20.10.2014

סיכום שיעור

התעכבנו בין היתר על פתרון השאלה שניתנה כשיעורי בית:

כתוב/כתבי שאילתה שתתן את רשימת שמות הסטודנטים ששאלו ספר שכתב המחבר Sam Wang , וגם לא שאלו ספר של המחבר Sherman Chow

על מנת לפתור השתמשנו, בין היתר במילת המפתח: Except אשר 'מחסירה' תוצאות שאילתה אחת מאחרת בצורה הבאה:

```
select sname from student
where id in
   (select id
    from book bk, borrow br
    where bk.isbn = br.isbn and author = 'Sam Wang')
except
select sname
from student where id in
   (select id from book bk, borrow br where bk.isbn =
    br.isbn and author = 'Sherman Chow');
```

בכתה הועלו רעיונות לפיתרון שונה כגון:

```
select sname from student
where id in
   (select id
    from book bk, borrow br
    where bk.isbn = br.isbn and author = 'Sam Wang'
    and author not = 'Sherman Chow')
```

שהתגלה כפיתרון סרק כיוון שאותו שדה (עמודה) של author אם משוים אותו לערך אחד (Sam Wang) ומוסיפים תנאי נוסף של אי שיוויון של אותו שדה לערך אחר ('Sherman Chow') , הרי מובן מאליו שהתנאי השני מתמלא, אם הראשון נכון, ולכן בהכרח התנאי השני אינו מגביל את בחירת השורות מעבר למה שהתנאי הראשון יצר. ולכן אין לנו ברירה, אלא לייצר שאילתה נוספת שתענה על התנאי השני בניפרד , ואז "להחסיר" את השנייה מהראשונה.

שאלה נוספת שניתנה כתרגיל בכתה הייתה:

מצא את מספרי הזהות של כל התלמידים ששאלו לפחות ספר אחד מספריה שממוקמת בעיר מגוריהם (כלומר לכל תלמיד עיר מגוריו.

כיוון שהרבה התקשו למצוא את הפיתרון היחסית לא מסובך, הגעתי למסקנה שהכתה צריכה תירגול נוסף (ביטוי מכובס ל 'טירטור' בצבא, אבל אנחנו לא בטירונות) לפני שהופכים לאשפי SQL, וכך נעשה.

20.10.2014

התחלנו לדבר על נושא של הצפנה ובטיחות מידע ואמרנו ש:

נדבר על 3 סוגי הצפנה:

1. הצפנה סימטרית
2. הצפנה על פי מפתח ציבורי ומפתח פרטי
3. טביעת אצבע (פונקצית האש לכיוון אחד) או Digest עבור הודעה. טביעת האצבע נישלחת בחלקו התחתון של אותו מסמך, message ו- digest יכולים להישלח בניפרד.

דוגמה להצפנה סימטרית - ברומא העתיקה השתמש יוליוס קיסר בשיטה של החלפת כל אות באות שהיא 3 קדימה, כלומר A הפכה ל- D בצורה סירקולארית, כלומר Z הפכה ל- C. כלומר קוד ההצפנה הוא 3 קדימה.
מזה אנחנו מסיקים שקוד הפיענוח הוא 3 אחורה. שיטת הצפנה כזו ניקראת סימטרית (אם ורק אם אפשר להסיק מ - d את e) e זה encryption ו- d זה decryption.

כדי להשתמש בהצפנה סימטרית יעילה, הצופן צריך להיות סודי (אפשר ליצור צופן מסובך שקשה לשבור, אבל צריך להסתיר אותו).

אם לא ניתן להסיק מ- e את d, אפשר ש- e יהיה מידע ציבורי כך שכל אחד יוכל להצפין את הודעתו, ורק זה שיש לו את קוד הפיענוח - d יוכל לקרוא את ההודעה. **שיטה זו ניקראת: public/private**

בחלק ב של הרצאה זו, נתאר אלגוריתם בשם RSA שמיועד ליצור שיטה של: **public/private**

(RSA- זה **לא** רוחמה/ שוצמן /אשר - גם אם היו רוצים מאד :)

ישנה שיטת הצפנה סימטרית שאפשר לאמר שהיא בטוחה לחלוטין (מבחינה הסתברותית), אולם אינה שימושית במיוחד.

כשהתחלנו לדבר על קוד בינארי ו- ASCII, התגלתה לנו עובדה לא מרנינה. רוב התלמידים בהו באוויר וטענו שאיבדו קשר עם המורה.

כדי להחזיר את הקשר, למדנו על קצה המזלג את שיטת הספירה הבינארית ועל הקצה של הקצה של המזלג גם את שיטת הספירה ההקסה דצימלית (והקשר האמיץ ביניהן). זו הייתה סטייה קלה מנושא ההצפנה, אבל לא ניתן ללמד חשבון דיפרנציאלי את מי שלא יודע חיבור וחיסור (גם אם משתדלים מאד).

זה בסדר, מידי פעם נגלה פערים בין הידע שניצבר והנושא עליו דנים, כך שכפי הניראה השלמות ידע יהפכו לשיגרה אצלנו, ונקווה שזה יועיל בבוא הזמן לכולם.