20 אוגוסט 2021

אבטחת מידע 10313

<u>פתרון תרגיל 2</u>

מרצה: ד"ר עמית קליינמן

בודק: ערד פלד

.1

a. The 3 weaknesses of the German messages and/or the Enigma machine itself which helped to break the Enigma code during WW2 are:
    i. The fact that any letter of the plaintext can not remain an identical letter in the corresponding position at the ciphertext.
    ii. A repeated identical message format in different messages (e.g., the date was written at the head of the message and salute to Hitler at the end of the message) enabled a known plaintext attack.
    iii. The fact that the session key was transmitted twice in a row at the beginning of the message. The key length was 3 letters and thus the 1st letter of the message was the same as the 4th letter, the 2nd same as the 5th and the 3ed same as the 6th. The polish Marian Rejewski built letter chains of the above-mentioned letter correspondences and characterized any of the enigma configurations by the lengths of these chains. When the polish absorbed Enigma ciphertexts, letter chains were built and examined and the Enigma configuration (and master-key) was deduced according to the chain lengths.

b. $\frac{5!}{3!\cdot 2!}$ 3! x 26^3 = 1054560

c. The master key is **ABE** since the 3 calculated chain lengths that were assembled out of the 30 absorbed messages (see the following page) are identical to the 3 chain lengths of the master key ABE as appeared in the database (the 1st record) of table 1.

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

2. המחלק המשותף הגדול ביותר ((Greatest Common Divisor (GCD)
GCD לזוגות הבאים כולל חישובים:

I. GCD(195,13) = GCD(15·13,13) = 13
II. GCD(250,17) = GCD(5·5·5·2,17) = 1
III. GCD(2021,60) = GCD(43·47,2·2·3·5) = 1
IV. GCD(333,259) = GCD(3·3·37,37·7) = 37
V. GCD(908,907) = GCD(2·2·227,907) = 1

3. אלגוריתם אוקלידס המורחב (Extended Euclidean Algorithm)
מצא X ו-Y המקיימים את המשוואות הבאות. בבקשה הצג את חישובייך

I. x·2020 + y·151 = GCD(2020,151)
II. x·2020 + y·275 = GCD(2020,275)

I. x·2020 + y·151 = GCD(2020,151)

a. 2020 = 13·151 + 57
b. 151 = 2·57+ 37
c. 57= 37·1 + 20
d. 37 = 20·1 + 17
e. 20 = 17·1 + 3
f. 17 = 3·5 + 2
g. 3 = 2·1 + **1**

1 = 3 - 2·1 = 3 - (17 - 3·5) = 6·3 - 17 = 6·(20-17·1) - 17 =
= 6·20 - 7·17 = 6·20 - 7·(37 - 20·1) = 13·20 - 7·37 =
= 13·(57-37·1) - 7·37 = 13·57 - 20·37 = 13·57 - 20·(151 - 2·57) =
53·57 - 20·151 = 53·(2020 - 13·151) - 20·151 = 53·2020 - 709·151 = 1

X=53, y=-709

II. x·2020+ y·275 = GCD(2020,275)

a. 2020 = 7·275 + 95
b. 275 = 2·95 + 85
c. 95 = 85·1 + 10
d. 85 = 10·8 + **5**
e. 10 = 5·2 + 0

5 = 85 - 8·10 = 85 – 8· (95-85·1) = 9·85 - 8·95 =
9·(275 - 2·95) - 8·95 = 9·275 - 26·95
9·275 - 26·(2020-7·275) = 191·275 - 26·2020 = 5

x=-26, y=191