בס"ד

תרגיל מספר 2

(להגשה עד ל 24.6)

בתקשורת client-server קלאסית, אויב בעל יכולת האזנה יכול לדעת בקלות מי מדבר עם מי. הצפנת המידע הנשלח מגינה על סודיותו, אבל לא מגינה על המטה-מידע, למשל, לא מגינה על מי שולח מידע למי.
בתרגיל זה נרצה לממש פרוטוקול המאפשר לאליס לדבר עם בוב בצורה אנונימית, כלומר, בלי שאויב מאזין יוכל לדעת שהם מדברים ביניהם (לייתר דיוק, האויב לא יוכל לדעת זאת בקלות).

הרעיון הוא כזה. במקום שאליס תשלח את המידע ישירות לבוב, אליס תשלח את המידע לשרת מתווך. השרת המתווך ירכז את כל ההודעות שהוא קיבל בפרק זמן מסויים (למשל דקה אחת), ואז בתום פרק הזמן, יעביר אותן ליעדן **בסדר אקראי** (כלומר, לא בסדר שבו הן נכנסו). מכיוון שחוץ מאליס ובוב יהיו לקוחות נוספים, יהיה קשה להתאים הודעה שנכנסת לשרת המתווך להודעה שיוצאת מהשרת המתווך, ולכן, יהיה קשה לאויב שמאזין לתעבורה (הן לנכנסת והן ליוצאת) לדעת מי מדבר עם מי.

כל ההודעות שנכנסות לשרת יהיו בגודל זהה. כל ההודעות שיוצאות מהשרת יהיו בגודל זהה.
השרת מייצר בתחילת התוכנית מפתח פרטי/פומבי, והמפתח הפומבי יינתן כקלט לקליינטים.
אליס ובוב מסכימים מראש על מפתח סימטרי k, ומצפינים בעזרתו את המידע.

$c = Enc(k, data)$

בכדי שהשרת המתווך יוכל לדעת לאן להעביר את המידע, הקליינט לוקח את ההודעה, ומשרשר לה את כתובת ה IP והפורט של היעד:

$msg = IP_B \,||\, Port_B \,||\, c$

כדי שהאויב המאזין לא ידע את המידע הזה, המידע הזה מוצפן באמצעות המפתח הפומבי PK של השרת:

$l = Enc(PK, msg)$

אליס שולחת לשרת המתווך את l. השרת מפענח את ההודעה עם המפתח הפרטי שלו.
בתום הסיבוב הנוכחי, הוא מעביר את c אל $IP_B,Port_B$ (כפי שהוגדר לעיל, בסדר אקראי). בוב מחלץ את data מ c.

הבעיה היא שאליס ובוב לא סומכים על השרת המתווך, וחוששים שאולי התוקף השיג שליטה עליו. ולכן, הם מחליטים להשתמש ב X שרתים מתווכים.
למשל, נניח ש X=3.
אליס רוצה לשלוח הודעה לבוב, ולכן עושה את השלבים הבאים:

$c = Enc(k,data)$
$msg = IP_B \| Port_B \| c$
$l_1 = Enc(PK_1, msg)$
$l_2 = Enc(PK_2, IP_1 \| Port_1 \| l_1)$
$l_3 = Enc(PK_3, IP_2 \| Port_2 \| l_2)$

כאשר PK_1,PK_2,PK_3 הינם מפתחות פומביים של שלושה שרתים מתווכים, ואליס שולחת את l_3 לשרת המתווך שהמפתח הפומבי שלו הוא PK_3.
השרת הזה מטפל בחבילה בדיוק כמו שהוגדר לעיל.
ההבדל הוא, שהוא יראה את כתובת ה IP והפורט של שרת מתווך אחר (ולא של בוב), ולכן יעביר את l_2 לשרת שכתובת הIP שלו היא IP_2 והפורט הוא $Port_2$.
וכך הלאה, עד שהשרת המתווך השלישי יראה את הכתובת של בוב ויעביר אליו את המידע.

עליכם לממש קליינט שולח, קליינט מקבל ושרת כמוגדר לעיל.
מידע אודות קלט/פלט מופיע בנספח.

<u>הגשה:</u>

- עבודה בפייתון גרסא 3 בלבד. אין אישור להשתמש בשום ספרייה, למעט ספריות הקריפטו שנלמדו בכיתה, סוקט, os, תאריך, רנדום, וספריות שקשורות למולטי-ת'רדינג. אם יש צורך מהותי בספרייה כלשהי אחרת, יש לבקש אישור להשתמש בה.
- שאלות יש לשלוח במייל. במודל יתעדכן מדי פעם קובץ שאלות ותשובות. באחריותכם להתעדכן בו. כל הנכתב בו מחייב את כולם.
- הגשה לסאבמיט בלבד.

- ניתן להגיש לבד או בזוג (לבחירתכם). לא ניתן להגיש בשום הרכב אחר. במידה ומגישים בזוג, רק אחד מבני הזוג מגיש את התרגיל.
- השורה הראשונה בתרגיל חייבת להיות:

  # full name 1, id 1, fullname 2, id 2

  כלומר, עם שם או שמות המגישים ותעודות הזהות שלהם. חובה להקפיד על הפורמט הזה בלבד. תרגיל שיוגש בלי שורה זאת בפורמט הנ"ל ירדו לו 10 נקי' מהתרגיל.
- עבודה עצמית בלבד. **"השראה"/שימוש בכל קוד שהוא של אחרים (כולל מהאינטרנט) אסור.** דבר זה נבדק אוטו' על ידי המערכת.
- יש לכלול תיעוד בסיסי. (כלומר, כל כמה שורות)

בהצלחה

נספח:

להלן פירוט הרצת לקוח שולח, שרת מתווך ולקוח מקבל.
הלקוח השולח, שנקרא לו אליס, מקבלת כקלט ארגומנט אחד וזהו מספר, נקרא לו X.

אליס טוענית קובץ בשם messagesX.txt (כאשר X הוא הארגומנט שקיבלה כקלט).
קובץ זה מכיל שורות אשר כל שורה מתארת הודעה שעל אליס לשלוח.
השורות יהיו בפורמט הבא:

[message] [path] [round] [password] [salt] [dest_ip] [dest_port]

כאשר :

message - הינו ההודעה שיש לשלוח
path - הינו מסלול השרתים שעל ההודעה לעבור
round - באיזה סיבוב יש לשלוח את ההודעה
password - סיסמא ליצירת מפתח סימטרי
salt - ליצירת מפתח סימטרי
dest_ip - כתובת היעד הסופי
dest_port - הפורט של היעד הסופי

למשל, להלן דוגמא לשורה שכזאת:

cccc 3,2,1 0 password password 127.0.0.1 5000

כאשר:

cccc הוא ההודעה שיש לשלוח
על ההודעה לעבור דרך השרת המתווך המזוהה כשרת מספר 3, ואז דרך שרת מתווך המזוהה כשרת מספר 2 ואז דרך שרת מתווך המזוהה כשרת מספר 1.
ה 0 אומר שעל ההודעה להישלח מיד בסיבוב הראשון. עם היה 1 זה היה אומר שעליה להישלח בסיבוב השני (כלומר, אחרי דקה), אם היה 2 זה אומר שעליה להישלח אחרי 2 דקי' וכך הלאה.

ה dest_ip ו dest_port זה ה IP,port של היעד, זה שאליו שרת מתווך מספר 1 (בדוגמא הזו) צריך להעביר אליו ההודעה.

השרת המתווך, שנקרא לו שרת מיקס, מקבל כקלט ארגומנט אחד וזהו מספר, נקרא לו Y.

שרת המיקס טוען קובץ בשם skY.pem (כאשר Y הוא הארגומנט שקיבל כקלט).
זהו הקובץ שמכיל את המפתח הפרטי שאיתו הוא יפענח את ההודעות שנכנסות אליו.

הלקוח המקבל, מקבל שני ארגומנטים, password ו salt אשר הם בעצם זהים לערכים הללו שאליס קיבלה.

הלקוח השולח והשרת מיקס אינם מדפיסים כלום למסך.
הלקוח המקבל מדפיס את ההודעה שקיבל, ואז תו רווח, ואז את השעה הנוכחית.

יש לתמוך בכמות לא מוגבלת של לקוחות ושרתים, מסלולים שונים בגדלים שונים, מפתחות שונים, קלטים שונים וכו'.
עם זאת, שימו לב שהקבצים שנתתי לכם, בנויים באופן כזה שסדר השרתים חשוב.
אם תנסו לשנות את הסדר ההצפנה לא אמורה לעבוד.
אתם יכולים ליצור קבצים נוספים לבדיקה, יש רק להקפיד על העקרון הבא.
קובץ pk1 הוא מפתח בגודל 2048
קובץ pk2 הוא מפתח בגודל 4096
קובץ pk3 הוא מפתח בגודל 8192
אתם יכולים ליצור קבצים אחרים עם מפתחות אחרים ובגדלים מתאימים, אך יש להקפיד שכאשר מבצעים הצפנה, ההצפנה הראשונה תהיה עם המפתח הקטן יותר, ולעלות לפי סדר הגדלים.
בדוגמא בהמשך תראו שעשיתי קלט עם המסלול 3,2,1 מה שאומר ששרת מספר 1 הוא השרת האחרון בשרשרת, ולכן הלקוח מצפין איתו ראשון, ולכן העקרון הנ"ל של הגדלים נשמר.

<u>להלן פירוט דוגמת הרצה, כאשר יש שולח אחד, שרת מיקס אחד, מקבל אחד, ונשלחת הודעה אחת:</u>

תוכן הקובץ messages1.txt:

```
cccc 2 0 password password 127.0.0.1 5000
```

אליס מחשבת

c = Enc(k,"cccc")

בהצפנה סימטרית, כאשר k הינו מפתח סימטרי לפי ה password וה salt שקיבלה כקלט.

ולאחר מכן מחשבת:

msg = 127.0.0.1 || 5000 || c

l = Enc(PK_2, msg)

וכן, את PK_2 היא טענה מקובץ בשם pk2.pem שנתון בתיקייה.

ערך המשתנה msg שיצא לאליס הוא:

\x7f\x00\x00\x01\x13\x88gAAAAABgxRkr4WOTou7EHnaBK2mV_tz2aPth_vu0yp
330II2Cp6jX3qLKPc6QF6B82s5bDkp_TSbaaFIc48vGzJyqbMeo9cR1A==

כאשר:

\x7f\x00\x00\x01 ⇒ 127.0.0.1

\x13\x88 ⇒ 5000

שימו לב שכתובת ה IP תמיד מקודדת ל 4 בתים והפורט לשני בתים.

יש להקפיד על הקידודים.

שאר הבתים הם ההצפנה של ההודעה cccc.

המפתח שאמור לצאת משימוש ב password ו salt הנ"ל הוא:

B1t-pFf2N-2tHSNF_jDyJuN9tIvsgkQA0hlRmipPj_I=

ערך המשתנה l שיצא לאליס הוא:

\x8e\xd6\x1de(\xa7.}\xfdlh\xa1\xaeAg\xb0\xc3f\x80\xca\x04~\xd7\xf6\xba\xe8
\xe2\x92/\xa2`\xcd\xa6\x83G\x95\x1f\x86>\xa4\x08Lj]\xbf\x7f\x1b\xd4\t\xcf\x
c9\xb8\xbf\x80\xa2\x98\x10\x9bq\xcfHI\xb7\xee\x82\x0c\x1b\xe0\xeb\x92X\x
b9\xb8"67\xc7\xab>\xd0\xa0\x1aC\x19\xd5C\x91\xea\xf5\x97\x00\xc4\x99\xd2
\x87I\xbb\xa8t\xe9%\xe6B\xd34;\xcd\xcd\xca9I\xf44\x8f
w\x92\xb0\xd0}\xf0gh\x14\x90\xe6\xc4\xe8N8F\xf0\x80hC\xd7\x815\xc1\x0f\x
12\x7f\xd0\x9f\xfb\x7f\xab&-\x9a\x8e\x90\xb7!K\x8d\xa4\x80\x96\x04\xf4\xd
9~d\xd3\x93\xd7\x9d~\xd0:VDD6\x94W\xa7\x91\x16\x1c\xf1\x89i:\xce\xa1\xc
3\x88\x88\x9e\x04\xadLeG\xf0\x8bCbi-<Ro%t\x0b\xd7xy\x8f\x14\xf6)\xc0\xfe\
xacw\xb8\xf0\xb2\xdf\xe2\xf1X\x86\xd7\xfc\xa4\xa5\xe5\xf7\xba\x99\xa5e\x0
c()o\xe7\xc9\xa3\xda\xea\xbb\xb7L\xb7\x8b\x05G\xf35\xda\xcfGP\xe6\x9b\xd2
\xa6\xef\'\x98\x98Y4\xafY\x81\xee\x8c\xbbO\x9d\xd0\x95u\xc4\x84\xbf6\x95\
x8f\xd0\x9dyNMS;9\xf5\x1f \xef\xa1\xb9\xac\x9f\xac\xf3\xc6\x9c
\xe2W\x83d.f\x8b\xb7\xfc\xc6u\xa7s\x90m\xa4Tz\x08\x0fWX\x82\xf7R1\x92\x

be\x99k4{\xb1\x8a\x04\x1f\'\xe5\x98CCr\xac]\x12:\xdb\xf9\x9aVX\x17i\xcb\xf
0\xa7\xdc\xa6\x14\x85._\'a\x8e\xd8\x07lSvd\xca\x1c\x1e\xc8x\xba\xb9Q\xb9\
xe7\xde<\x18\xd9\x07\xf1\x0bJ\xc4c\xea(\x98\x1b\xec@H\xc2\xbc\xe1\x9d\x8
9t7\xc4E9n\x1b\xe4\x19_\x87\x11!O\x9a\xda\x0f\xabp\xecM\xd6\xc8e0\xd4xB
\x00s\xab\xc1\xd7\x1eu\x8a\xc6c\xdbg\xd6\xb3`\xea\x94\xd4\xa5T\xcc\xc9\xf
7\xb7i\xd36\xc7\x010\xd37\r\xb6\xb6\xd4\xc1\x13\x03\xac5\xce\x87\xfc\xee\
xe9`\x17h2\xa6\xf6/\x08\x00\xb0\x9f\xf7\xff\x05,)v_\x85d\x0bv\xb6\xb7\xc1\
x0c\x1e\x9f

כעת אליס מעבירה את ההודעה לשרת המיקס.
השרת מפענח את ההצפנה ומקבל בעצם את אותו הערך של המשתנה msg.
הוא ממתין שיגמר הסיבוב, ואז שולח את msg לכתובת הIP והפורט שהופיעו ב msg
את ההודעה c.
הלקוח המקבל, מפענח את c, בעזרת הצפנה סימטרית, כאשר k הינו מפתח סימטרי
לפי ה password וה salt שקיבל כקלט ומדפיס למסך:

cccc 16:50:12

<u>להלן פירוט דוגמת הרצה, כאשר יש שולח אחד, 3 שרתי מיקס, מקבל אחד, ונשלחת הודעה אחת:</u>

תוכן הקובץ messages1.txt:

ddd 3,2,1 0 password password 127.0.0.1 5000

אליס מחשבת

c = Enc(k,"ddd")

בהצפנה סימטרית, כאשר k הינו מפתח סימטרי לפי ה password וה salt שקיבלה
כקלט.
ולאחר מכן מחשבת:

msg = 127.0.0.1 || 5000 || c

$l_1 = Enc(PK_1, msg)$

$l_2 = Enc(PK_2, IP_1 || Port_1 || l_1)$

$l_3 = Enc(PK_3, IP_2 || Port_2 || l_2)$

את PK_1 היא טענה מקובץ בשם pk1.pem שנתון בתיקייה. (בהתאם, PK_2 מקובץ pk2.pem וכך הלאה).

את כתובות ה IP היא שלפה מקובץ בשם ips.txt. בהרצה זו, תוכנו היה:

```
127.0.0.1 9000
127.0.0.1 9001
127.0.0.1 9002
```

ולכן, כתובת ה IP המסומנת כ IP_1 היא כתובת ה IP בשורה הראשונה והפורט $Port_1$ הוא מספר הפורט בשורה הראשונה וכך הלאה.

ערך המשתנה msg שיצא לאליס הוא:


```
\x7f\x00\x00\x01\x13\x88gAAAAABgxRtQtyFYTUML1JG_SgXykXdfzRxfT-xQupX
w5GrPHJ5Ga3HyHJEeP3rHsPPFC7z0cVp30jQn6BH7A7PEzaQ_zIak1A==
```


ערך המשתנה l_1 שיצא לאליס הוא:


```
R\xff#\xe7\xec<S.\x8d\x87\x11\xca\x89\r\xa0\x0f\xab\xd6\xc8\xd8\x9a$R\xeb\
x15\xb7h\x9a\x00\xfc\x8b8m\x9f\xdc\xed\x08DO\xe0\xca\xe3J\xa0\xa6}\x9c\x
c4L\xc0\xb6\xa2\xf6e\xa8\'\xd4.*?wX\xb4\xa2\xe9HF9X\xdbz\xeb\xd41\xa2c+\
xd5\x95\xad\x98)\xbb\xfe\xc9\xfam\xca\xf4z\xee\x10/m\xb6\xb3V\n\x8as\x1c
\xd7\xc2y\xc8\xb4.\xf3\xb0\xe6{\xd2\xf40\x15\x87R%{\xa8|vc\x02\x0f\xdcf-\x
ae\xa5\xfb\xb5\x17\xbc\x96\x0f\xf6\xc0[\x15\xd4RPP\xd3\xdanK\xbd\xac#\xd
7\x91\xa7\xb9d\x06/\xfdD/z<\xee\xcb\x9c!\x13O.\x81\x06\xa2\x8a\xdfv\xf2\x
cc\xeb\x1b_\x924\xa4\x0cw6\xfdm\x02\x98/R\x0c\x06fz\xa1\xb49Qe\x87hN\xe
7\xba\x9dP\xb1\xa8\xfd\x0bd\xe2"\xa6G\x18\r\xa3l\xaf\xc1PEz\x044\xac[G\xe
bW\xd0\xd0\xc8\xf7\xbf\x0fcZ\xf5\x88\x0f\x96\x9a\xe3\xb0\x0b\xf95\\\'4\xf9
```


ערך המשתנה l_2 שיצא לאליס הוא:


```
\x03[5I\x1f\xde\x8eE\x03n\x9f\x1dG\xbaO_\x8dR(\xc8\xdc\xb6\x0b\xb2@c\xd
ck\x87>\xf9q@\x11\xaa\xb1(\xbeb\xa9\xb1\xf5;\x86\xf9\xe8C\xdc\x88\xbc\x9
3*\xfdgX\xd6V\x10[\xf8M\xe5T\x07[\xa3)K3\\0<\x96\n\x90\x92\x99\xcb\xd9o\
xba\xa7\xdcmr\xd5\x9b\x02\xe1A\xf9\xc4\xc5iE\xd4\xdd\x18\xcb\xdb\xd6S\x9
d\x1e2\x0e\x06\xee\xad1\x93\xcf\x07\xf7k\xc6\xa8\xcc\xd1\xf6F\x90\x02\xfb\
x87\x14\x9f\x07\x93\x90;_P\xac\xaa\xf0\xa9\xa1\xd3W\xac!\x91\r\xcb\xe3\xa
ed\xbfF\xc4\xf4\xf7+E\xfc\xd0\x93P\x9c@\xe9c#y\xee\x95\t!\xcb7\xbe\x10t\x
c2ES\xcaerh\xdd\xec\xd1\x1d\xce\xc3\\(\x1d-\xa6FC]\xea\xcf\xf5(m\xd8\xca\x
dfs\x04s}A\x88>\x86\xb7
```

9\x13\x86U\xa4_(\x12\x0c/q\xd5\xc2\xc0\x0e_\xc4\xddi\x87gJ/\x13\xe8\x03\x
fa\xa7\x06\xb4\x83\xc7}6\xc3m\x10\x85l\xd9`4\x97\xe4kg\xc6)\xe2P\x8a]\x01
D\xb5\xa6\xabW\xd9\x99G\x88\xa17\x02\xa7\x9b4T\xa6\xc0\x89\xba\x83K
\xc9\x1f6\x15\xa3\xafH\xa7\x0fY\xbb\xf7\x05\xc9d\x01k\x83)\x7f\x1f\x96\xfe
\xc5\x11\xe6C3\x7f}z\xa2\xbb\xe9k+\xc7L\xf1I\xc37\xea\xf7}+\x7f;\xdd\xee\x9
0\xa7|x\x9ae\x0f\x03˙\xa2q\xe1g\xe9o\xdc\xa3\xebbQUm\xe3\x0e!\xa1\x17\t
Mu\xf3\xabr\x13\xa9\xb8\xd6B]\xb5\x10\xaf>\x86\xeb@f\xd5\x08\xa1\xa8v\x
abAi3v);\xfa\xfc\x84 r\xe2c\x1fyin\xff:\x9f\x01\x0c\xd4\x08\xc3
\xbf\x84s\xdd/e\xdfg\xd26\x7ff\xd5\x19\xe3Zt\x9d\xde\xb7\x83\xa4\x8e|\xe2\
xd2\x98\xa6\xa3/\x07"D\xa9\xa7$\x1b%\x86l\x04\r\xb2\xf5+\xff?\xcer\x1c-\x1
f~\xc8\xaem\x8cG\xd7i]]o\xc4\xaa\xe0|\xcc\xe88\x1aM^/\xb2gO<\xd61\t\xa2\x
fe\xe6\x03\x95G_{\xd5(h\xf8y

ערך המשתנה l_3 שיצא לאליס הוא:

B\xa3\x8d\xb0$\'V\xb2\r\x8c\x9eL@\xbe\xee&S\r\x9b\x87]\x12\x14\xd9U\x0b
\xe5\x91\xb0Z\xe1\xe7\xd0G\x9d\xbc\xba\xfc\x82\xb3b\xddU\xcb"\x9b\x80y\
x8a\xde\xaejx\x97|@\xbc!\r\xd3\xe0S\xebc\xfb\x88\xa0\xb9\xe3\x03wD\x1e/Z
\x15\xa9N\xfaH]\x1e\'\xa3\'\xae\xac\xaaI\xae\x83P\x9eql\x07m\xe82j\xc6\x98
P\xcd\x8fS\xf0\xb2$A^\x1f\xae\xde/D\xdd\x00\x0fo\x05\xfan^\x85\xd8\x84at\
x84\x82\xeaG\xe3\xc4W\xca~\xfcg\xee\xcd\xa0[\x05\xe8G\xa4_&\x91a^\x9fe\x
c0\x18=W\xa8\x84Iyo\xde\xaa>\t\xf7\xe3\xcc\x07˙}Z^\xba\x1aw\xc5\xce\xef\x
ff\xf3Y\xea9\x10\x88L\xc8\x19y{4\x88\xfc\x92\xd9\x02m\xc3\x85\x94g\xec\xb
3\xae\xb5\x9f\x1fZ\xc6,T\xf3\xa9\xaf\xbcB]\x8d\xae8\x1ehN3\x83\x147\xbe\x
18\x85\xca\xc7<`,\x1f\xd4w\xa4\xf2k;)EhiX\xa1T\x83P\xb0\xc6:b\x8a\xb7i\xb
5Rm8\x9e\xf7\x86\x02m\xf7\xc0`\xf7o\xb1,q\xa8\x11\xe7,\xa1\x83\xe1y\x1d.
%\xea]b\xf5\x8e\x1f\xaa\x12\x90v\x88\xfb~\x15\xf0p\xa7\xaf\x88\xd4\xc3\xf9
m\xeaeC\xf6L\xb43Hp\x9fGq\xac\xa0\x08}_\x93\x08S\x16|<\x898\xdd\xb2\x1f\
xee\x9e\x8c\x14\xeb)%\x86\xd4R\x88\x04\x82\x15XE>z\xf5qnW\xdf\x8c;]\x0cf
\x16bSY\xe0N\xcc\xe1C\x9b\xf19k\xc2-q\xb12R\xfd\xc6\x9e\xd0\xe1AN\xde\n
\xb2%g\xe0arh~By\xbb\x04\x85=c\x89H\xf2\x11\xe74\x11@\xab\x86\x0b\x98\
xfeJT\x91\xb3j\xe4\'+0O,U[&\xdf<Tm\xf1yk\xb73\xd4\xb9\x90j:\x0f\xff}\xa2d)
]K\xff\x1a\x7f\xa4\x9e\x8a\xfa\x1f\xb7\x17:)}\xf6N\x15[1\xb022\x01b\x8c\x10
\xc3\x98]A\xd9\xd2\r`l\xc2\x14\x853\xbe`S",\x05=\xe8,\xbd9\xf8\xe7\xf7!\'˙\

xafP\xa9t2\x9a@\xbf7\x14\xbe\xa1O\x87\xd2\xfb\x93\tXa\x8bGP\xfb\x96\x80\
x99\xb6K\xbb\xf5\xa3\xb7\x07\x99\xcc\xe7[\x1a\x9dM<\x88U\x93\xe0\x93\x9
1X\xb8\xb4\x03I\xae\xe2\xfe@\x98RG&]f\x0fAo\xf5\x15\xdf\x08}\xdc%\x08\xd
d\xf4h\x0c\x93\x1d\xb3y\xab\x98y\xd9\x18\xa8\xc7\\\xd2\xfd\xbe\xbe\xf3g\x
e3\xf7E\x98\x81vc1nS\\i\xa0L\xaeR\xbd)\xbb\x17
\xc8\x8e{\xadK\x07\x90\xf8\xe57\t\xecn\'\xbeD\xb2P\x17\xafZ\xf3\xe45:\x11\
xc2\xe6N\x9eNA\x14\x90-\xd6\xfbZ\xe3_\xeeLf\xe7\x02\xfa\xe4\'\xcepA\x1afb
\xc37\xae\x82\x05@<\x8dQ\xf76\x8b\xab1\x9d#X>\xc2?\xf8g\xda\xaf\xaa\xb6\
xee\x10\x8eG\x84H\x13\x15\xf4\xe2\xceSo\x0c\xb6`\x93\x15V\xcd\xac˙l\xb6t
P\xa1\xdfz3A\xe8\xa71S/\x96\x7fUWZeU\x82W\xd7\x15\x18\x0f\xed\x1b\xdcj\
xc3\xabWB\x8e\xbc\xea\xb8\xc6\xdbtWD#\x0e\x9b-G\xd1\x18\xb8\'\x0c\xda\x
fa\x9e\xdfi)@\xc7\xad@J\xf0\xb5\xd0\x8d_\x87\xdeZ\x01\x0c\x13o#@\xfa\\?z
\'\xef\x82\xd5O\x00\x10\xbc5\xa9\xf7n&j+#8\xcdOF\xd1\x88~\x0f\x0b\xc7\x1
d\xd4\xa3\x17Gn\x90\x1cP\x08\xab\xd2\x96"|\x963\x89\xd9\xcb\xd9\t>K\xc0\
xeeY\x19l\xe3g\xa7K\x8e\xe5\xc5E\x0e\\\xa1\xfb\x01\x11\xb8\xfd\x02\xe32\x
94VB\xf9\x84w\x99\xefP\xb3tR\x91\xba}XJ\xd1\x84\x90,"?-\xdfB\x18\xeaY\xe
8\'\x0e\x9a\x94<\x1a\xe53\x10\xaa~9GI2?\xea\xe9u\x16\xc3\xae\xd5\xe8&7\xc
4EH\x92\xaa\xd7\x04q\xd3\x16\xa1\xf4\x02y\xadS\x0b\xa2\xbfK\xf2\x146\xcb
fy\x80\xc5NJ\xadO\x8a\xddt\x96\x04\xab\xd5Q\xf0\x13ug<\xc4O0\xc18T]\xc4\
xc2\x13\\\xdb\xf5iQ\x8d\xb5JD\x18+\xe4\x9b\xe8\xac\xbe\xf5\xe4\xc3\xc4

כעת אליס מעבירה את ההודעה l_3 לשרת המיקס שכתובתו $IP_3,Port_3$.
השרת מפענח את ההצפנה.
הוא ממתין שיגמר הסיבוב, ואז שולח לכתובת הIP והפורט שהופיעו בהודעה את התוכן. שימו לב, לא שולחים את הIP והפורט, אלא רק את התוכן המוצפן של ההודעה.
השרת המיקס השני עושה כנ"ל וכן השרת השלישי.
השרת השלישי שולח ללקוח המקבל, שמפענח ומדפיס:

ddd 16:51:45