שאלות

1.אנו מבצעים הצפנה חלקית עבור $\vec{w}=w_{1,}w_{2,.}....,w_l$ <u>ספציפי</u>.
כאשר כמות ה $\{c_{i,1},c_{i,2}\}$ תלויה באורך l (אורך מילת הוירוס).
מה קורה כאשר שולחים וירוס אחר $\vec{w}'\neq\vec{w},\vec{w}'\epsilon F$ - כאשר F הוא סט מצבי הקבלה (מילות הוירוס)?
למשל אם $length(\vec{w}')>length(\vec{w})$ אז אין לנו מספיק זוגות $\{c_{i,1},c_{i,2}\}$.
אבל גם אם הם באותו גודל ורק שונים, עדיין יש בעיה – כלומר לא נצליח לפענח את הצ'ק.

*בעצם השאלה: לפי הסכמה המוצעת, אם בוצעה הצפנה עם $\vec{w}$, והמכונה של השרת זיהתה התקפה עם המילה $\vec{w}',\vec{w}'\neq\vec{w}$,למה שהשרת יצליח לפדות את הצ'ק?

$$CT=(w,c_m,c_{start1},c_{start2},(c_{1,1,}c_{1,2}),....,(c_l,1,c_l,2),c_{end1},c_{end2})$$

<u>פתרון אפשרי ל(1):</u>
*הא"ב שלנו יהיה $\chi=\{0,1\}^8$ (כלומר בתים)
*נבחר אוסף של אותיות $x\subset\chi$, ונבנה מ- x מילת וירוס <u>אחת בלבד</u> $\{\vec{w}=w_{1,}w_{2,.}....,w_l|\quad w_i\epsilon x,\ i\epsilon\{1,..,l\}\}$
*נאפשר חזרות ב- w_i עבור אותיות מ- x .
*נגדיר סט נוסף של אותיות $y\subset\chi\setminus x$ (נניח מספרים לפי ASCII).
*כל האותיות ב- y יהיו אותיות שנתעלם מהן (שקול ל nope עבור וירוס "אמיתי").
כלומר בקבלת אחת מהן כקלט למכונת המצבים,נשאר באותו מצב.
*כל שאר האותיות,כלומר $\chi\setminus y$ (בין עם הן אותיות וירוס מ-x ובין אם "סתם" אותיות) יעבירו אותנו למצבים אחרים במכונת המצבים.

עכשיו, אין בעיה לחזור לעבוד עם הסכמה המקורית כל עוד השרת לא מכיר את $\vec{w}$, אלא רק הלקוח וה CA, והשרת נותן אמור מלא ב CA (הסכמה במלואה מופיעה בסעיף 3)

2. הצלחנו להצפין את $m\epsilon G_T$ (שמוגרל רנדומלית) ואז לפענחו בסכמה הנוכחית , אבל לא הצלחנו להבין איך בעזרת הקובץ :
"param" אפשר לבחור את P – המספר הראשוני בעזרתו נקבעים גדלי החבורות.

3. כיוון שאנו עובדים עם איברים מהחבורות אותם אי אפשר לשלוח כמו שהם על הקו, צריך לבנות מיפוי בין כל איבר בחבורה לבין string. אחד האיברים שנרצה לבנות עבורו מיפוי שכזה יהיה הצ'ק $Bond\epsilon G_T$ והשרת חייב להכיר אותו כדי שיוכל לפדות את הצ'ק . כלומר במימוש שסיכמנו עליו יהיה לשרת מיפוי מטקסט לצ'ק – כיוון שהצ'ק לא מוצפן כאן השרת יכול לפדות אותו.

4. בסכמה הנוכחית, כיוון שהשרת הוא זה שבונה את מכונת המצבים, הוא בהכרח מכיר את כל מילות הוירוס, בפרט הוא מכיר את מילת הוירוס $\vec{w}$ עליה בוצעה ההצפנה (בהנחה שיש פיתרון לבעיה שהעלנו בסעיף (1)).
בנוסף, השרת מכיר את כל האיברים שמיצגים את אותיות הא"ב שלנו, לכן יודע בדיוק מהן האותיות והסדר שלהן כדי לייצג את מילת הוירוס בעזרת איברים מהחבורה G_1 .
בהינתן מילת הצ'ק המוצפנת (מסומנת במאמר ב- c_m),אותה חייב הלקוח לשלוח,ובצרוף $\vec{w}$,יכול להפוך את ההצפנה החלקית להצפנה מלאה (מסומנת למעלה ב- CT).
ברגע שהלקוח ישלח לו את SK ,יוכל השרת לפענח את הצ'ק ולפדות אותו -וזה בלי שום קשר לדו-שיח שאמור להתקיים בינו לבין הלקוח, ובלי תלות בהאם נשלחה מילה חוקית או מילת וירוס.

לכן אנו מציעים את הסכמה הבאה במקום, בה ניתן ל CA- בגלל שהשרת והלקוח סומכים עליו יותר סמכויות.
ה CA יהיה מי שמייצר את המכונת מצבים ומכיר את הוירוסים (אסור לשרת לדעת עליהם כדי שלא יוכל להשלים בעצמו את ההצפנה על הצ'ק ולקבל את CT).

<u>Setup</u>
1. השרת והלקוח מבקשים מ CA את מכונת המצבים
2. ה CA עונה לשרת עם מכונת מצבים $S.M$ וללקוח עם $S.M+F_{set\ of\ all\ the\ forbidden\ virus\ words}$
3.הלקוח שולח ל CA את $<SK, w, enc_w(Bond)>$ -שוב,מניחים שהבעיה ב(1) נפתרה
4. ה CA מנסה לפענח את הצ'ק. אם מצליח עוברים לשלב הבא, אחרת מודיע על סיום התקשורת (לקוח רמאי)
5.הלקוח דובר אמת.ה CA מודיע ללקוח שהאימות הצליח, ושולח לשרת $<SK, enc_w(Bond)>$ **(בלי w!)**
6. הלקוח והשרת יכולים להתחיל לדבר בינהם

*שאר הסכמה ללא שינוי.

<u>בעיות בסכמה הנוכחית:</u>

כיוון שהשרת מקבל את מכונת מצבים, עם מספיק כוח עיבוד הוא יכול לרוץ עליה עם קלטים לפי בחירתו עד שיגיע למצב קבלה. ברגע שהגיע למצב קבלה יש ברשותו את מילת הוירוס והוא יכול לפדות את הצ'ק.
זה מצב לא תקין כי הלקוח לא שלח וירוס ועדיין מפסיד את הצ'ק.

<u>פתרונות אפשריים:</u>
1.נוסיף למכונת המצבים מנגנון חתימה מבוסס מפתח פרטי/ציבורי, וכל מעבר במכונה יותנה בקבלת הודעה חתומה – אימות החתימה בלבד יאפשר מעבר למצב הבא. השרת יתעלם מהודעות שהחתימה עליהן לא טובה וע"י זה ימנע מלהריץ אצלו את הוירוס. הבעיה במנגנון זה הוא שהלקוח עדיין יכול לשלוח הודעות וירוס (עם חתימה לא חוקית עליהן) ולצאת ללא נזק - כיוון שהשרת לא יצליח לאמת את החתימה ולכן לא יוכל להשתמש במכונת המצבים.
פיתרון זה אפשרי אבל לא מספיק טוב .

2.לבחור את אורך מילת הוירוס להיות מספיק גדול - לפרוץ אותה לוקח $O(256^{length(\vec{w})})$ שימושים במכונת המצבים.
פתרון זה נראה לנו הרבה יותר הגיוני כיוון שהרעיון המקורי של הצלחה בפענוח הצ'ק אמ"מ נשלחה מילת וירוס נשמר ללא כל שינויים- במידה ולא רוצים לזכור מילים ארוכות מידי אפשר היה לקחת את המילה ולהפעיל עליה פונק' hash כדי להגיע לאורך שיוגדר כבטוח.

*לצורכי פרזטציה עדיין נרצה לעבוד עם מילות וירוס באורכים קצרים כמו "virus" מטעמי נוחות