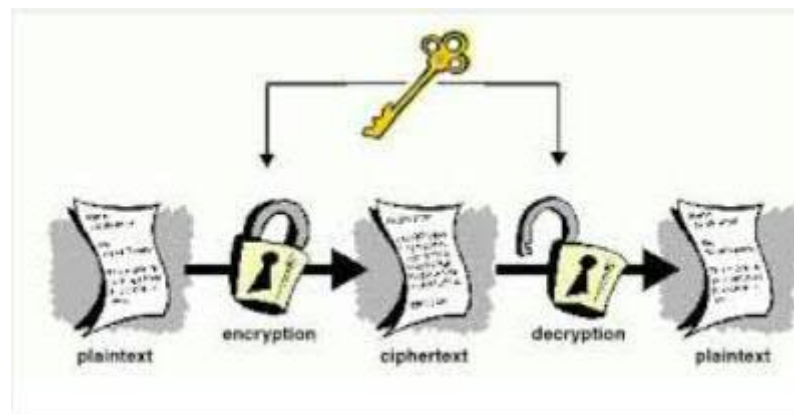


צפנים וקודים

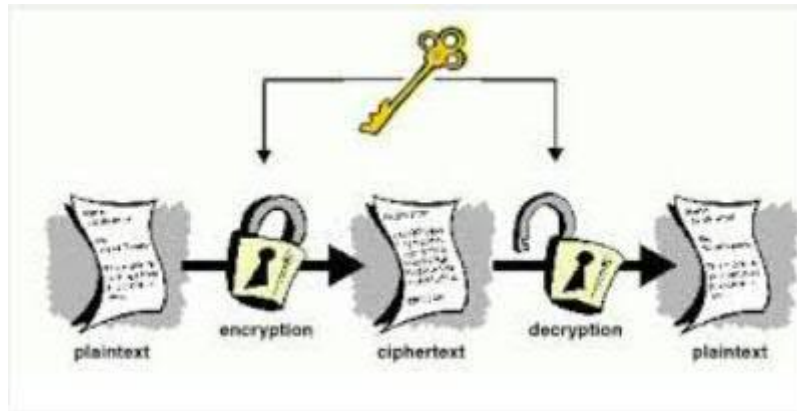
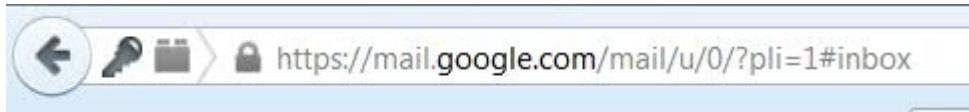
שלי גריון



הצפנה



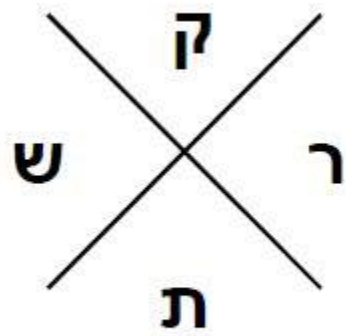
הצפנה



- מה זה צופן?
- למה מצפינים?
- מה מצפינים?
- איך מצפינים?

צופן החלפה – דוגמא

צופן פיג-פן



ל	כ	י
•	•	•
ס	נ	מ
•	•	•
צ	פ	ע
•	•	•

ג	ב	א
ו	ה	ד
ט	ח	ז

דוגמא: נצפין ביחד את ההודעה:

מחר הטיול

פעילות בקבוצות: פענוח כתב סתרים



צופן החלפה – דוגמא

צופן אתב"ש

• הכינו טבלת אתב"ש:

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

• צופן החלפה הוא צופן שבו כל אות בטקסט מוצפנת על-ידי אות אחרת או סימן אחר מוצפן.



צופן החלפה – דוגמא

צופן אתב"ש

• הכינו טבלת אתב"ש:

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

• הנביא ירמיהו מנבא פורענות על שני עמים, אך הוא מצפין את שמות העמים עליהם ניבא. נסו לגלות על מי הנבואות:

• "איך נלכדה ששך ותיתפס קהילת כל ארץ" (ירמיהו נ"א מ"א)

• "הנני מעיר על ... יושבי לבקמי רוח משחית" (ירמיהו נ"א א')

חידה

כמה אפשרויות יש לייצר צפני החלפה בהם מחליפים
כל-אחת מאותיות הא"ב באות אחרת מהא"ב?



פתרון החידה

כמה אפשרויות יש לייצר צפני החלפה בהם מחליפים כל-אחת מאותיות הא"ב באות אחרת מהא"ב?

1,124,000,727,777,607,680,000



יותר ממספר גרגירי החול בכדור הארץ!

צופן הזזה – דוגמא

צופן קיסר

• צופן קיסר הוא דוגמא לצופן הזזה שבו כל אות מוזזת שלושה צעדים קדימה.

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

• דוגמא: נפענח ביחד את המוצפן:

נס חנהלול

• פעילות בזוגות: הצפנת הודעות בעזרת גלגלי ההצפנה.



חידה

הידיעה הבאה הוצפנה בצופן הזזה כלשהו, אך אינכן יודעות מהו גודל ההזזה.
נסו בכל-זאת לפענח את הצופן.

The image shows a rectangular box containing the Hebrew word 'פפנימו' (Pepnimo) written in a cursive, handwritten style. The letters are black on a light, textured background.

צופן ערבול

• הסקיי-טייל שימש כמכשיר הצפנה לצבא ביוון העתיקה לפני 2400 שנה.



• דוגמא: הכנת מסר סודי.

צופן ערבול

- הסקיי-טייל שימש כמכשיר הצפנה לצבא ביוון העתיקה לפני 2400 שנה.



- צופן שבו האותיות משנות את מיקומן, אך אינן מוחלפות באותיות אחרות נקרא צופן ערבול.
- פעילות בקבוצה: ערבול שמות.

צופן האניגמה

מלחמת העולם ה-II



מלחמת הצוללות

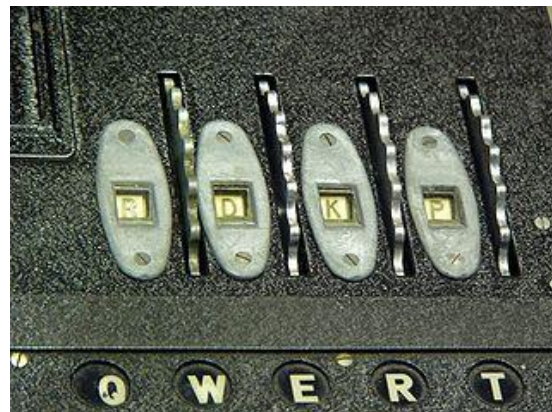


האניגמה



סודקות את תקרת הזכוכית - מאי 2015

איך זה עובד?



פיצוח האניגמה

בלצ'לי פארק



אלן טיורינג

Alan Turing

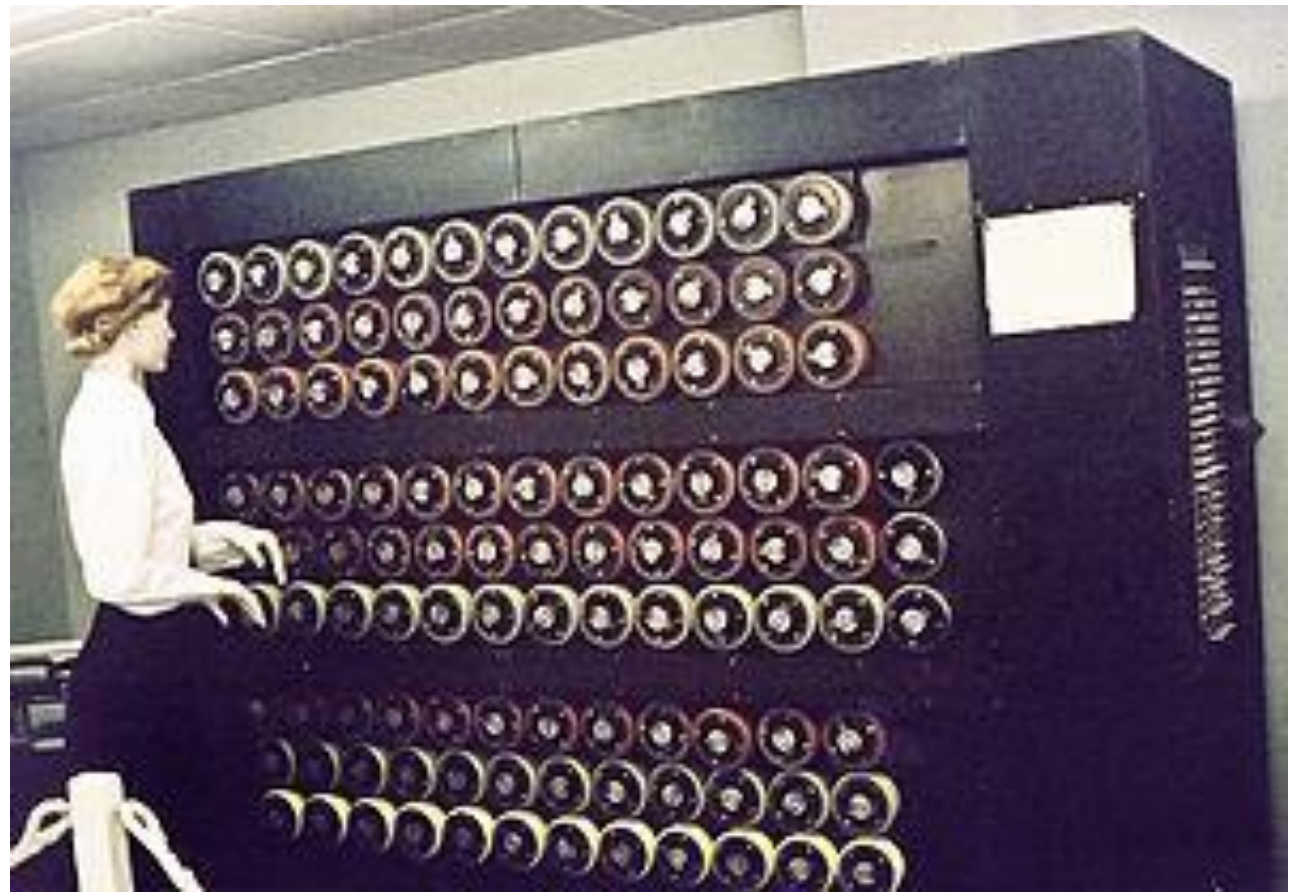
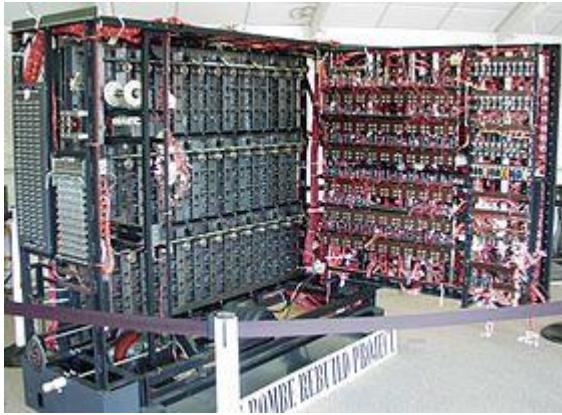
1954 – 1912



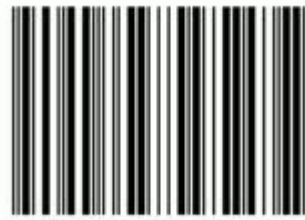
תרומות עיקריות

ממניחי היסודות למדעי המחשב. היה הדמות המרכזית בפיצוח מכונת ההצפנה "אניגמה". הוגה הרעיונות החשובים של מכונת טיורינג ומבחן טיורינג.

פיצוח האניגמה - בומבה



קודים



56.310 243.031 3

קוד לגילוי שגיאות ספרת ביקורת



- מה זו ספרת ביקורת?
- למה צריך ספרת ביקורת?
- אילו שגיאות עלולות לקרות?

חישוב ספרת ביקורת של מספר תעודת הזהות

								רשמו את מספר תעודת הזהות (כולל ספרת ביקורת) ב-9 ספרות	
1	2	1	2	1	2	1	2	X	מתחת למספר אנו רושמים מספרים שנקראים משקלים
								X	כפלו כל ספרה מתעודת הזהות בספרה שמתחתיה (המשקל)
								X	הפכו את התוצאות לספרה אחת: אם יצא מספר דו-ספרתי חשבו את סכום הספרות שלו
									חברו את סכום כל הספרות לקבלת תוצאה
X	X	X	X	X	X	X	X		חשבו את ספרת האחדות של התוצאה שהתקבלה
X	X	X	X	X	X	X	X		חשבו את הפרש: 10 פחות המספר שהתקבל – זו ספרת הביקורת!

- אילו שגיאות ספרת הביקורת הזו מוצאת?
- אילו שגיאות ספרת הביקורת הזו לא מוצאת?

