שבירת צופן RC4

מבוא

צופן RC4 מדליף מידע על המפתח הסודי כפי שהוסבר בהרצאה. בפרט ניתן להשתמש בעובדה זו ובידע על מבנה ההודעה שמועברות בפרוטוקול WEP, כדי למצוא את המפתח ששימש להצפנה. בפרוטוקול WEP, הבית הראשון בכל הודעה גלויה הוא AA (בבסיס 16). ניתן להשתמש במידע זה ובהקלטה של הרבה הודעות מוצפנות כדי לגלות את 5 הבתים של המפתח הסודי בית-אחרי-בית.

הוראות

יחד עם דף הסבר זה תמצאו קובץ בשם wep.out. קובץ זה מכיל 500,000 הודעות WEP שהוצפנו באמצעות הצופן RC4. אורך כל הודעה מוצפנת הוא 7 בתים: 3 בתים של וקטור האתחול (IV) ואחריהם 4 בתי צופן.

עליכם לכתוב תכנית שמוצאת את המפתח ששימש להצפנת ההודעות. התכנית לא תקבל פרמטרים. התכנית תניח שבתיקיה שממנה היא מורצת קיים קובץ wep.out כמתואר. התכנית תדפיס (רק) את המפתח ששימש להצפנה בכתיב הקסדצימלי ללא 0x ועם רווחים בין הבתים, לדוגמא: AA BB CC DD EE.

כדי לוודא שהמפתח שמצאתם נכון השתמשו בזוג ההודעות הבא שמובא להלן.
הודעה גלויה: AA AA 03 00 00 00 08 06
הודעה שהוצפנה עם המפתח הסודי ווקטור האתחול 00 00 00: a9 52 ae 67 3d 92 d8 cc

הוראות הגשה

1. יש להגיש קובץ ZIP שמכיל
   1. קובץ מקור של התכנית
   2. הוראות קומפילציה והרצה
   3. צילום מסך של הפעלת התכנית בו נראית ההדפסה של המפתח הסודי
2. שם הקובץ צריך לכלול את מספרי ת.ז. של כל חברי הקבוצה.

בהצלחה!