
גיבוב (Hash)



CYBER SCHOOL



השיעור מציג את מושג הגיבוב, שיטות ליישום וכיצד ניתן לנתח ולעבוד עם נתונים שעברו Hash.

מושגים בהצפנה

אלגוריתמים ל-Hash





CYBER SCHOOL

קריפטוגרפיה (הצפנה) מעשית

מושגים בהצפנה

הצפנה (קריפטוגרפיה)



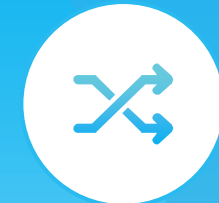
כאשר משתמש מגדיר סיסמה במחשב Windows10, מערכת ההפעלה מאחסנת אותה באופן מקומי עם ה-hash שלה.



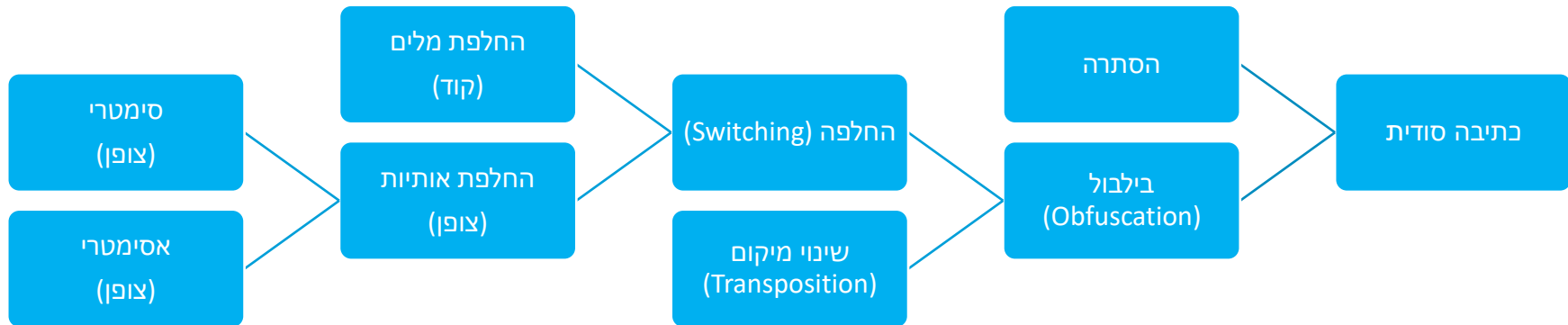
מה זה?
קריפטוגרפיה היא ענף של המתמטיקה המשמשת כדי להבטיח תקשורת מאובטחת.



שיטות הצפנה



ניתן ליישם קריפטוגרפיה במספר דרכים, כפי שמוצג בתרשים.



תיאור השיטות



להלן הסברים על כל שיטת הצפנה.

הסתרה	הסתרת הודעה כך שלא ניתן לחשוף אותה.
בילבול (Obfuscation)	ערבול טקסט כדי להפוך אותו לבלתי קריא.
שינוי מיקום	שינוי סדר האותיות.
החלפה (Switching)	החלפת אותיות באותיות אחרות או מילים במילים אחרות.
סימטרי	מפתח אחד הן להצפנה והן לפענוח.
אסימטרי	מפתח אחד להצפנה, ואחר לפענוח.





קידוד



Hashing
(גיבוב)



צופן סימטרי



צופן אסימטרי

טכנולוגיות משתמשות בטכניקות אלה כדי להסתיר נתונים חשובים.





מטרת הקידוד

הקידוד נעשה כדי להפוך נתונים מפורמט שמתאים למערכת אחת לפורמט שניתן לשלוח אותו למערכת אחרת ועדיין להשתמש בהם כראוי.

קידוד תווים

שיטה לייצוג קבוצת תווים עם קבוצת תווים אחרת.

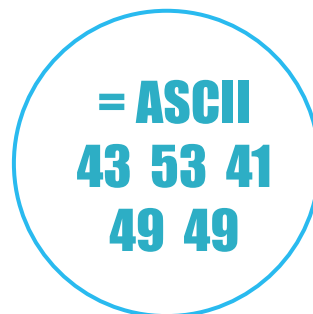




Base64



Base32



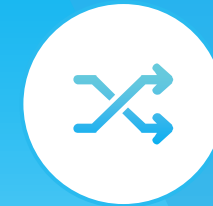
ASCII-Hex



קוד מורס



קידוד מבוסס Base64



הוספת דיפון
אם יש צורך,

התאמת האות
הנכונה מטבלה
משותפת

חלוקת הערכים
הבינאריים
לקבוצות של 6
ביט

שילוב הערכים
הבינאריים

המרת ASCII
לבינארי



טבלת 64 Base Charset



מכיוון שרצף של ששה ביטים מניב $2^6=64$ אפשרויות, טבלת המרות Base64 כוללת 64 ערכים.

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
Padding		=									



Base64 בפייתון



ניתן לקודד ולפענח נתונים באופן אוטומטי באמצעות פייתון.
ספריית Base64 מכילה פונקציות קידוד ופענוח.
קידוד ופענוח Base64 הוא תהליך פשוט וקל להבנה.

```
import base64
data = "This is text!"

# Standard Base64 Encoding
encodedBytes = base64.b64encode(data.encode("utf-8"))
encodedStr = str(encodedBytes, "utf-8")
print(encodedStr)

# Standard Base64 decoding
decodedBytes = base64.b64decode(encodedStr)
decodedStr = str(decodedBytes, "utf-8")
print(decodedStr)
```

Output:

```
VGhpcyBpcyB0ZXh0IQ==
```

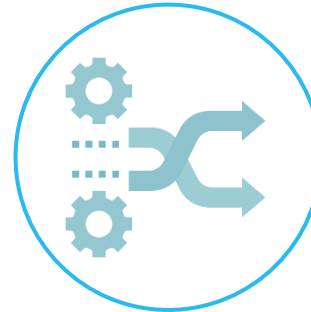
```
This is text!
```



מקרה מבחן - אניגמה



מכונת Enigma הייתה מכשיר שנועד לספק מידע מוצפן.



אבטחת המערכת התבססה על הגדרות אשר שונו מדי יום.



הצפנת האניגמה נפרצה בשנת 1932, ושוב בשנת 1941.



מעבדה - קידוד ידני מבוסס Base64



30 - 15 דקות 

המשימה

תרגול קידוד Base64 ידני.

השלבים

- יש להשיג ערך בינארי.
- יש לחלק אותו לקבוצות של שישה ביט.
- יש להמיר אותו לאותיות הנכונות.
- יש לבדוק את התוצאות.

קבצים קשורים

מסמך מעבדה

כלים

דפדפן



CYBER SCHOOL



CYBER SCHOOL

קריפטוגרפיה (הצפנה) מעשית

אלגוריתמים לפונקציית Hash (גיבוב)

אלגוריתמים לפונקציית Hash (גיבוב)

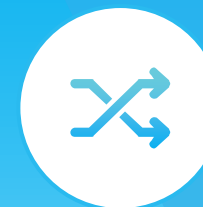


פונקציה חד כיוונית
Hash ממיר קלט בכל אורך לפלט בעל אורך קבוע
מראש.



עיצוב הפונקציה
כל שינוי בקלט יגרום לשינוי משמעותי בפלט.

אלגוריתמים נפוצים



משמעות	סוג Hash
מפתח ייחודי באורך 128 ביט	MD5
מפתח ייחודי באורך 160 ביט	SHA1
מפתח ייחודי באורך 256 ביט	SHA256
מפתח ייחודי באורך 384 ביט	SHA384
מפתח ייחודי באורך 512 ביט	SHA512
מפתח ייחודי באורך 128 ביט, גרסה של MD4	NT Hash



LSASS



טבלאות Hash



פתרונות
הלבנה



כלים לזיהוי
פורנזי

טכנולוגיות רבות עובדות עם hashes כדי להשיג
פונקציונליות משופרת.

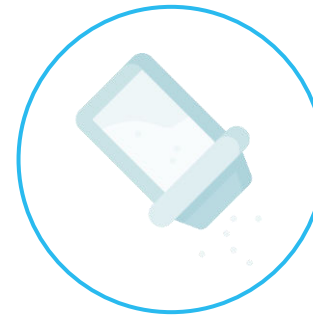


Salt & Pepper



Salt

נתונים אקראיים המשמשים כקלט נוסף לפונקציית hash או ביטוי סיסמה.



Pepper

אינדיקציה סודית שנוספה לטקסט לפני שעובר hash על ידי פונקציית hash.



ניתן להשתמש ב Salt ו-Pepper כחיזוק כנגד התקפות brute-force.



טבלת Rainbow



משמשת לפיצוח hash.
רשימה מוגדרת מראש של hashes.
חוסכת זמן בזמן התקפת brute-force.



מעבדה - פיצוח של Hash Rainbow Table



30 - 45 דקות

המשימה

יש לפצח את ה-hash הנתון באמצעות טבלת rainbow.

השלב

יש ליצור טבלת rainbow.

יש לפצח את ה-Hash.

קבצים קשורים

מסמך מעבדה

כלים

Rtsort
rcrack

VirtualBox
Kali Linux
Rtgen



CYBER SCHOOL



שאלות?

