אבטחת מידע – מטלה 1

אלעזר פיין

1. כיצד אפשר לדעת אם מערכת מאובטחת? נבצע Vulnerability Scans + **Penetration-Testing** – נחפש נקודות תורפה **Vulnerabilities** אותן ניתן לתקוף באמצעות **Exploits** – מתקפה המנצלת את הפגיעות הספציפית, נתקוף ונראה האם וכיצד המערכת מתמודדת.

2. א. בשיטה זו הPLAINTEXT שאנחנו כבר פיצחנו נוסף לKEY על מנת לפצח את שאר הCIPHER.

CIPHER TEXT: **UEPN KWNAJ TUBL**
PRIMER: **SECURITY**
FULL KEY: **SECURITYCANTTOUCHTHIS (autokey – append plain txt to primer for full key)**
PLAIN TEXT: **CANT TOUCH THIS**

	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	
	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	
A	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	10
B	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	A	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	3,9
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	2
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	6
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	11
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	5
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	1
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	7, 12, 13
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	4
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	8
Z	Z	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	

LENGEND

- PLAINTEXT
- PRIMER-KEY
- CIPHERTEXT
- PLAINTEXT ACTING AS KEY (AUTOKEY)

ב. בעצם בשיטה זו הPLAINTEXT מתחלק לשורות באורך של הPRIMER כאשר כל שורה היא הKEY לשורה שמתחתיה, לכן האותיות שיפגעו הן אותן אותיות בעמודה של האות שנפגעה מאותה אות והלאה:

```
SECURITY

CANTTOUC     8
HTHISABC     16
DEFGHIJK     24
LMNOPQ?S     32
TUVWXY?A     40
BCDEFG?I     48
```

במקרה זה כל אות במיקום {31+8n | n >= 0} תיפגם, כל השאר בסדר.

ג. כן, ברור שניתן כי אם הפעלנו n פונקציות f כדי להגיע ממחרוזת A למחרוזת B, זו בעצם הרכבת פונקציות אז לפי הגדרה (אין פה בעיית תחום\טווח) קיימת פונקציה F אשר מחליפה את ההרכבה (F(A) = f(f(A)) = B).

המפתח הוא: **KIEOIQMWWECGD**, בגלל שהוצפן פעמיים צריך להיות באורך הPLAINTEXT כדי לפצח בצעד אחד.

3. ויז'נר רגיל, המפתח חוזר על עצמו עד אורך הPLAINTEXT.

PLAINTEXT: ELAZARFINEAB
KEY: CYBERCYBERCY
CIPHERTEXT: GJBDRTDJRVCZ

		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
E	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
L	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
A	B	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	A
Z	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
A	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
F	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
I	B	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	A
N	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
A	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
B	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

4. **Brute-Force Attack** זו שיטת התקפה בה מנסים כל צופן\סיסמא אפשרית עד שמוצאים את הנכונה. שיטה זו עדיין נפוצה בשימוש כיום ומהווה איום משמעותי, מכיוון שאינה מסתמכת על נק' תורפה במערכת אלא על סיסמאות חלשות \ נפוצות \ קלות לניחוש. שיטה זו פחות מעשית עבור סיסמאות מורכבות וארוכות (זמן מחשב ארוך מדי לפיצוח), ו\או כאשר יש שכבות הגנה נוספות (לדוגמא MFA). אם עומד לרשותנו כוח חישוב מספק והצלחנו לצמצם את מרחב האפשרויות, והמטרה רלוונטית מבחינת חשיבות (לדוגמא אנשים\גופים ספציפיים) ו\או היקף (לדוגמא מאגרי חשבונות \ משתמשים) אז הגיוני שנבחר בה, במיוחד כי היא פחות ידנית ויותר משהו שנבצע בעזרת אוטומציה. המשאב העיקרי שמגביל אותנו הוא זמן.