

הצפנה

ההיסטוריה מלאה דוגמאות כבר לפחות 3000 שנה. אנשים מאז ומעולם הסתקרנו לדעת מה אחד מוסר לרעהו.

בעבר בעיקר מסרים צבאיים נשמרו בסוד. הרצון להעביר מסר לאחד או יותר מקומות או אנשים, מעלה מיידית את האפשרות שהמסר יקלט בדרך על ידי גורם בלתי רצוי - מה שנקרא Interception



זוהי מרי מלכת סקוטלנד שזממה להדיח את בת דודתה, אליזבת, מלכת אנגליה. היא הועמדה למשפט בשנת 1586. מרי התכתבה עם בני בריתה בעזרת הודעות

מוצפנות. בני בריתה הורשעו על פי הודאתם והוצאו להורג. כעת, גורלה של מרי יקבע אם יהיה ניתן לפענח את הצופן של מכתביה לקושרים (שהיו בידי בית המשפט והתובעים).

שובר הקודים הטוב בממלכה, נקרא למשימה ואתם מוזמנים לבדוק מה עלה בגורל הצופן ובגורלה של מרי.

בעיקרון ישנן שתי שיטות של הצפנת מסרים. האחת נקראת: **סימטרית והשניה א-סימטרית**. אנחנו נלמד את שתיהן, למרות שהיום בעיר משתמשים בשיטה השניה.

ההבדל העיקרי ביניהן זה שבשיטה הסימטרית קיים מפתח אחד להצפנה ולפיענוח. בהנחה שרק הצדדים המעורבים יודעים אותו, אפשר להבטיח סודיות.

בשיטה השניה שניקראת גם פרייבט קי / פבליק קי, הרבה (כולם) יכולים לדעת את מפתח ההצפנה (פבליק), אבל רק הצד המקבל יודע את מפתח הפיענוח (פרייבט).

הצפנה סימטרית

ישנן שתי דרכים עיקריות. הזזה או החלפה (transposition or substitution)

הזזה

קודם נראה מה שנקרא 'צופן יוליוס קייסר', קובעים מפתח שהוא מקדם הזזה. למשל מפתח שהוא 3 (המפתח יהיה כל מספר בין 1 ל 25, או כפולות שלהם). למשל 21 או 210 זה אותו מפתח בעיקרון. תמיד אפשר לקחת את המודולו 25 (השארית בחלוקה) של המספר, או בפייתון: 25%n. (ההזזה היא מעגלית. למשל Y הופך ל B).

נראה איך זה עובד עם מפתח 3:

ההודעה החופשית (ללא הצפנה):

The fox jumped over the fence

ההודעה המוצפנת:

Wkg ira mxpshg ryhu wkg igqfg

כעת נכתוב 2 תוכניות. אחת מקבלת משפט באנגלית, מפתח הצפנה ואינדיקציה אם רוצים הצפנה או פיענוח. התוכנית תדפיס את המשפט החדש (המוצפן או המפוענח).

התוכנית השניה תקבל רק משפט מוצפן ותצטרך לתת כפלט את מפתח ההצפנה.

על פי הכללים עד כה, לא ממש קשה למצוא את המפתח.

אפשר כמובן לעשות טרנספוזיציות הרבה יותר קשות, במיוחד לטקסט ארוך. למשל עבור משפט באורך 35 תוים ישנן 35! (35 עצרת אפשרויות לסידורים שונים שזה בערך: 50,000,000,000,000,000,000,000,000 אפשרויות).

החלפה - Substitution

למשל, נקבע את הצופן הבא:

a b c d e f g
j a p l w i q

שלא כמו בצופן הקיסר שבו ישנם רק 25 מפתחות אפשריים, בצופן החלפה כזה ישנם: 400,000,000,000,000,000,000,000,000 אפשרויות.

אם האוייב יכול לבדוק כל אפשרות בשניה אחת, יקח לו מיליארד פעם חיי היקום לבדוק את כולן.

נקודה למחשבה

ניסיון מעניין לפענח הודעות מוצפנות על ידי צופן החלפה מתבסס על תדירות הופעת אותיות.

ידועה לנו טבלה של אחוזי המופעים של אותיות מניתוח מספר רב של טקסטים באנגלית, כלהלן:

<u>Letter</u>	<u>Percentage</u>
a	8.1
b	1.5
c	2.8
d	4.3
e	12.7
f	2.2
g	2.0
h	6.1
.	.
.	.
.	.
.	.
z	0.1