

**הסבר קצר להתקפה:**

אז אנחנו בעצם נתקלים פה בהתקפה דומה להתקפה הבסיסית. החולשה שננצל היא שבפדינג שמשתמשים בpkcs v2 הסוד חייב להתחיל ב00 והסרבר שהקוד שלנו פונה אליו עונה לנו האם הפדינג חוקי או לא חוקי. הסוד שלנו הוא , ואנחנו מצאנו את ההצפנה שלו  כאשר האזנו ברשת. נשים לב שאם ניקח מספר a ונשלח אותו בצורה הבאה לסרבר . הסרבר ינסה לעשות פענוח ויודיע לנו במקרה שההצפנה בלתי חוקית

 כלומר מצאנו דרך לבדוק האם ההצפנה של כפולה של הסוד שאנחנו מנסים לגלות היא חוקית.

**על בחירת B:**

אנחנו יודעים מבחירת B שהוא נראה כך (בבתים) 010…0 כלומר הבית הראשון והכי משמעותי הינו 0 השני הוא 1 וכל השאר הם 0. כלומר כדי להיות ממש קטנים מB אנחנו חייבים ששני הבתים הכי משמעותיים שלנו יהיו שניהם 0 ולאחר מכן זה לא משנה מה יגיע נהיה קטנים מספיק. כלומר אם הסרבר עונה לנו האם מספר מסויים הוא הצפנה חוקית (מתחיל ב00) הוא בעצם אומר לנו האם המספר קטן ממש מB או לא. מצורת הבנייה של pkcs v2 ידוע לנו שהצופן שלנו m מתחיל ב00 ולכן נמצא בין 0 לB.

**שלב 1:**

עכשיו אם ידוע לנו שa\*m<B אז 2am<2\*B זה נכון מכיוון שהנחנו ש2\*B<n. לכן נרוץ על חזקות של 2 ונחפש את החזקה הראשונה כך שa\*m>=B ואז נקבל שa/2\*m>=B/2 וגם a/2\*m<=B.

**בשלב 2:** זה פשוט אי שוויונות די ברורים הנובעים מאותו הגיון של שלב 1. חושב לשים לב שאי השוויונות הללו הם תחת מודולו n ולכן הם נכונים. בסוף שלב 2 קיבלנו מספר m\*f2 כך שהוא נמצא בין n לn+B.

**בשלב 3:**

אז עכשיו נעבור להסתכל על הכפולות הללו כטווחים אפשריים לm. אם ידוע לנו שa\*m נמצא בין l and r אז m נמצא בין l/a and r/a (תחת עיגול מתאים).

לכן קיבלנו משלב 2 שm נמצא בין n/f2 לבין n+B/f2. עכשיו אנחנו ממשיכים ובוחרים כפולות של m ומעדכנים בעזרתם את החסמים על m, נשים לב שכל פעם שאנחנו בוחרים f3\*m חדש הוא תחילה בין in לin+2B. לאחר שאנחנו שולחים אותו לסרבר אנחנו מקבלים שf3\*m בין in+B לבין in+2B או בין in לin+B, אלו חצאים של הטווח המקורי כך שכל פעם אנחנו לפחות חוצים את הטווח האפשרי של m ולכן תוך מספר שאילותות סופי נקבל טווח בגודל 1 ונמצא את הצופן m.