הצפנה

אולימפידע 2007

"עולמות של תקשורת"

אדיר גרוס

הקדמה - אינטרנט

Internet

כרטיסי אשראי

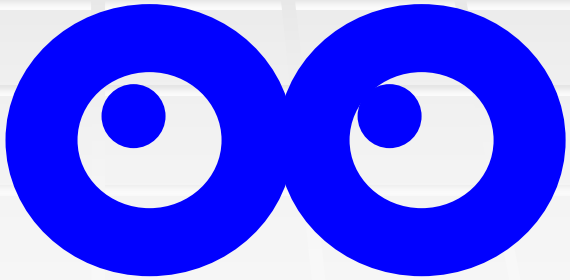
תעודות זהות

השבון בנק

דוגמא

B → www.store.com

B → כרטיס אשראי → www.store.com



$$$

מהי הצפנה?

הסתרת המשמעות של **מסר** *קריא*

והפיכתו בעזרת שיטה מתמטית

לטקסט מוצפן

אותו יכול לפענח ולשחזר

*רק מי שבידיו ה***מפתח** *המתאים*

מטרות ההצפנה

- פרטיות
- אימות
- שלמות מידע

צפנים קלאסיים

- צופן קיסר
- צופן ויז'נר
- צופן ורנם
- צופן רוטור – אניגמה

צפנים מודרניים

- סימטריים : RC4, DES, AES
- א-סימטריים: RSA

צפנים סימטריים

- *המפתח הדרוש להצפנה זהה למפתח הדרוש לפיענוח*

צופן זרם – RC4

ריבסט (1987)

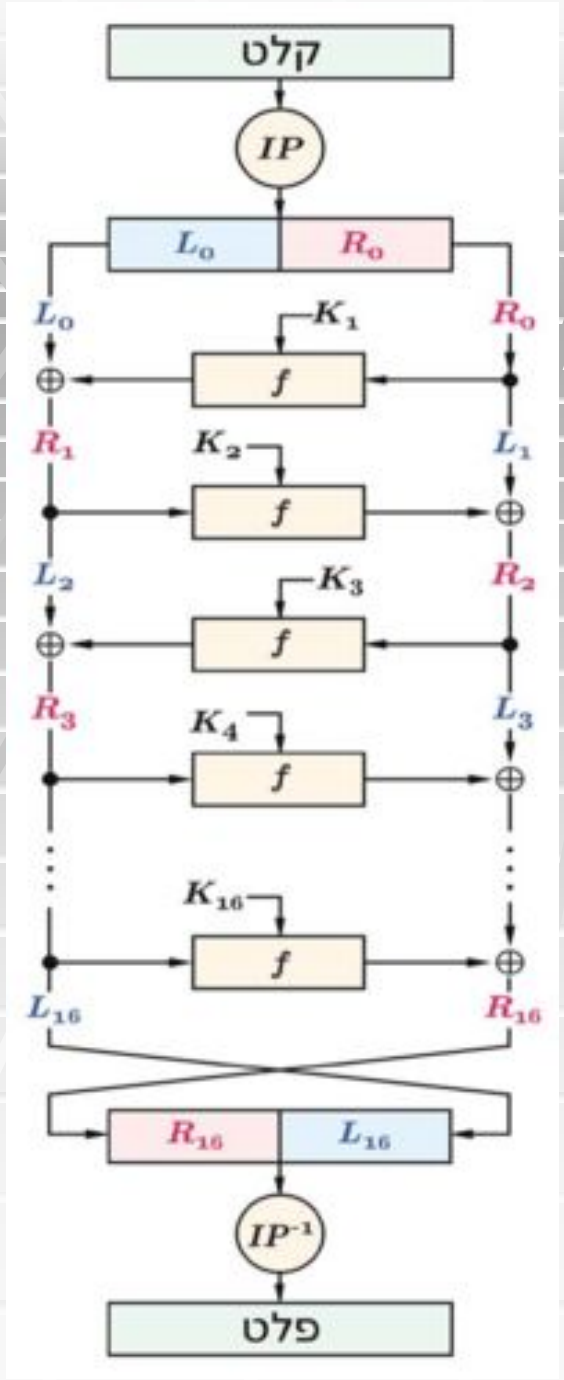
- צופן זרם (Stream Cipher) הוא צופן סימטרי המצפין באמצעות ביצוע פעולות על סיביות בודדות
- RC4 הוא צופן זרם מבוסס תוכנה
- נמצא בשימוש נפוץ בפרוטוקולי אבטחה כמו SSL לאבטחת הרשת ו WEP (אבטחת רשת אל-חוטית)

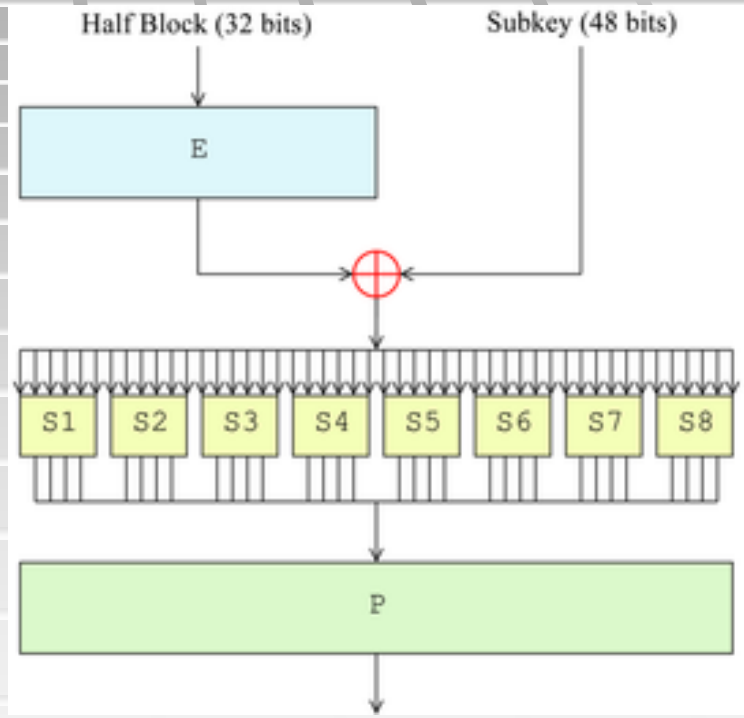
Data Encryption Standard (DES)

1975 IBM

- התקבל ב- 1976 כתקן האמריקאי להצפנה אזרחית
- נמצא בשימוש נרחב
- צופן בלוקים
- קל ליישום

DES (המשך)


קלט
IP
L_0
R_0
K_1
f
K_2
K_3
K_4
K_{16}
L_1
R_1
L_2
R_2
L_3
R_3
L_{16}
R_{16}
IP^{-1}
פלט


Half Block (32 bits)
Subkey (48 bits)
E
S1
S2
S3
S4
S5
S6
S7
S8
P

Advanced Encryption Standard

- צופן Rijndael הומצא ע"י שני קריפטוגרפים מבלגיה
- נבחר כשימוש לתקן מתוך 15 צפנים
- נקבע כתקן בשנת 2001
- פשוט, עמיד ויעיל

הצפנה סימטרית (סיכום)

יתרונות הצפנה סימטרית:

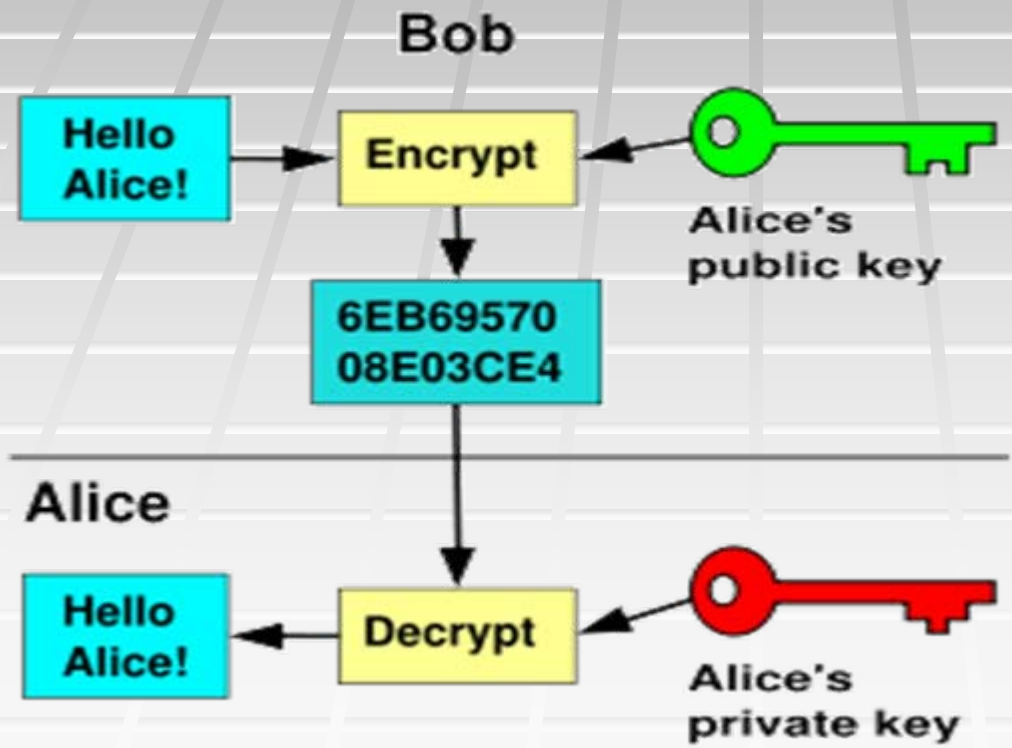
- *מהירות ויעילות*
- *מפתח קצר*

חסרונות הצפנה סימטרית:

- *קושי בשיתוף המפתח*
- *לא מעשי במערכות מרובות משתתפים*
- *צורך בהחלפת מפתחות לעיתים קרובות*

הצפנה א-סימטרית

המפתח המשמש להצפנה **שונה** *מהמפתח המשמש לפיענוח*



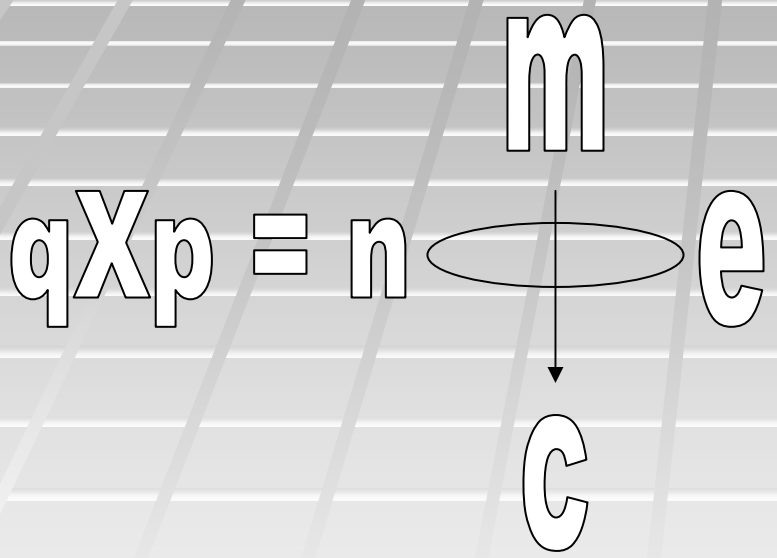
RSA

- הומצא על ידי רונלד ריבסט, עדי שמיר ולאונרד אדלמן ב- 1977, ועליה הם קיבלו את פרס טורינג

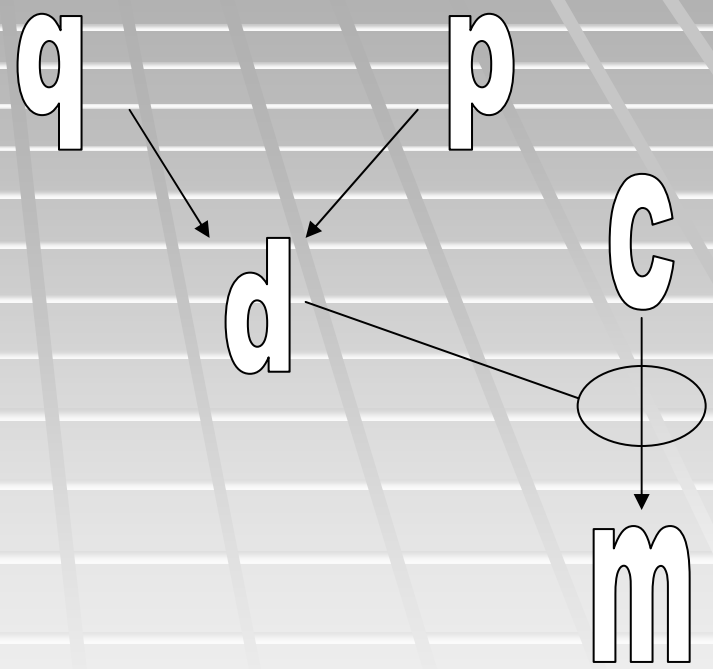
- פריצת דרך להצפנה מודרנית
- נחשב לאלגוריתם בטוח
- נפוץ כיום באבטחת מידע, בתקשורת מחשבים ובמסחר אלקטרוני

RSA (המשך)

הצפנה



פיענוח



הצפנה א-סימטרית (סיכום)

יתרונות הצפנה א-סימטרית :

- *המפתח הפרטי צריך להישמר בסוד והוא לא מועבר*
- *ניהול ותחזוקה קלים, במיוחד ברשתות גדולות*
- *המפתח נשמר לאורך זמן*
- *אפשרות לוידוא זהויות*

חסרונות הצפנה א-סימטרית :

- *איטית*
- *מפתח ארוך מאוד*
- *השיטה המתמטית לא הוכחה ופתרון לה יכול עדיין להימצא*

מערכות היברידיות

- *מערכת המשלבת הצפנה סימטרית עם הצפנה א-סימטרית*

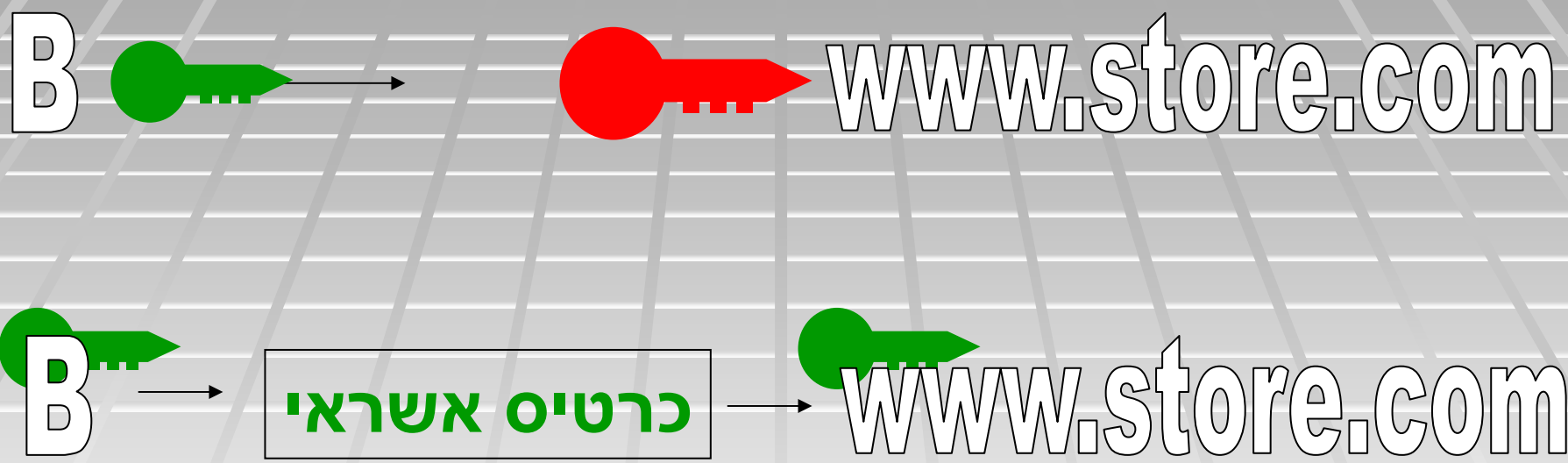
- *העברה של המפתח בתקשורת גלויה מתבצעת בעזרת שיטה א-סימטרית כמו RSA ולהצפנה עצמה וההצפנה עצמה נעשית באמצעות הצפנה סימטרית כמו AES*

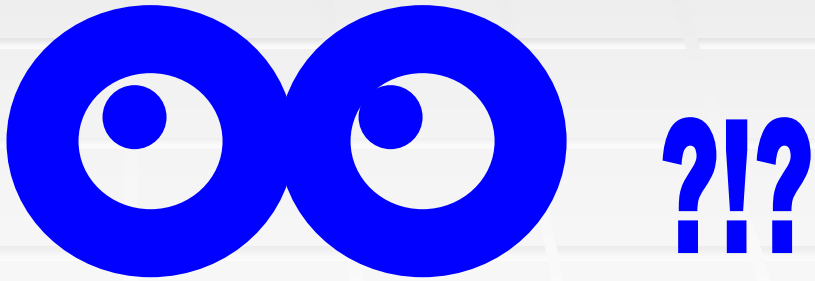
- *לדוגמא: PGP ו-SSL*

SSL

- דרך נפוצה לאבטחת מידע על גבי רשת האינטרנט
- מערכת היברידית
- יכול להשתמש כמעט בכל צופן
- מיושם בעיקר בדפדפן

תהליך ההצפנה המלא





?!?

סיכום

- *ההצפנה חשובה* **בתקשורת ובאבטחת מידע**

- *ההצפנה היא חלק חשוב לתפעול הצבא*

- *הצפנה היא* **תחום אקדמי**

- *ההצפנה היא חלק חשוב* **בתקשורת האינטרנט**

ביבליוגרפיה

- *ויקיפדיה, האינציקלופדי החופשית en/he.wikipedia.org*
- *אתר ההכנה לאולימפידע*
- *סודות ההצפנה - מאת סיימון סינג*
- *Cryptology – Prof. Eli Biham, CS Department Technion, June 1999*
- *Cryptography from A to Z, Feb. 2007*

מכללת הי-טק