אבטחת מידע – מטלה 2

אלעזר פיין

.1

1.1 חסרונות:

א. החיסרון העיקרי שהאיץ את תהליך הפיצוח היא העובדה שאות לא מוחלפת עם עצמה. אפשר לחפש בצופן חלק צפוי מראש כמו "הייל היטלר" ולמצוא אותו ע"י ניסוי חלקים בצופן שאינם מכילים אף אות ממנו, כשמוצאים חלק כזה מנסים לפצח את שאר הצופן לפי התבנית המוסקת.
למעשה הבריטים פיתחו מכונה המבוססת על אניגמה שתיקנה את החיסרון הזה (TYPEX), והייתה אמצעי התקשורת הבריטי היחיד שהגרמנים לא הצליחו לפענח.

ב. 2 הצדדים המתקשרים חייבים להשתמש באותה קונפיגורציה, לגרמנים הייתה טבלה חודשית בה עבור כל יום הייתה רשומה הגדרה אחרת למכונה כל שכולם היום מתואמים. אם בעלות הברית הצליחו להשיג טבלה שכזו, אז הם היו יכולים לקרוא הודעות עד סוף אותו חודש ללא בעיה.

ג. בתחילת כל הודעה היו מעבירים את המפתח לאותה תשדורת פעמיים, כך שישר יודעים שהאות במקום ה- i בתחילת המסר שווה לאות במקום ה- i + len(key). הפולנים השתמשו בעובדה זו ע"מ לבנות שרשראות של אותיות כאשר לכל שרשרת יש קשר חד ערכי לקונפיגורציה ומפתח.

1.2 מספר אופציות:

$$\binom{5}{3} * 3! * 26^3 = 1{,}054{,}560$$

בחירת 3 דסקיות מתוך חמש
סידור פנימי של הדסקיות
בחירת מפתח באורך 3 מתוך 26 אותיות האלף בית

1.3

	1→4	2→5	3→6
A	C	P	G
B	T	D	K
C	A	U	H
D	Q	I	Q
E	F	R	V
F	B	M	Y
G	E	F	F
H	I	O	A
I	H	H	E
J	P	S	R
K	L	B	I
L	M	N	O

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

ניתן לראות לפי טבלה #1 כי המפתח המתאים לאורכי השרשראות הנ"ל הוא **ABE**.

2. נשתמש באלגוריתם הבא:

```
def gcd(n, m):
    if n % m == 0:
        return m
    return gcd(m, n % m)
```

I. 195 % 13 = 0 -> gcd(195, 13) = **13**

II. gcd(250, 17) = gcd(17, 12) = gcd(12, 5) = gcd(5, 2)
= gcd(2, 1) = **1**

III. gcd(2021, 60) = gcd(60, 41) = gcd(41, 19) = gcd(19, 3)
= gcd(3, 1) = **1**

IV. gcd(333, 259) = gcd(259, 74)
= gcd(74, 37) = **37**

V. gcd(908, 907)
= gcd(907, 1) = **1**

.3

Algorithm:

1. Find the quotient (Q) and the remainder (R) when max is divided by min.

   ➔ R = max(a,b) – Q*min(a,b)

2. If R = 0, then gcd(a, b) = min. The expression for the previous value of R gives an expression for gcd(a, b) in terms of a and b. Stop.

3. Otherwise, use the current values of min and R as the new values and go back to step 1.

S

.I

max	min	Q	R	R = max - Q*min	R(a,b)
2020	151	13	57	57 = max - 13d	**57 = a - 13b**
151	57	2	37	37 = max - 2d	37 =b - 2(a - 13b) = **-2a + 27b**
57	37	1	20	20 = max - d	20 = (a - 13b) - (-2a + 27b) = **3a - 40b**
37	20	1	17	17 = max - d	17 = (-2a + 27b) - (3a -40b) = **-5a + 67b**
20	17	1	3	3 = max - d	3 = (3a - 40b) - (-5a + 67b) = **8a - 107b**
17	3	5	2	2 = max - 5d	2 = (-5a + 67b) - 5(8a - 107b) = **-45a + 602b**
3	2	1	1	1 = max - d	1 = (8a - 107b) - (-45a + 602b) = **53a - 709b**
1	1	1	0	0 = max - d	0 = (-45a + 602b) - (53a - 709b) = **-98a + 1311b**

➔ x = 53, y = -709, gcd(2020, 151) = 1

.II

max	min	Q	R	R = max - Q*min	R(a,b)
2020	275	7	95	95 = c - 7d	**95 = a - 7b**
275	95	2	85	85 = c - 2d	85 = b - 2(a - 7b)= **-2a + 15b**
95	85	1	10	10 = c - d	10 = (a - 7b) - (-2a + 15b) **= 3a - 22b**
85	10	8	5	5 = c - 8d	5 = (-2a + 15b) -8(3a - 22b) **= -26a + 191b**
10	5	2	0	0 = c - 2d	0 = (3a - 22b) - 2(-26a + 191b) **= 55a - 404b**

➔ x = -26, y = 101, gcd(2020, 275) = 5