אבטחת מידע 10313

<u>תרגיל 1 – פיתרון</u>

מרצה: ד"ר עמית קליינמן

בודק: ערד פלד

1. **פגיעות** היא פרצת אבטחה במערכת, **ניצול** הוא קטע קוד או מידע המנצל את פרצת האבטחה במטרה לשנות את ההתנהגות הרצויה של המערכת.
בדיקות חדירות הן מתקפות מתוכננות ומבוקרות במטרה למצוא פגיעויות במערכת, פעמים רבות הארגון משלם עליהן כסף כדי לשפר את אבטחת המידע במערכות שלו.

.2

א. לפיתרון שאלה זו ניתן להשתמש בנוסחאות הבאות ובטבלה:

For Encryption:

$$C_i = (P_i + K_i) \bmod 26$$

For Decryption:

$$P_i = (C_i - K_i) \bmod 26$$

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	
18	19	20	21	22	23	24	25	

תחילה נכתוב את הסתר והמפתח ונתרגם אותם למספרים מהטבלה:

C	U	E	P	N		K	W	N	A	J		T	U	B	L
	20	4	15	13		10	22	13	0	9		19	20	1	11
K	S	E	C	U		R	I	T	Y						
	18	4	2	20		17	8	19	24						
P															

לאחר מכן, נשתמש בנוסחת הפענוח ונשלים את המפתח עם הגלוי שנקבל:
(הטבלה היא לאחר 3 צעדי פענוח)

C	U	E	P	N		K	W	N	A	J		T	U	B	L
	20	4	15	13		10	22	13	0	9		19	20	1	11
K	S	E	C	U		R	I	T	Y	**C**		**A**	**N**		
	18	4	2	20		17	8	19	24	**2**		**0**	**13**		
P	**C**	**A**	**N**												
	2	**0**	**13**												

כך תראה הטבלה לאחר כל הפענוח:

C	U	E	P	N		K	W	N	A	J		T	U	B	L
	20	4	15	13		10	22	13	0	9		19	20	1	11
K	S	E	C	U		R	I	T	Y	**C**		**A**	**N**	**T**	**T**
	18	4	2	20		17	8	19	24	**2**		**0**	**13**	**19**	**19**
P	**C**	**A**	**N**	**T**		**T**	**O**	**U**	**C**	**H**		**T**	**H**	**I**	**S**
	2	**0**	**13**	**19**		**19**	**14**	**20**	**2**	**7**		**19**	**7**	**8**	**18**

אפשר לראות שהמסר הוא **Cant Touch This**.

ב. חל שיבוש באות ה-31, לכן נצפה שהתו ה-31 יפוענח לא נכון.
המפתח תלוי בתווים שבגלוי ואורכו המקורי הוא 8, לכן תהיה לנו טעות במפתח בתו ה-39 (8+31).
מכיוון שהמפתח שגוי בתו ה-39, גם הפענוח של התו ה-39 יהיה לא נכון מה שיגרור תו שגוי נוסף במפתח במקום ה-47 (8+39) וכך כל 8 תווים עד סוף המסר.

ג. לאחר שנצפין פעם נוספת עם אותו המפתח, נקבל את הסתר **MIRH BEGYD XJOV**.
נמלא שוב את הטבלה ונחפש מפתח מתאים, נוכל למצוא מפתח כזה באורך המסר:

C	M	I	R	H		B	E	G	Y	D		X	J	O	V
	12	8	17	7		1	4	6	24	3		23	9	14	21
K															
P	C	A	N	T		T	O	U	C	H		T	H	I	S
	2	0	13	19		19	14	20	2	7		19	7	8	18

הפעם נשתמש בנוסחא כדי למצוא את המפתח:

C	M	I	R	H		B	E	G	Y	D		X	J	O	V
	12	8	17	7		1	4	6	24	3		23	9	14	21
K	**K**	**I**	**E**	**O**		**I**	**Q**	**M**	**W**	**W**		**E**	**C**	**G**	**D**
	10	**8**	**4**	**14**		**8**	**16**	**12**	**22**	**22**		**4**	**2**	**6**	**3**
P	C	A	N	T		T	O	U	C	H		T	H	I	S
	2	0	13	19		19	14	20	2	7		19	7	8	18

המפתח הוא **KIEOIQMWWECGD**.

3. תחילה נכתוב את השם לפי הדרישה בשאלה – **ARADPELLEDBC**, זה יהיה הגלוי (Plain text).
בעזרת המפתח **CYBER**, נצפין את הגלוי כדי לקבל את הסתר (Cipher text).

לצופן Vigenère, ניתן להשתמש בנוסחאות הבאות :

Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i + 26) \bmod 26$

נרצה להצפין ולכן נשתמש בנוסחא הראשונה, ראשית נמלא את הטבלה עם הגלוי והמפתח:

P	A	R	A	D	P	E	L	L	E	D	B	C
	0	17	0	3	15	4	11	11	4	3	1	2
K	C	Y	B	E	R	C	Y	B	E	R	C	Y
	2	24	1	4	17	2	24	1	4	17	2	24
C	**C**	**P**	**B**	**H**	**G**	**G**	**J**	**M**	**I**	**U**	**D**	**A**
	2	15	1	7	6	6	9	12	8	20	3	0

לי יצא הסתר **CPBHGGJMIUDA**, לכל אחד אמור לצאת משהו שונה בהתאם לשם שלו אך זה תהליך ההצפנה.

4. מתקפת כוח גס הינה מתקפה בה עובדים בשיטה של ניסוי וטעייה במטרה למצוא ערך מסויים, בדרך כלל סיסמא או מפתח הצפנה.
שיטה זו איננה מעשית עבור פרוטוקולי האבטחה המודרניים המקובלים לשימוש היום מכיוון שביצועה יכול לקחת אפילו כמה שנים.
לעומת זאת, ישנם מקרים בהם התקפה זו יכולה לעבוד במצבים בהם המחשב יכול לעמוד בבדיקה של כל האופציות בזמן סביר, למשל מערכת הדורשת סיסמא באורך 4 תווים המכילה רק ספרות.