MAC* :

תיאור MAC מבוסס CBC ו-MAC מבוסס על פונקציות $hash$ קריפטוגרפיות.

<u>מבוסס CBC</u> :

בשיטה מבוססת CBC עם הבלוקים $M_1, \dots, M_n$, ניצור $C_1, \dots, C_n$, נזרוק את כל מה שיצרנו פרט לאחרון ונוציא את ההודעה $M_1, \dots, M_n$ יחד עם $MAC_k(M) = C_n$ שיצרנו (כאן אנו שולחים את ההודעה עצמה שהיא סדרת $M_1, \dots, M_n$ לא מוצפנת). שיטה זו טובה אם מספר הבלוקים המרכיבים את ההודעה הוא קבוע וידוע מראש, אך לא בטוח כאשר מספר הבלוקיםn לא ידוע מראש. דוגמא לזיוף במקרה של גודל לא קבוע מראש :

- תחילה נשלח (M_1, C_1) כאשר C_1 הוא הטאג של M_1.
- לאחר מכן נשלח (C_1, C_2) כאשר C_1 ההודעה שלנו – ההודעה הקדומת עם הטאג שלה, ו-C_2 הטאג של הודעה זו.

כעת ניתן לזייף אימות להודעה בת שני בלוקים :$\left(M_1 \circ \vec{0}\ , C_2\right)$ - שרשור ההודעה עם ההודעה הריקה,ף והטאג הוא מה שהיה קודם.

שיטות שונות להתמודד עם בעיותיות זו : במצגת.

<u>פונקציות $hash$ קריפטוגרפיות</u> :

...