

הצפנה - אליס, בוב ושות'

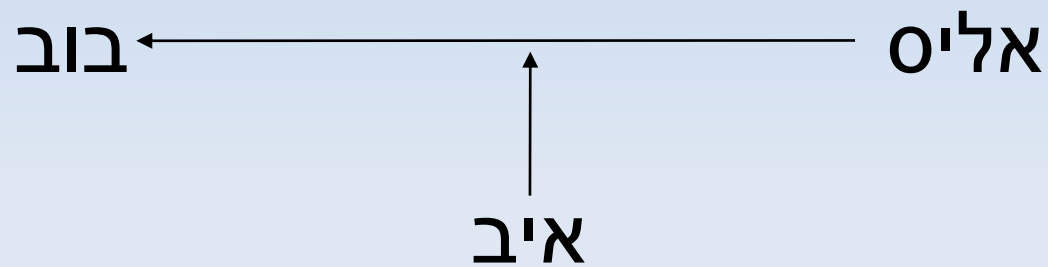
עמיחי פרץ קלופשטוק

Am1chay.p.k@gmail.com



מה ולמה - הצפנה

למה להצפין?



היסטוריה של ההצפנה

המצרים הקדמונים

ספר ירמיהו

יוליוס קיסר

גלילאו גליליי

מרי מלכת הסקוטים

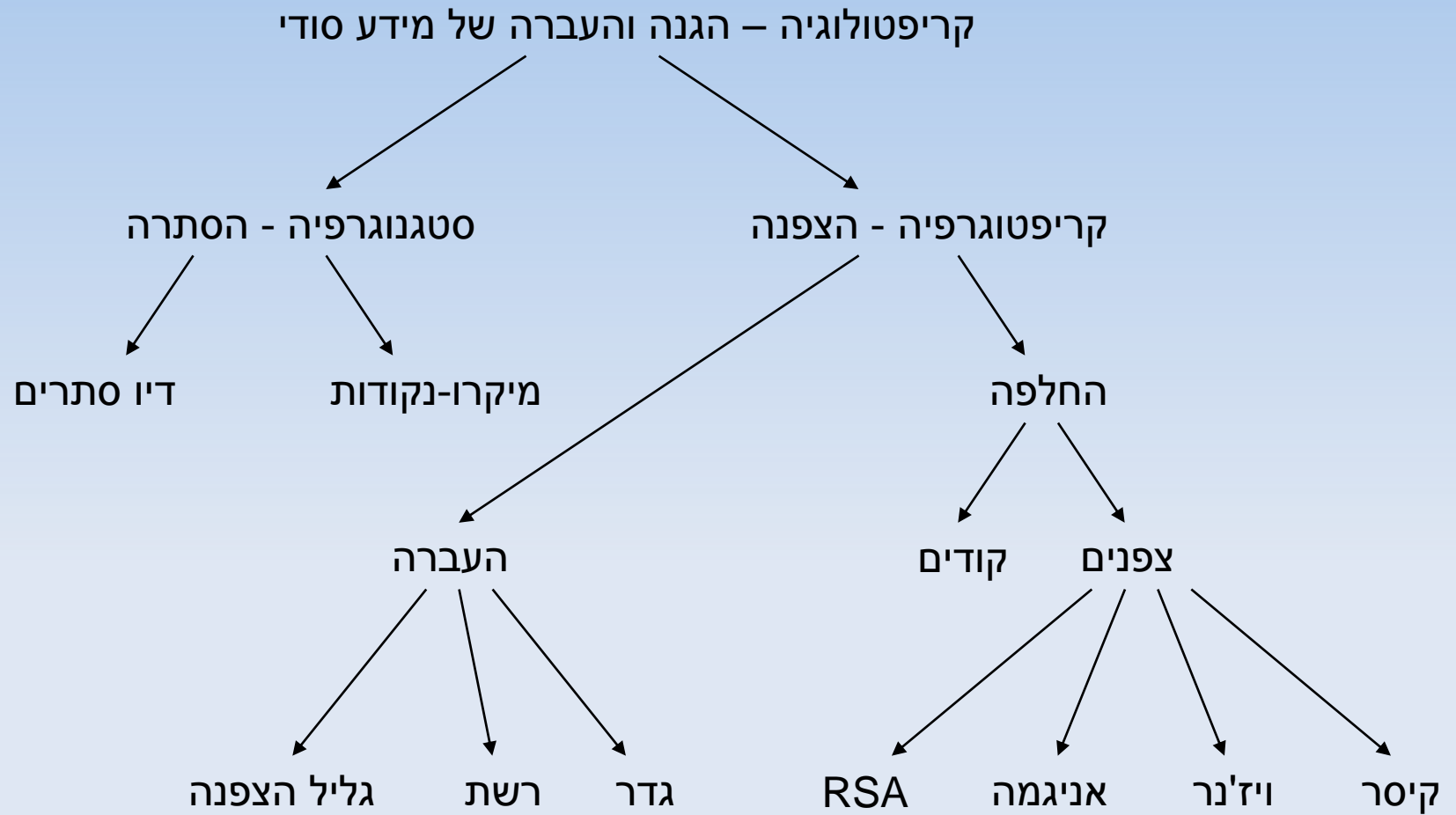
מלחמות העולם



WAR!



קריפטולוגיה



סוגי צפנים

סטגנוגרפיה
הסתרה של מסר

מיקרו נקודות

דיו סתרים

הסתרה כקעקוע שעליו צמח שיער

הסתרה על לוח עץ מצופה שעווה

הסתרה מתחת לקליפת ביצה

גליל הצפנה

קריפטוגרפיה
הצפנה של טקסט

צופן אתב"ש

צופן קיסר

צופן החלפה

צופן ויז'נר

אניגמה

RSA

הצפנה קוואנטית

יתרונות וחסרונות

סטגנוגרפיה

הסתרה של מסר

יתרונות:

יעילות ללא תלות במפתח

לא גורם חשד

חסרונות:

מספר הודעות מוגבל

ניתן לפענח בקלות יחסית

קריפטוגרפיה

הצפנה של טקסט

יתרונות:

יעילות תלויה במפתח

צפנים שאינם ניתנים לפענוח

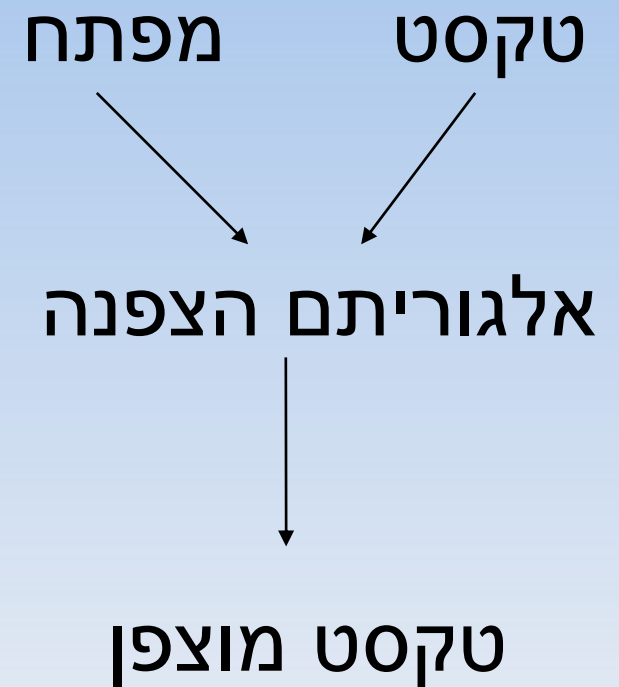
מגוון שיטות הצפנה

חסרונות:

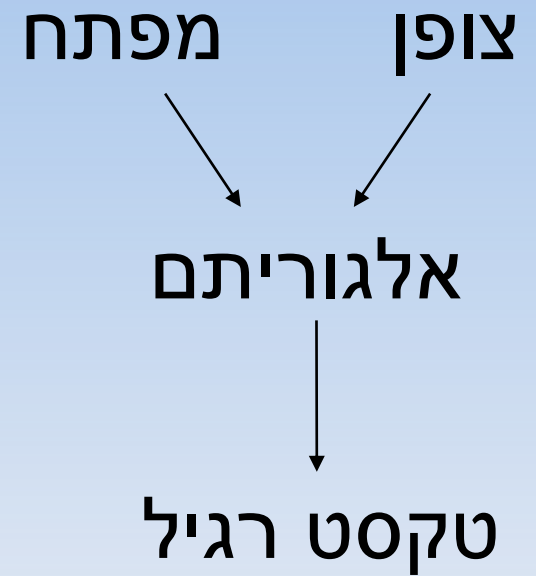
הפצת המפתחות

במסר ניכר שהוא מוצפן

שליבים בהצפנה



שליבים בפענוח



צופן אתב"ש

ספר ירמיהו:

"וּמַלְךְ שֹׁשֶׁךְ יִשְׁתָּה אַחֲרֵיהֶם"
"הֲנִנִּי מַעִיר עַל בָּבֶל וְאֵל יֹשְׁבֵי לֵב קָמִי רוּחַ מְשַׁחִית"
"אֵיךְ נִלְכְּדָה שֹׁשֶׁךְ וַתִּתְפַּשׂ תְּהַלֵּת כָּל הָאָרֶץ אֵיךְ הִיְתָה לְשִׁמָּה בְּכָל בְּגוּיִם"

ששך = בבל
לב קמי = כשדים

תרגיל:

רטט רמקק קרט שרט, קרט רקפכ רקכ שרט

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת
א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

צופן קיסר

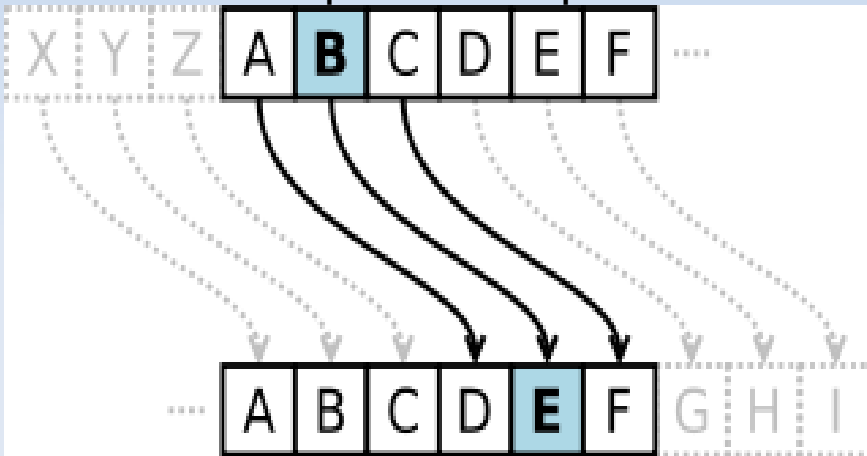
דוגמאות:

yhql, ylgl, ylfl. = Veni, vidi, vici.

בעברית:

צבא של עכברים עליהם מפקד אריה יכול לעשות יותר מצבא של אריות עליו מפקד עכבר.
שהד בס קנהאמע קסמחע ערתז דאמח מנטס סקבטג מטגא עשהד בס דאמטג קסמט ערתז קנהא.

תרגיל:



באח באח במא בעכ, בעכ במא באח באח

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת א ב ג

פענוח צופן קיסר

p hzzbyl fvb p ohk yhaoly il aol mpyza thu pu h cpsshnl yhaoly aohu zljvuk pu yvtl



a b c d e f g h i j k l m n o p q r s t u v w x y z

צופן החלפה

דוגמאות:

”אע 10 חפקאו עד שזעאו תכפדו, שדי עותאזאו תאזשסאצ, פשדי עדש”.

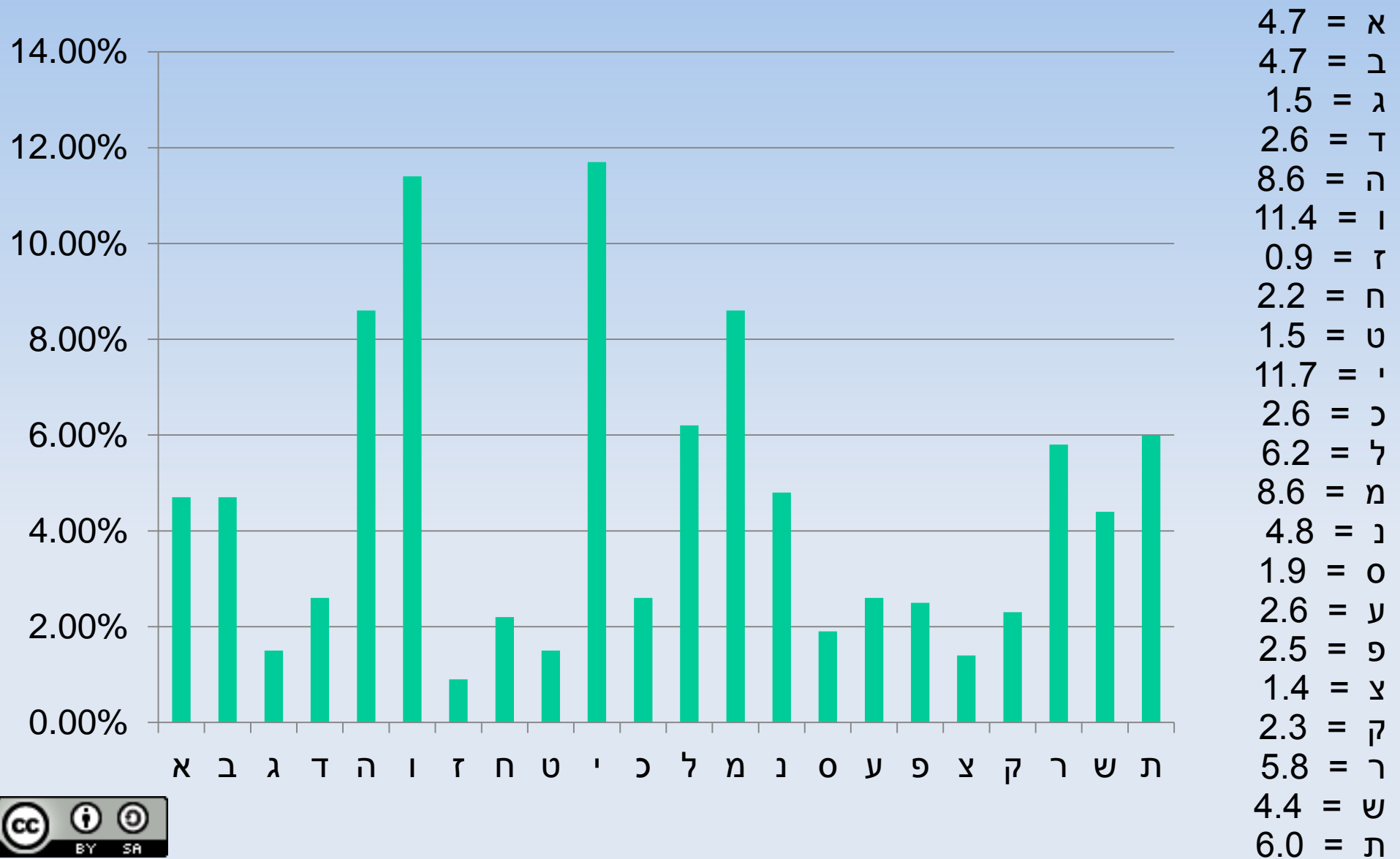
”יש 10 סוגים של אנשים בעולם, אלה שמבינים בינארית, ואלה שלא”.

תרגיל:

זגע זעב זגע

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת
ש ת ק ר י פ ט ג ה א ב ד ו ז ח כ ל מ נ ס ע צ

ניתוח תדירויות



פענוח צופן החלפה

,=(- <![=
,=(- <![=
,=(<%){(,%[#/\$
?=-)<#\$\$

,=(- <![=
,=(\$ /%+(#=#!
,!\$^\$ ((~ =|
.==| \$= (/&)|

!\$^\$ ((~!|
,=(- <![=
,=(>+[=()-\$/=
.=<% -%#@ =

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

פענוח של צופן ויז'נר

dlc mer krb **dlc** nse gild xm **dlc** wssci, dyv lexpsxgyryv tsbtmciq.



שיפור צופן ויז'נר

הודעה מוצפנת:

fjhhq cv ytmr-simhuded, mw xlsd pvddabe igv wzdefxk.



http://img2.tapuz.co.il/forums/1_94784909.htm תוכנה אוטומטית לשימוש בצופן ויז'נר:

סודיות מושלמת (צופן וורנר)

צופן:

שטבִּקֶּת לזדחחזך ומגתרתנִסְכִּיב ןאח חאהפב
שםסאע ןנ ןופ מקיסףִּר תרפמרער נרשוז
דמיטטז פעגשאנ םסעׁוב דהִּרִּץ שפמקט פב םי
טש צקִּפִּשא שדהִּעס ןִּפִּגבשה, ןהך רדרסה
הִּרִּיז.



XD

א ב ר ם

מפתח:

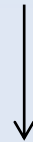
י פ כ ז



י צ ח ק

מפתח:

א ש ל ו



י ע ק ב

מברק צימרמן

תאריכים:

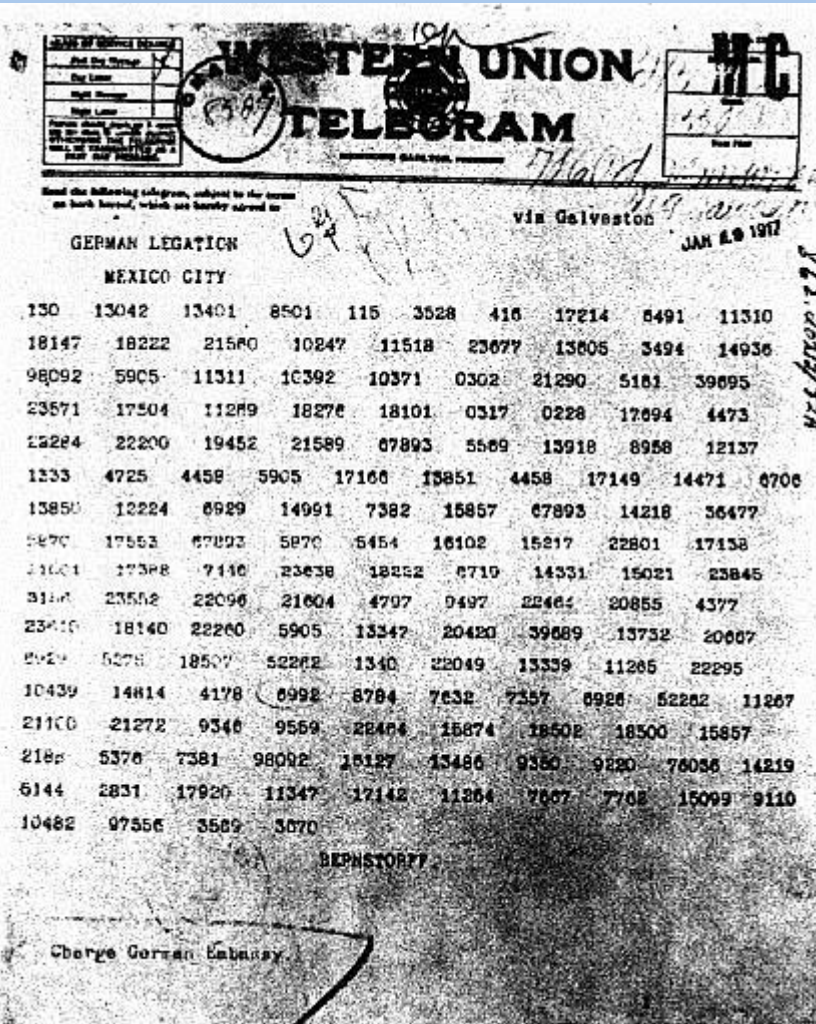
- נשלח: 16/1/1917
- יורט: 17/1/1917
- פוענח: 17/1/1917

חשיבות:

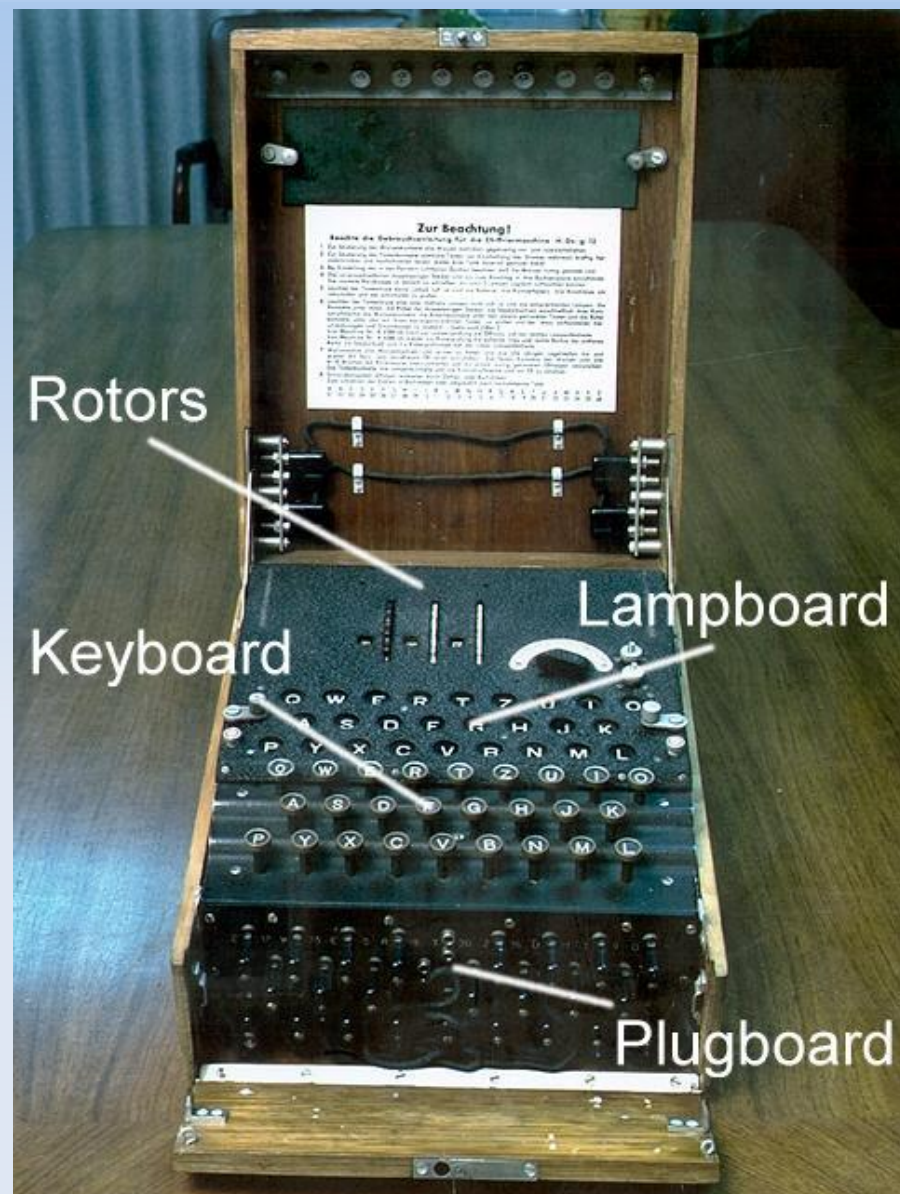
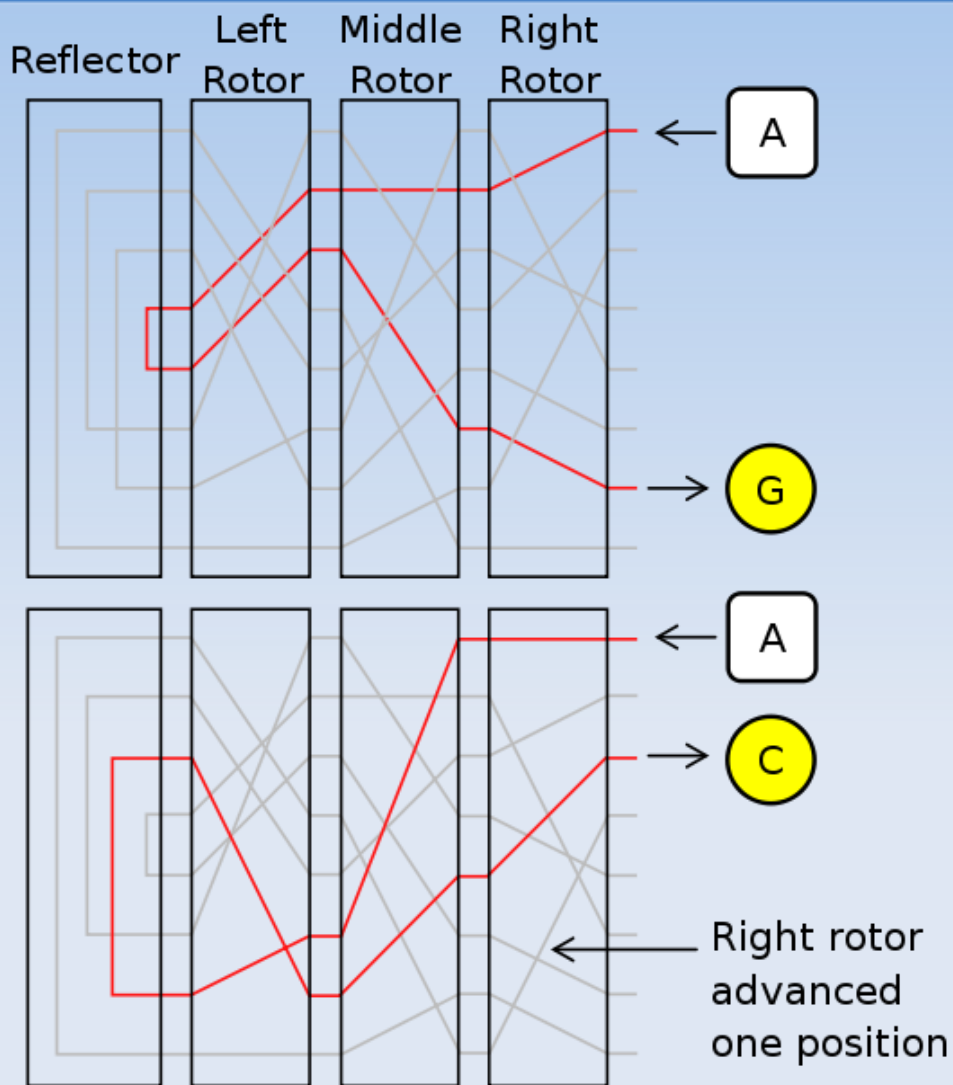
- גילוי יכולות הפענוח של בריטניה או -
- עיכוב חבירת ארה"ב לבריטניה נגד הגרמנים

בסופו של דבר:

- מסירה לארה"ב תוך הצהרה שהתקבל מבוגד מקסיקני
- הכרזת מלחמה אמריקנית על הגרמנים ב-6/4/1917



אניגמה



אניגמה

מספר המפתחות האפשריים:

• מצבי המערבלים: 17,576

X

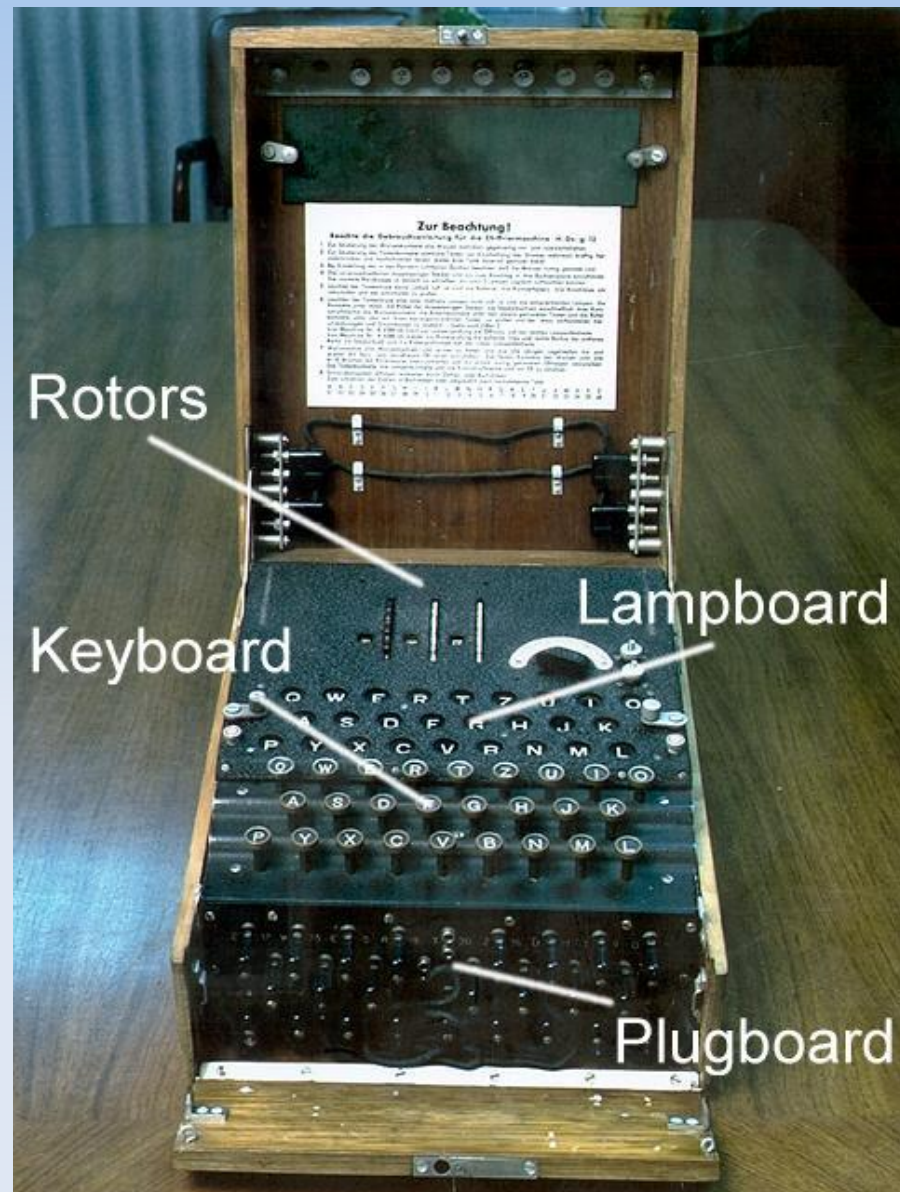
• סידור המערבלים: 6

X

• לוח המרכזייה: 100,391,791,500

=

• סה"כ מעל - 10,000,000,000,000,000 אפשרויות



פיצוח האניגמה

:1932

• מפתח אישי יוצפן פעמיים ברצף - abcabc

• ABCDEF GHI JK LMNOPQRSTU VWXYZ
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
• FQHPLWOG BMVRXU YCZ I TNJE A SDK

• מתוך הרבה הודעות התקבלה השרשרת: $J \rightarrow M \rightarrow X \rightarrow S \rightarrow T \rightarrow N \rightarrow U \rightarrow J$
• מספר אפשרויות/שרשראות מוגבל - 105,456

:1938

• מיכון הפענוח – מכונת "בומֶּבֶה"

:1939

• הוספה של שני מערבלים נוספים – הגדלת מספר האפשרויות מ-6 ל-60

• הגבלה ביכולות ניתוח הצפנים – לא איכותית אל כמותית

פיצוח האניגמה

תחילת מלה"ע השנייה:

- שיפור מכונות ה"בומבה" ע"י בעלות הברית – מכונות "בומב"
- ניתוח עריסות (הייל היטלר, אנא הגב, דו"חות קבועים וכד')

דצמבר 1941:

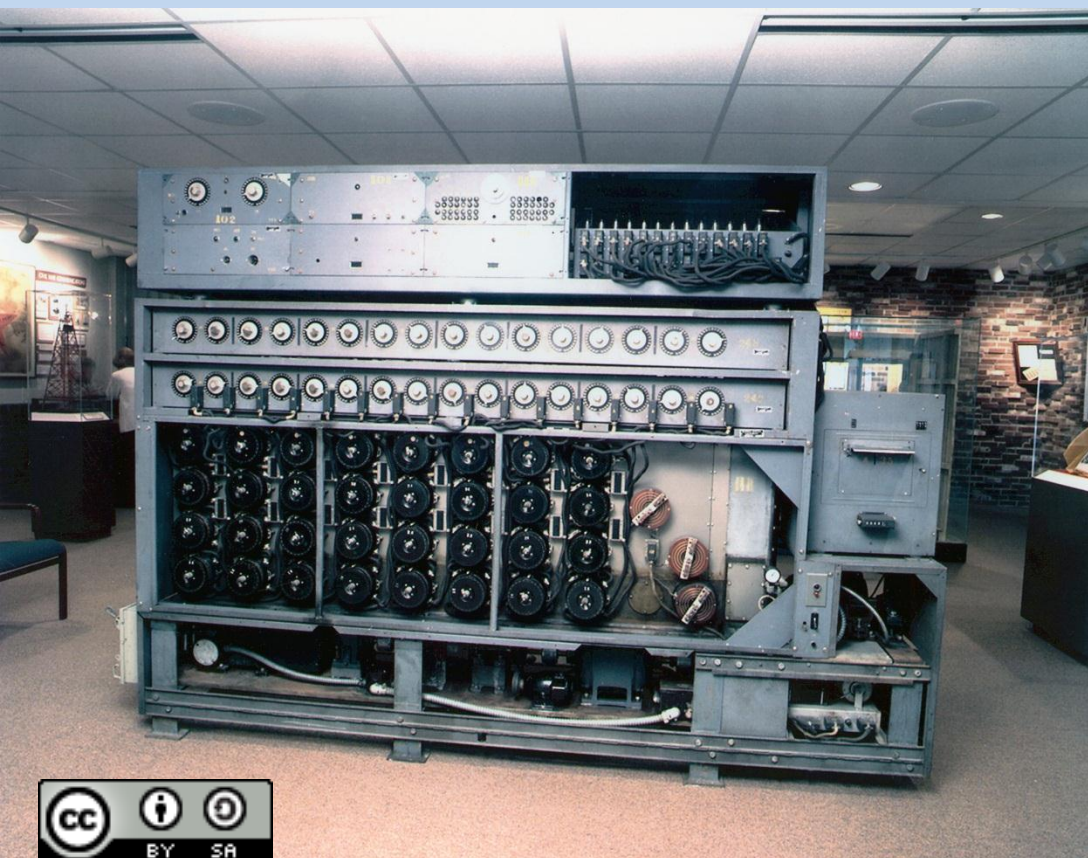
- הוספת מערבלי רביעי
- הגבלה ביכולת ניתוח הצפנים

מאי 1943:

- ייצור מכונות בומב משופרות ע"י ארה"ב

ספטמבר 1944:

- הפסקת ייצור עקב ההתקדמות במלחמה



כמה דברים נוספים

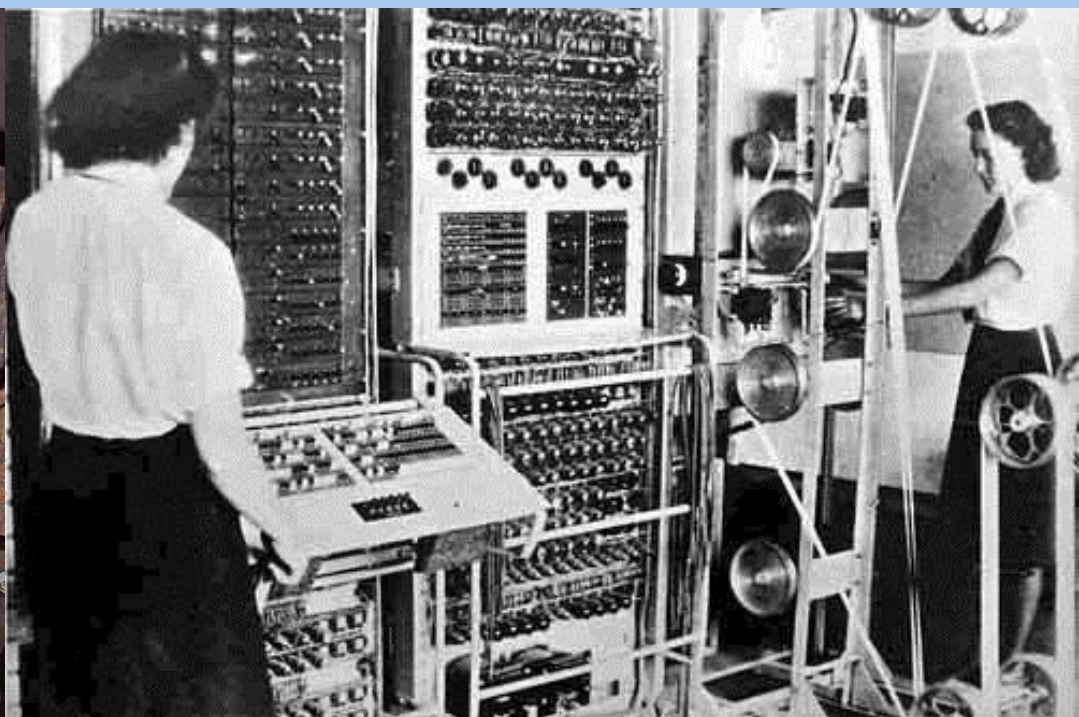
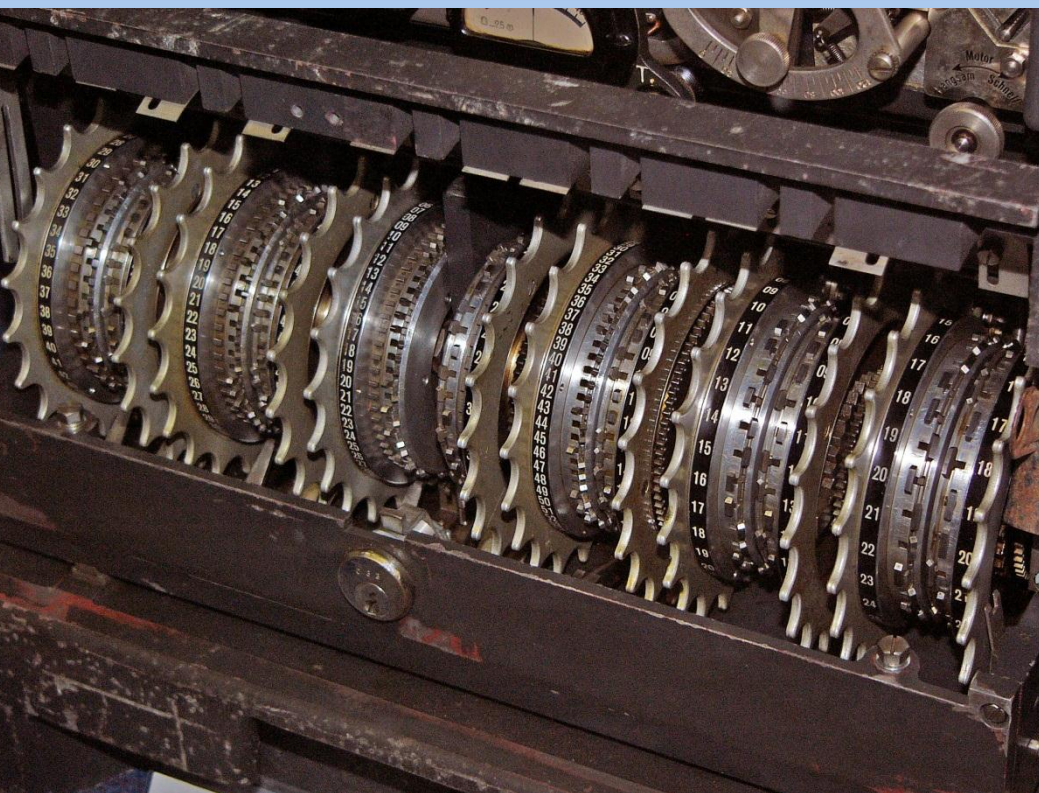
חולשות:

- אי יכולת להצפין אות בעצמה

לאחר מלה"ע השנייה:

- מכירה של מכונות אניגמה ע"י ארה"ב ובריטניה, תוך הצהרה שהן בטוחות...

לורנץ וקולוסוס



- קולוסוס סימן 1 – פבואר 1944
- קולוסוס סימן 2 – יוני 1944

צפנים ממוחשבים

הפעלת פעולות מתמטיות על הודעה בקוד ASCII

הודעה:

Haifux = 01001000, 01100001, 01101001, 01100110, 01110101, 01111000.

אלגוריתם: הכפלה של כל אות במפתח
מפתח: 2

צופן:

10010000, 11000010, 11010010, 11001100, 11101010, 11110000

אינסוף אלגוריתמים להצפנה – אין הגבלה בגלל נוחות השימוש

AES vs DES

AES

- פותח ע"י יואן דימן ווינסט ריימן
- התקבל כתקן בשנת 2001
- שיתוף הקהילה בתכנון ותחרות, ללא ה-NSA

DES

- פותח בשנת 1975 ע"י IBM וה-NSA
- התקבל כתקן הצפנה בשנת 1976
- לא היה שיתוף של הקהילה בתכנון

RC4

- פותח בשנת 1987 במעבדות RSA ע"י רונלד ריבסט
- משמש ב-SSL וב-WEP
- הודלף בשנת 1994 באופן אנונימי באינטרנט
- בסופו של דבר ההדלפה אומתה ע"י ריבסט

בעיית הפצת המפתחות

רשת של 15 משתתפים:

$$15 * 14 * 3 = 630$$

רשת של 20 משתתפים:

$$20 * 19 * 3 = 1140$$

רשת של 50 משתתפים:

$$50 * 49 * 3 = 7350$$

רשת של 100 משתתפים:

$$100 * 99 * 3 = 29700$$

פרוטוקול דיפי - הלמן

שלבים:

תיאום ערכי Y ו- P ($2 < Y < P$) לפונקצייה $Y^X \pmod{P}$ באמצעות קו לא מאובטח

בוב:

1. בחירת מספר סודי: B

2. חישוב של $Y^B \pmod{P}$

3. סימון התוצאה כ- β ושליחה

4. חישוב של $Y^\alpha \pmod{P}$

אליס:

1. בחירת מספר סודי: A

2. חישוב של $Y^A \pmod{P}$

3. סימון התוצאה כ- α ושליחה

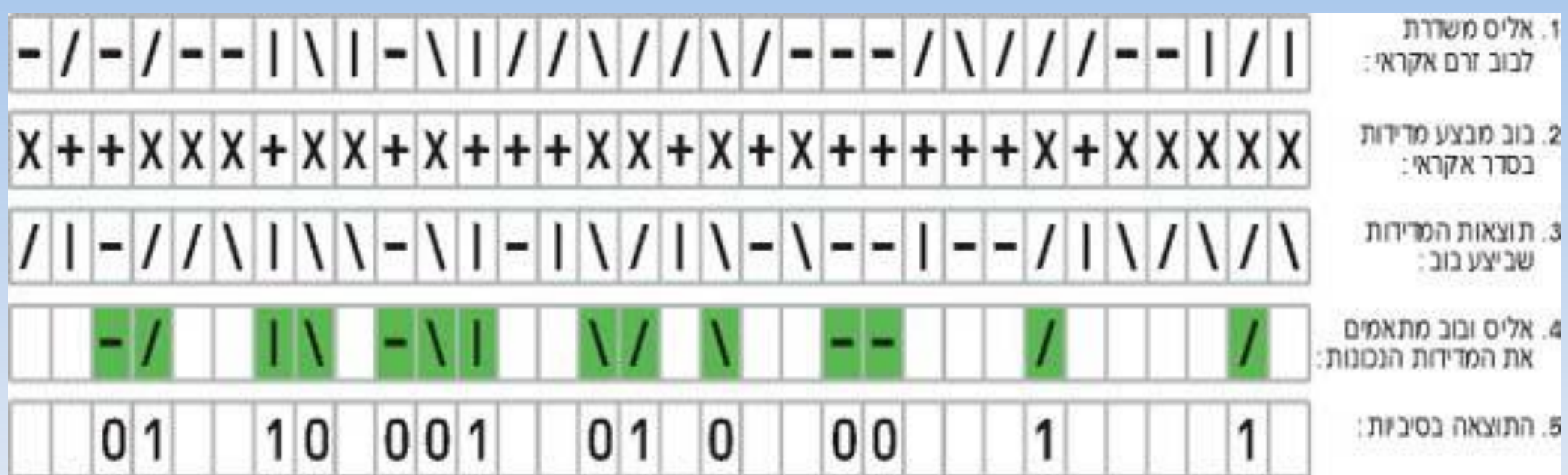
4. חישוב של $Y^\beta \pmod{P}$

איב

תוצאה זהה: K

רשת אמון ומסיבת החלפת מפתחות

הצפנה קוואנטית



העתיד של ההצפנה

אלגוריתם למציאת מספרים ראשוניים מתוך מכפלתם?

מחשוב קוואנטי?

הצפנה קוואנטית?

תקופת ביניים?

ומה הלאה?

אז מה היה לנו?

- ענפי הקריפטולוגיה
- הצפנה סימטרית
- הצפנה אסימטרית
- הצפנה קוואנטית
- העתיד של הקריפטולוגיה

שאלות? תגובות? הערות?



פורסם ע"י זהבית סודאי