שאלה 1:

חלק 1:

1) שיטת התקפה זו בקיצור "מרעלה את ה DNS" על ידי השתלטות על authority records, כך שהתוקף מקים שרת שהוא authoritative ל domain שהוא רוצה לתקוף ומציף את הקורבן עם פקיטות מזויפות שאומרות לעשות authority delegation לשרת שהתוקף הקים, וכך כאשר הקורבן מקבל את הפקטה הזו הוא יאמין שהשרת הזה שנמצא בשליטת התוקף הוא authoritative ל domain שהוא מנסה לגשת אליו ויאמין לתשובות שלו אך לצערו הרב התוקף יכול להפנות אותו לאן שהוא רוצה. ההבדל מההתקפה שתוארה בהרצאה נובע מזה שבהרצאה ראינו איך מזייפים record אחד של אתר ספציפי אבל כאן ניתן להשתלט על domain שלם בגלל שבמקרה שההתקפה מצליחה הקורבן מאמין לתשובות של שרת שהתוקף הקים והוא יכול לשלוח לקורבן כל תשובה שהוא רוצה ב domain הזה ולא רק לאתר ספציפי כמו שראינו בכיתה וזה הרבה יותר חזק!
2) היתרונות של התקפה זו שהיא מאפשרת התשלטות על domain שלם ולא רק על אתר ספציפי כך שאחרי הצלחת ההתקפה התוקף יכול לתקוף הקורבן בכל פעם שהוא ניגש לאתר ב domain וכמובן שזה מעלה את הסיכויים שהתוקף יצליח בהשגת מטרותיו (למשל אם הן גניבת מידע מהקורבן).
3) כדי להגן מפני התקפה זו, הוצע להפוך את ה source port לרנדומלי וגם את ה query id לרנדומלי כך שכאשר שניהם רנדומליים יש בערך 2^{27} אפשרויות שונות לקומבנציה של שניהם וזה מנמיך את הסיכויים שכאשר תוקף מנסה לשלוח query להשתלט על domain הוא יצליח כי זה כבר מספר עצום בהשוואה למה שהיה קודם 2^{16} שאפשר לתוקף להצליח בערך פעם ב 10 שניות.

חלק 2:

נמצא בקבצי ההגשה האחרים!

שאלה 2:

1) פעולת MIXCOLUMN שראינו בתרגול משנה את כל העמודה אך פעלות ROTATECLOCKWISE לא תמיד משנה את כל העמודה, למשל ניתן לראות זאת בעמודה הראשונה בדוגמה שניתנת עם השאלה כך שיחסית יש פחות שינויים ולכן זה כבר רומז לנו שהצופן החדש פחות בטוח. נניח גודל של 128 סיביות ונקבל שיש לנו 16 בלוקים כל אחד בגודל 8 סיביות כך שלכל בלוק מאלו יש 2^8 אפשרויות שונות. נציע לבצע את התקפת ה Chosen Plain text הבאה: כפי שתיארנו קודם יש 2^8 אפשרויות לערכים של כל בלוק, ולכן 2^8 זוגות של (P, C) מספיקות בשביל הפענוח.
כלומר נצטרך $O(2^8)$ זמן בכדי להצפין ולפענח את הטבלה באופן דומה לתרגיל שנראה בכיתה.
ונצטרך לכל אחד מ 16 הבלוקים טבלה בגודל 2^8 לפענוח, ואותה כמות של טבלאות ובאותן גדלים להצפנה.
כלומר נצטרך $O(2 \cdot 2^8 \cdot 16) = O(2^{13})$.
2) פעולת ROTATECLOCKWISE הינה פעולה לינארית כי מתקיים ש: $RC(x \oplus y) = RC(x) \oplus RC(y)$ כאשר RC מציין ROTATECLOCKWISE, ראינו בכיתה ש BYTESUBSTITUTION הינה פעולה לא לינאראת ולכן היא מקשה על התוקפים. כיוון שהחלפנו פעולה לא לינארית בפעולה לינארית, נקבל שהצופן החדש הוא פחות בטוח מהצופן המקורי עקב לינאריות הפעולה החדשה. הלינאריות כאן מורידה את הבטיחות של הצופן כי הפלט של פעולות לינאריות הינו יותר קל לצפות על ידי התוקף ולכן הוא יכול להשתמש בזה בכדי לנסות ולשבור את ההצפנה למשל בהתקפות Chosen Plain Text כיוון שניתן לתאר את הפעולות של האלגוריתם כפעולה לינארית ועכשיו יותר קל לשבור את זה על ידי מציאת פעולתה ההופכית.
3) הצופן שהמרצה מציע יהי חזק לפחות באותה מידה כמו הצופן המקורי כיוון שהפעולות של האלגוריתם שומרו כמו שהיו רק עשינו ROTATECLOCKWOISE למפתח כך שהשינוי העיקרי הוא באיזה מפתח מצפין כל בלוק אך ראינו בכיתה שזה לא באמת חשוב לנו ולכן לא פגענו באמינות של האלגוריתם המקורי ומתקבל שהצופן החדש הוא לפחות חזק באותה מידה!
4) הצפנה לא מאובטחת של zoom:

i. ראינו בתרגול שכאשר משתמשים בהצפנה של ECB מתקיים: $C_i = E_k(M_i)$ ו $C_i = C_k \Leftrightarrow M_i = M_k$ כך שתוצאת הצפנה של שני בלוקים היא זהה אם יש להם אותו ערך כיוון שאין תלות בבלוקים אחרים. ובמקרה שיש הרה בלוקים שחוזרים על עצמם אז התוקף יוכל לזהות אותם דרך התכונה שהזכרנו למעלה. ובאופן דומה לתמונה של TUX שראינו בכיתה, התוקף יהיה מסוגל לראות את התבנית, ומכאן נובעת החולשה שהחוקרים טוענים.

ii. בכדי להיפטר הבעיה שלהם, אני מציע לחברת zoom להשתמש בהצפנה של CBC אשר בה יש תלות בהצפנה של בלוק עם הצפנת זה שנמצא לפניו כך שמתקיים $C_i = E_k(M_i \oplus C_{i-1})$ ולכן עכשיו הסיכוי שהצפנה של בלוקים זהים היא זהה שואף לאפס ויקשה על התוקף לזהות את הבלוקים הללו באופן דומה למה שהוא יכל לעשות ב ECB.

5) איזו הודעה הוצפנה:

i. כאשר משתמשים ב ECB:

כפי שהזכרנו מקודם, בהצפנה של ECB מתקיים: $C_i = E_k(M_i)$ ו $C_i = C_k \Leftrightarrow M_i = M_k$ ולכן אם נכניס שני בלוקים זהים, נקבל שיש להן הצפנה זהה. ואם נכניס שני בלוקים שונים, נקבל שהצפנתן שונה! כלומר נסתכל על תוצאת ההצפנה ואם התקבלה הצפנה שמורכבת משני בלוקים זהים אז אנחנו יודעים ששני הבלוקים שהיו זהים הם אלו שהוצפנו, אחרת הבלוקים השונים הם אלו שהוצפנו.

ii. כאשר משתמשים ב Interleaved-CBC:

נגדיר שתי הודעות בתבניות הבאות:

$$M_1 = M\ M, M_2 = M\ M\ \oplus 27$$

נתאר את התוצאות של *Interleaved-CBC*:

a. על M_1: $C_1 = E_k(M \oplus IV_0), C_2 = E_k(M \oplus IV_1)$ כך שבעצם שניהם שונים זה מזה כיוון ש $IV_0 \neq IV_1$ כפי שנתון בשאלה כי $IV_1 = IV_0 \oplus 27$

b. על M_2: $C_1 = E_k(M \oplus IV_0), C_2 = E_k(M \oplus 27 \oplus IV_1) = E_k(M \oplus 27 \oplus IV_0 \oplus 27) = E_k(M \oplus IV_1)$

כלומר התקבל $C_1 = C_2$ עבור הודעות מסוג M_2 ו $C_1 \neq C_2$ עבור הודעות מסוג M_1.

כך, אם ההצפנות של הבלוקים אחרי ההצפנה הם זהים אז נידע שזו הודעה מסוג 2, אחרת זאת הודעה מסוג 1 כפי שתיארנו למעלה.

6) בהתחלה עומר מאזין להודעה שנשלחת על ידי רועי והוא יודע שהיא "כן" או "לא" והמערכת שולחת את הערך של IV_0 שהיא הולכת להשתמש בו בגלוי ולכן הוא יודע את ערכו גם כן ששומש להצפנת ההודעה הראשונה M_0 אשר שווה ל $C_0 = E_k(M_0 \oplus IV_0)$, לאחר השידור והגרלת ערך חדש, הוא יודע את הערך של IV_1 כיוון שהמערכת משדרת אותו בגלוי. עכשיו הוא יכול לנצל את העובדה שהמסר המועבר הוא מסר בינארי ו להכניס המסר הבא: כאשר y מסמן "כן", $M_{attack} = y \oplus IV_0 \oplus IV_1$ כך כאשר הוא מוכנס לצופן אז מתקבל $C_{attack} = E_k(y \oplus IV_0 \oplus IV_1 \oplus IV_1)$ ולכן $C_{attack} = E_k(y \oplus IV_0)$ ועכשיו שיש לנו את זה אז נשווה את זה עם C_0 ההצפנה של ההודעה הראשונה שנשלחה ואם הם שווים אז נדע שההודעה שנשלחה היא "כן". אירת, נדע שההודעה שנשלחה היא "לא". כאן זה אפשרי כיוון שההודעה מורכבת מבלוק אחד ויש למסר ערך בינארי, במציאות זה לא מתקיים ברוב המקרים ולכן אינו ישים כל כך.