מבוא לקריפטוגרפיה מודרנית (0368-3049)

נכתב ע"י רון גולדמן
ע"פ הרצאות של פרופ' בני אפלבאום

28 באוקטובר 2025

תוכן העניינים

פרק 1

מבוא

1.1 הצפנה

הגדרה 1.1 [פונקצית הצפנה]. $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$.

הגדרה 1.2 [פונקצית פיענוח]. $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

נניח והמפתח $k \sim \mathrm{Unif}(\mathcal{K})$.
מרחב ההודעות $\mathcal{M} = \{0,1\}^*$.
הרבה פעמים אורך ההודעות קשור למרחב המפתחות.
נכונות: לכל $m \in \mathcal{M}, k \in \mathcal{K}$

$$D_k(E_k(m)) = m$$

1.2 מודל התקשורת

- שתי צדדים - אליס ובוב
- קו תקשורת אמין
- סכמת הצפנה משותפת: E, D, k.
- מטרה: לשלוח בבטיחות הודעה m.

1.3 מטרות אבטחה

יש מספר מטרות שנרצה להשיג

- אף יריב לא יכול לקבוע את m
- אף יריב לא יכול לקבוע אף אינפורציה לגבי m
- אף יריב לא יכול לקבוע אינפורציה משמעותית לגבי m

שאלות חשובות:

- מה היריב יודע מראש?

- מה המגבלות החישוביות של היריב?

האם בכלל אפשר לפרמל מתמטית את מושג הסודיות?

1.4 מודל היריב: מאזין פאסיבי

איב מאזינה לערוץ התקשורת.

- איב מנסה לגלות אינפורציה לגבי m
- איב יודעת את האלגוריתמים E, D (עיקרון קרכהוף)
- איב יודעת את מרחב ההודעות
- איב תפסה את $E_k(m)$
- איב לא יודעת את k