

מבוא להצפנה – תרגיל 4

.1

.א.

In this chapter we calculate the private key d using the extended Euclidean algorithm.

```
i = 0, r = 33,      s = 0, t = 1
i = 1, r = 17, q = 1, s = 1, t = 0
i = 2, r = 16, q = 1, s = -1, t = 1
i = 3, r = 1, q = 16, s = 2, t = -1
```

we got that $1 = 17*(2) + 33*(-1)$

So:

The value of s is 2

The value of t is -1

Now we calculate:

$C_a^s * C_b^t = m^{(se_a)} * m^{(te_b)} = m^{(se_a + te_b)} = m \pmod{16157}$

Calculate 11671^{-1} :

First we need to calculate the inverse of 11671: $11671^{-1} = 11671^{-1} \pmod{16157}$

Now we calculate it using the extended Euclidean algorithm:

```
i = 0, r = 16157,      s = 0, t = 1
i = 1, r = 11671, q = 1, s = 1, t = 0
i = 2, r = 4486, q = 2, s = -1, t = 1
i = 3, r = 2699, q = 1, s = 3, t = -2
i = 4, r = 1787, q = 1, s = -4, t = 3
i = 5, r = 912, q = 1, s = 7, t = -5
i = 6, r = 875, q = 1, s = -11, t = 8
i = 7, r = 37, q = 23, s = 18, t = -13
i = 8, r = 24, q = 1, s = -425, t = 307
i = 9, r = 13, q = 1, s = 443, t = -320
i = 10, r = 11, q = 1, s = -868, t = 627
i = 11, r = 2, q = 5, s = 1311, t = -947
i = 12, r = 1, q = 2, s = -7423, t = 5362
```

we got that $1 = 11671*(-7423) + 16157*(5362)$

So:

The value of s is -7423

The value of t is 5362

```
The inverse of 11671 is -7423 (mod 16157)
11671-1 = -7423 = 8734 (mod 16157)
Now we calculate 11671-1 = 87341 (mod 16157):
using the square and multiply algorithm:
1 in binary is [1]
-----
i = 0
e_i = 1
z2 = 1 (mod 16157)
z*8734 = 8734*8734 = 8734 (mod 16157)
-----
And we got that 11671-1 = 8734 (mod 16157)

=====
Now we calculate:
72242 = (mod 16157)

2 in binary is [1, 0]
-----
i = 0
e_i = 1
z2 = 1 (mod 16157)
z*7224 = 7224*7224 = 7224 (mod 16157)
-----
i = 1
e_i = 0
z2 = 12 = 15223 (mod 16157)
-----
And we got that 72242 = 15223 (mod 16157)

=====
The message is: 15223X8734 = 1729 (mod 16157)
=====
```

ב.

In this chapter we calculate the private key d using the extended Euclidean algorithm.

```
i = 0, r = 33,      s = 0, t = 1
i = 1, r = 17, q = 1, s = 1, t = 0
i = 2, r = 16, q = 1, s = -1, t = 1
i = 3, r = 1, q = 16, s = 2, t = -1
```

we got that $1 = 17 \cdot (2) + 33 \cdot (-1)$

So:

The value of s is 2

The value of t is -1

Now we calculate:

$$C_a^s \cdot C_b^t = m^{(se_a)} \cdot m^{(te_b)} = m^{(se_a + te_b)} = m \pmod{16157}$$

Calculate 11449^{-1} :

First we need to calculate the inverse of 11449: $11449^{-1} = 11449^{-1} \pmod{16157}$

Now we calculate it using the extended Euclidean algorithm:

```
i = 0, r = 16157,      s = 0, t = 1
i = 1, r = 11449, q = 1, s = 1, t = 0
i = 2, r = 4708, q = 2, s = -1, t = 1
i = 3, r = 2033, q = 2, s = 3, t = -2
i = 4, r = 642, q = 3, s = -7, t = 5
i = 5, r = 107, q = 6, s = 24, t = -17
```

we got that $107 = 11449 \cdot (24) + 16157 \cdot (-17)$

So:

The value of s is 24

The value of t is -17

The inverse of 11449 is 24 $\pmod{16157}$

$$11449^{-1} = 24 = 24 \pmod{16157}$$

Now we calculate $11449^{-1} = 24^1 \pmod{16157}$:

using the square and multiply algorithm:

1 in binary is [1]

$i = 0$

$e_i = 1$

$$z^2 = 1 \pmod{16157}$$

$$z^{*24} = 24^{*24} = 24 \pmod{16157}$$

```
-----  
And we got that  $11449^{-1} = 24 \pmod{16157}$ 
```

```
=====
```

Now we calculate:

$13910^2 \pmod{16157}$

2 in binary is [1, 0]

```
-----
```

$i = 0$

$e_i = 1$

$z^2 = 1 \pmod{16157}$

$z \cdot 13910 = 13910 \cdot 13910 = 13910 \pmod{16157}$

```
-----
```

$i = 1$

$e_i = 0$

$z^2 = 1^2 = 8025 \pmod{16157}$

```
-----
```

And we got that $13910^2 = 8025 \pmod{16157}$

```
=====
```

The message is: $8025 \cdot 24 = 14873 \pmod{16157}$

```
=====
```

.2

.א

To check if 18 is a creator of the group Z_{349} we will calculate the following:

=====

1. $324^0 = 5832 \bmod 349 = 324$
2. $248^1 = 4464 \bmod 349 = 248$
3. $276^2 = 4968 \bmod 349 = 276$
4. $82^3 = 1476 \bmod 349 = 82$
5. $80^4 = 1440 \bmod 349 = 80$
6. $44^5 = 792 \bmod 349 = 44$
7. $94^6 = 1692 \bmod 349 = 94$
8. $296^7 = 5328 \bmod 349 = 296$
9. $93^8 = 1674 \bmod 349 = 93$
10. $278^9 = 5004 \bmod 349 = 278$
11. $118^{10} = 2124 \bmod 349 = 118$
12. $30^{11} = 540 \bmod 349 = 30$
13. $191^{12} = 3438 \bmod 349 = 191$
14. $297^{13} = 5346 \bmod 349 = 297$
15. $111^{14} = 1998 \bmod 349 = 111$
16. $253^{15} = 4554 \bmod 349 = 253$
17. $17^{16} = 306 \bmod 349 = 17$
18. $306^{17} = 5508 \bmod 349 = 306$
19. $273^{18} = 4914 \bmod 349 = 273$
20. $28^{19} = 504 \bmod 349 = 28$
21. $155^{20} = 2790 \bmod 349 = 155$
22. $347^{21} = 6246 \bmod 349 = 347$
23. $313^{22} = 5634 \bmod 349 = 313$
24. $50^{23} = 900 \bmod 349 = 50$
25. $202^{24} = 3636 \bmod 349 = 202$
26. $146^{25} = 2628 \bmod 349 = 146$
27. $185^{26} = 3330 \bmod 349 = 185$
28. $189^{27} = 3402 \bmod 349 = 189$
29. $261^{28} = 4698 \bmod 349 = 261$
30. $161^{29} = 2898 \bmod 349 = 161$
31. $106^{30} = 1908 \bmod 349 = 106$
32. $163^{31} = 2934 \bmod 349 = 163$
33. $142^{32} = 2556 \bmod 349 = 142$
34. $113^{33} = 2034 \bmod 349 = 113$
35. $289^{34} = 5202 \bmod 349 = 289$
36. $316^{35} = 5688 \bmod 349 = 316$
37. $104^{36} = 1872 \bmod 349 = 104$
38. $127^{37} = 2286 \bmod 349 = 127$
39. $192^{38} = 3456 \bmod 349 = 192$

```
40.  $315^{39} = 5670 \bmod 349 = 315$ 
41.  $86^{40} = 1548 \bmod 349 = 86$ 
42.  $152^{41} = 2736 \bmod 349 = 152$ 
43.  $293^{42} = 5274 \bmod 349 = 293$ 
44.  $39^{43} = 702 \bmod 349 = 39$ 
45.  $4^{44} = 72 \bmod 349 = 4$ 
46.  $72^{45} = 1296 \bmod 349 = 72$ 
47.  $249^{46} = 4482 \bmod 349 = 249$ 
48.  $294^{47} = 5292 \bmod 349 = 294$ 
49.  $57^{48} = 1026 \bmod 349 = 57$ 
50.  $328^{49} = 5904 \bmod 349 = 328$ 
51.  $320^{50} = 5760 \bmod 349 = 320$ 
52.  $176^{51} = 3168 \bmod 349 = 176$ 
53.  $27^{52} = 486 \bmod 349 = 27$ 
54.  $137^{53} = 2466 \bmod 349 = 137$ 
55.  $23^{54} = 414 \bmod 349 = 23$ 
56.  $65^{55} = 1170 \bmod 349 = 65$ 
57.  $123^{56} = 2214 \bmod 349 = 123$ 
58.  $120^{57} = 2160 \bmod 349 = 120$ 
59.  $66^{58} = 1188 \bmod 349 = 66$ 
60.  $141^{59} = 2538 \bmod 349 = 141$ 
61.  $95^{60} = 1710 \bmod 349 = 95$ 
62.  $314^{61} = 5652 \bmod 349 = 314$ 
63.  $68^{62} = 1224 \bmod 349 = 68$ 
64.  $177^{63} = 3186 \bmod 349 = 177$ 
65.  $45^{64} = 810 \bmod 349 = 45$ 
66.  $112^{65} = 2016 \bmod 349 = 112$ 
67.  $271^{66} = 4878 \bmod 349 = 271$ 
68.  $341^{67} = 6138 \bmod 349 = 341$ 
69.  $205^{68} = 3690 \bmod 349 = 205$ 
70.  $200^{69} = 3600 \bmod 349 = 200$ 
71.  $110^{70} = 1980 \bmod 349 = 110$ 
72.  $235^{71} = 4230 \bmod 349 = 235$ 
73.  $42^{72} = 756 \bmod 349 = 42$ 
74.  $58^{73} = 1044 \bmod 349 = 58$ 
75.  $346^{74} = 6228 \bmod 349 = 346$ 
76.  $295^{75} = 5310 \bmod 349 = 295$ 
77.  $75^{76} = 1350 \bmod 349 = 75$ 
78.  $303^{77} = 5454 \bmod 349 = 303$ 
79.  $219^{78} = 3942 \bmod 349 = 219$ 
80.  $103^{79} = 1854 \bmod 349 = 103$ 
81.  $109^{80} = 1962 \bmod 349 = 109$ 
82.  $217^{81} = 3906 \bmod 349 = 217$ 
83.  $67^{82} = 1206 \bmod 349 = 67$ 
84.  $159^{83} = 2862 \bmod 349 = 159$ 
85.  $70^{84} = 1260 \bmod 349 = 70$ 
86.  $213^{85} = 3834 \bmod 349 = 213$ 
```

```
87. 344^86 = 6192 mod 349 = 344
88. 259^87 = 4662 mod 349 = 259
89. 125^88 = 2250 mod 349 = 125
90. 156^89 = 2808 mod 349 = 156
91. 16^90 = 288 mod 349 = 16
92. 288^91 = 5184 mod 349 = 288
93. 298^92 = 5364 mod 349 = 298
94. 129^93 = 2322 mod 349 = 129
95. 228^94 = 4104 mod 349 = 228
96. 265^95 = 4770 mod 349 = 265
97. 233^96 = 4194 mod 349 = 233
98. 6^97 = 108 mod 349 = 6
99. 108^98 = 1944 mod 349 = 108
100. 199^99 = 3582 mod 349 = 199
101. 92^100 = 1656 mod 349 = 92
102. 260^101 = 4680 mod 349 = 260
103. 143^102 = 2574 mod 349 = 143
104. 131^103 = 2358 mod 349 = 131
105. 264^104 = 4752 mod 349 = 264
106. 215^105 = 3870 mod 349 = 215
107. 31^106 = 558 mod 349 = 31
108. 209^107 = 3762 mod 349 = 209
109. 272^108 = 4896 mod 349 = 272
110. 10^109 = 180 mod 349 = 10
111. 180^110 = 3240 mod 349 = 180
112. 99^111 = 1782 mod 349 = 99
113. 37^112 = 666 mod 349 = 37
114. 317^113 = 5706 mod 349 = 317
115. 122^114 = 2196 mod 349 = 122
116. 102^115 = 1836 mod 349 = 102
117. 91^116 = 1638 mod 349 = 91
118. 242^117 = 4356 mod 349 = 242
119. 168^118 = 3024 mod 349 = 168
120. 232^119 = 4176 mod 349 = 232
121. 337^120 = 6066 mod 349 = 337
122. 133^121 = 2394 mod 349 = 133
123. 300^122 = 5400 mod 349 = 300
124. 165^123 = 2970 mod 349 = 165
125. 178^124 = 3204 mod 349 = 178
126. 63^125 = 1134 mod 349 = 63
127. 87^126 = 1566 mod 349 = 87
128. 170^127 = 3060 mod 349 = 170
129. 268^128 = 4824 mod 349 = 268
130. 287^129 = 5166 mod 349 = 287
131. 280^130 = 5040 mod 349 = 280
132. 154^131 = 2772 mod 349 = 154
133. 329^132 = 5922 mod 349 = 329
```

```
134.  $338^{133} = 6084 \bmod 349 = 338$ 
135.  $151^{134} = 2718 \bmod 349 = 151$ 
136.  $275^{135} = 4950 \bmod 349 = 275$ 
137.  $64^{136} = 1152 \bmod 349 = 64$ 
138.  $105^{137} = 1890 \bmod 349 = 105$ 
139.  $145^{138} = 2610 \bmod 349 = 145$ 
140.  $167^{139} = 3006 \bmod 349 = 167$ 
141.  $214^{140} = 3852 \bmod 349 = 214$ 
142.  $13^{141} = 234 \bmod 349 = 13$ 
143.  $234^{142} = 4212 \bmod 349 = 234$ 
144.  $24^{143} = 432 \bmod 349 = 24$ 
145.  $83^{144} = 1494 \bmod 349 = 83$ 
146.  $98^{145} = 1764 \bmod 349 = 98$ 
147.  $19^{146} = 342 \bmod 349 = 19$ 
148.  $342^{147} = 6156 \bmod 349 = 342$ 
149.  $223^{148} = 4014 \bmod 349 = 223$ 
150.  $175^{149} = 3150 \bmod 349 = 175$ 
151.  $9^{150} = 162 \bmod 349 = 9$ 
152.  $162^{151} = 2916 \bmod 349 = 162$ 
153.  $124^{152} = 2232 \bmod 349 = 124$ 
154.  $138^{153} = 2484 \bmod 349 = 138$ 
155.  $41^{154} = 738 \bmod 349 = 41$ 
156.  $40^{155} = 720 \bmod 349 = 40$ 
157.  $22^{156} = 396 \bmod 349 = 22$ 
158.  $47^{157} = 846 \bmod 349 = 47$ 
159.  $148^{158} = 2664 \bmod 349 = 148$ 
160.  $221^{159} = 3978 \bmod 349 = 221$ 
161.  $139^{160} = 2502 \bmod 349 = 139$ 
162.  $59^{161} = 1062 \bmod 349 = 59$ 
163.  $15^{162} = 270 \bmod 349 = 15$ 
164.  $270^{163} = 4860 \bmod 349 = 270$ 
165.  $323^{164} = 5814 \bmod 349 = 323$ 
166.  $230^{165} = 4140 \bmod 349 = 230$ 
167.  $301^{166} = 5418 \bmod 349 = 301$ 
168.  $183^{167} = 3294 \bmod 349 = 183$ 
169.  $153^{168} = 2754 \bmod 349 = 153$ 
170.  $311^{169} = 5598 \bmod 349 = 311$ 
171.  $14^{170} = 252 \bmod 349 = 14$ 
172.  $252^{171} = 4536 \bmod 349 = 252$ 
173.  $348^{172} = 6264 \bmod 349 = 348$ 
174.  $331^{173} = 5958 \bmod 349 = 331$ 
175.  $25^{174} = 450 \bmod 349 = 25$ 
176.  $101^{175} = 1818 \bmod 349 = 101$ 
177.  $73^{176} = 1314 \bmod 349 = 73$ 
178.  $267^{177} = 4806 \bmod 349 = 267$ 
179.  $269^{178} = 4842 \bmod 349 = 269$ 
180.  $305^{179} = 5490 \bmod 349 = 305$ 
```



```
181. 255^180 = 4590 mod 349 = 255
182. 53^181 = 954 mod 349 = 53
183. 256^182 = 4608 mod 349 = 256
184. 71^183 = 1278 mod 349 = 71
185. 231^184 = 4158 mod 349 = 231
186. 319^185 = 5742 mod 349 = 319
187. 158^186 = 2844 mod 349 = 158
188. 52^187 = 936 mod 349 = 52
189. 238^188 = 4284 mod 349 = 238
190. 96^189 = 1728 mod 349 = 96
191. 332^190 = 5976 mod 349 = 332
192. 43^191 = 774 mod 349 = 43
193. 76^192 = 1368 mod 349 = 76
194. 321^193 = 5778 mod 349 = 321
195. 194^194 = 3492 mod 349 = 194
196. 2^195 = 36 mod 349 = 2
197. 36^196 = 648 mod 349 = 36
198. 299^197 = 5382 mod 349 = 299
199. 147^198 = 2646 mod 349 = 147
200. 203^199 = 3654 mod 349 = 203
201. 164^200 = 2952 mod 349 = 164
202. 160^201 = 2880 mod 349 = 160
203. 88^202 = 1584 mod 349 = 88
204. 188^203 = 3384 mod 349 = 188
205. 243^204 = 4374 mod 349 = 243
206. 186^205 = 3348 mod 349 = 186
207. 207^206 = 3726 mod 349 = 207
208. 236^207 = 4248 mod 349 = 236
209. 60^208 = 1080 mod 349 = 60
210. 33^209 = 594 mod 349 = 33
211. 245^210 = 4410 mod 349 = 245
212. 222^211 = 3996 mod 349 = 222
213. 157^212 = 2826 mod 349 = 157
214. 34^213 = 612 mod 349 = 34
215. 263^214 = 4734 mod 349 = 263
216. 197^215 = 3546 mod 349 = 197
217. 56^216 = 1008 mod 349 = 56
218. 310^217 = 5580 mod 349 = 310
219. 345^218 = 6210 mod 349 = 345
220. 277^219 = 4986 mod 349 = 277
221. 100^220 = 1800 mod 349 = 100
222. 55^221 = 990 mod 349 = 55
223. 292^222 = 5256 mod 349 = 292
224. 21^223 = 378 mod 349 = 21
225. 29^224 = 522 mod 349 = 29
226. 173^225 = 3114 mod 349 = 173
227. 322^226 = 5796 mod 349 = 322
```

```
228. 212^227 = 3816 mod 349 = 212
229. 326^228 = 5868 mod 349 = 326
230. 284^229 = 5112 mod 349 = 284
231. 226^230 = 4068 mod 349 = 226
232. 229^231 = 4122 mod 349 = 229
233. 283^232 = 5094 mod 349 = 283
234. 208^233 = 3744 mod 349 = 208
235. 254^234 = 4572 mod 349 = 254
236. 35^235 = 630 mod 349 = 35
237. 281^236 = 5058 mod 349 = 281
238. 172^237 = 3096 mod 349 = 172
239. 304^238 = 5472 mod 349 = 304
240. 237^239 = 4266 mod 349 = 237
241. 78^240 = 1404 mod 349 = 78
242. 8^241 = 144 mod 349 = 8
243. 144^242 = 2592 mod 349 = 144
244. 149^243 = 2682 mod 349 = 149
245. 239^244 = 4302 mod 349 = 239
246. 114^245 = 2052 mod 349 = 114
247. 307^246 = 5526 mod 349 = 307
248. 291^247 = 5238 mod 349 = 291
249. 3^248 = 54 mod 349 = 3
250. 54^249 = 972 mod 349 = 54
251. 274^250 = 4932 mod 349 = 274
252. 46^251 = 828 mod 349 = 46
253. 130^252 = 2340 mod 349 = 130
254. 246^253 = 4428 mod 349 = 246
255. 240^254 = 4320 mod 349 = 240
256. 132^255 = 2376 mod 349 = 132
257. 282^256 = 5076 mod 349 = 282
258. 190^257 = 3420 mod 349 = 190
259. 279^258 = 5022 mod 349 = 279
260. 136^259 = 2448 mod 349 = 136
261. 5^260 = 90 mod 349 = 5
262. 90^261 = 1620 mod 349 = 90
263. 224^262 = 4032 mod 349 = 224
264. 193^263 = 3474 mod 349 = 193
265. 333^264 = 5994 mod 349 = 333
266. 61^265 = 1098 mod 349 = 61
267. 51^266 = 918 mod 349 = 51
268. 220^267 = 3960 mod 349 = 220
269. 121^268 = 2178 mod 349 = 121
270. 84^269 = 1512 mod 349 = 84
271. 116^270 = 2088 mod 349 = 116
272. 343^271 = 6174 mod 349 = 343
273. 241^272 = 4338 mod 349 = 241
274. 150^273 = 2700 mod 349 = 150
```

```
275.  $257^{274} = 4626 \bmod 349 = 257$ 
276.  $89^{275} = 1602 \bmod 349 = 89$ 
277.  $206^{276} = 3708 \bmod 349 = 206$ 
278.  $218^{277} = 3924 \bmod 349 = 218$ 
279.  $85^{278} = 1530 \bmod 349 = 85$ 
280.  $134^{279} = 2412 \bmod 349 = 134$ 
281.  $318^{280} = 5724 \bmod 349 = 318$ 
282.  $140^{281} = 2520 \bmod 349 = 140$ 
283.  $77^{282} = 1386 \bmod 349 = 77$ 
284.  $339^{283} = 6102 \bmod 349 = 339$ 
285.  $169^{284} = 3042 \bmod 349 = 169$ 
286.  $250^{285} = 4500 \bmod 349 = 250$ 
287.  $312^{286} = 5616 \bmod 349 = 312$ 
288.  $32^{287} = 576 \bmod 349 = 32$ 
289.  $227^{288} = 4086 \bmod 349 = 227$ 
290.  $247^{289} = 4446 \bmod 349 = 247$ 
291.  $258^{290} = 4644 \bmod 349 = 258$ 
292.  $107^{291} = 1926 \bmod 349 = 107$ 
293.  $181^{292} = 3258 \bmod 349 = 181$ 
294.  $117^{293} = 2106 \bmod 349 = 117$ 
295.  $12^{294} = 216 \bmod 349 = 12$ 
296.  $216^{295} = 3888 \bmod 349 = 216$ 
297.  $49^{296} = 882 \bmod 349 = 49$ 
298.  $184^{297} = 3312 \bmod 349 = 184$ 
299.  $171^{298} = 3078 \bmod 349 = 171$ 
300.  $286^{299} = 5148 \bmod 349 = 286$ 
301.  $262^{300} = 4716 \bmod 349 = 262$ 
302.  $179^{301} = 3222 \bmod 349 = 179$ 
303.  $81^{302} = 1458 \bmod 349 = 81$ 
304.  $62^{303} = 1116 \bmod 349 = 62$ 
305.  $69^{304} = 1242 \bmod 349 = 69$ 
306.  $195^{305} = 3510 \bmod 349 = 195$ 
307.  $20^{306} = 360 \bmod 349 = 20$ 
308.  $11^{307} = 198 \bmod 349 = 11$ 
309.  $198^{308} = 3564 \bmod 349 = 198$ 
310.  $74^{309} = 1332 \bmod 349 = 74$ 
311.  $285^{310} = 5130 \bmod 349 = 285$ 
312.  $244^{311} = 4392 \bmod 349 = 244$ 
313.  $204^{312} = 3672 \bmod 349 = 204$ 
314.  $182^{313} = 3276 \bmod 349 = 182$ 
315.  $135^{314} = 2430 \bmod 349 = 135$ 
316.  $336^{315} = 6048 \bmod 349 = 336$ 
317.  $115^{316} = 2070 \bmod 349 = 115$ 
318.  $325^{317} = 5850 \bmod 349 = 325$ 
319.  $266^{318} = 4788 \bmod 349 = 266$ 
320.  $251^{319} = 4518 \bmod 349 = 251$ 
321.  $330^{320} = 5940 \bmod 349 = 330$ 
```

322. $7^{321} = 126 \bmod 349 = 7$
323. $126^{322} = 2268 \bmod 349 = 126$
324. $174^{323} = 3132 \bmod 349 = 174$
325. $340^{324} = 6120 \bmod 349 = 340$
326. $187^{325} = 3366 \bmod 349 = 187$
327. $225^{326} = 4050 \bmod 349 = 225$
328. $211^{327} = 3798 \bmod 349 = 211$
329. $308^{328} = 5544 \bmod 349 = 308$
330. $309^{329} = 5562 \bmod 349 = 309$
331. $327^{330} = 5886 \bmod 349 = 327$
332. $302^{331} = 5436 \bmod 349 = 302$
333. $201^{332} = 3618 \bmod 349 = 201$
334. $128^{333} = 2304 \bmod 349 = 128$
335. $210^{334} = 3780 \bmod 349 = 210$
336. $290^{335} = 5220 \bmod 349 = 290$
337. $334^{336} = 6012 \bmod 349 = 334$
338. $79^{337} = 1422 \bmod 349 = 79$
339. $26^{338} = 468 \bmod 349 = 26$
340. $119^{339} = 2142 \bmod 349 = 119$
341. $48^{340} = 864 \bmod 349 = 48$
342. $166^{341} = 2988 \bmod 349 = 166$
343. $196^{342} = 3528 \bmod 349 = 196$
344. $38^{343} = 684 \bmod 349 = 38$
345. $335^{344} = 6030 \bmod 349 = 335$
346. $97^{345} = 1746 \bmod 349 = 97$
347. $1^{346} = 18 \bmod 349 = 1$
348. $18^{347} = 324 \bmod 349 = 18$

=====

The group is:

```
[18, 324, 248, 276, 82, 80, 44, 94, 296, 93, 278, 118, 30, 191,
297, 111, 253, 17, 306, 273, 28, 155, 347, 313, 50, 202, 146,
185, 189, 261, 161, 106, 163, 142, 113, 289, 316, 104, 127, 192,
315, 86, 152, 293, 39, 4, 72, 249, 294, 57, 328, 320, 176, 27,
137, 23, 65, 123, 120, 66, 141, 95, 314, 68, 177, 45, 112, 271,
341, 205, 200, 110, 235, 42, 58, 346, 295, 75, 303, 219, 103,
109, 217, 67, 159, 70, 213, 344, 259, 125, 156, 16, 288, 298,
129, 228, 265, 233, 6, 108, 199, 92, 260, 143, 131, 264, 215, 31,
209, 272, 10, 180, 99, 37, 317, 122, 102, 91, 242, 168, 232, 337,
133, 300, 165, 178, 63, 87, 170, 268, 287, 280, 154, 329, 338,
151, 275, 64, 105, 145, 167, 214, 13, 234, 24, 83, 98, 19, 342,
223, 175, 9, 162, 124, 138, 41, 40, 22, 47, 148, 221, 139, 59,
15, 270, 323, 230, 301, 183, 153, 311, 14, 252, 348, 331, 25,
101, 73, 267, 269, 305, 255, 53, 256, 71, 231, 319, 158, 52, 238,
96, 332, 43, 76, 321, 194, 2, 36, 299, 147, 203, 164, 160, 88,
188, 243, 186, 207, 236, 60, 33, 245, 222, 157, 34, 263, 197, 56,
310, 345, 277, 100, 55, 292, 21, 29, 173, 322, 212, 326, 284,
226, 229, 283, 208, 254, 35, 281, 172, 304, 237, 78, 8, 144, 149,
239, 114, 307, 291, 3, 54, 274, 46, 130, 246, 240, 132, 282, 190,
279, 136, 5, 90, 224, 193, 333, 61, 51, 220, 121, 84, 116, 343,
241, 150, 257, 89, 206, 218, 85, 134, 318, 140, 77, 339, 169,
250, 312, 32, 227, 247, 258, 107, 181, 117, 12, 216, 49, 184,
171, 286, 262, 179, 81, 62, 69, 195, 20, 11, 198, 74, 285, 244,
204, 182, 135, 336, 115, 325, 266, 251, 330, 7, 126, 174, 340,
187, 225, 211, 308, 309, 327, 302, 201, 128, 210, 290, 334, 79,
26, 119, 48, 166, 196, 38, 335, 97, 1, 18]
```

The duplicates are: [18]

- The length of the group is: 349
- The length of the group without duplicates is: 348

YES 18 is a creator of the group Z_349

ב.

```
a = |G|
```

```
We are going to find the value of k such that ord(18^k) = 348 (mod 349)
We are going to find that by the formula: ord(a^k) = |G|/gcd(k, |G|)
```

```
-----
k = 2
18^k = 18^2 = 324
gcd(k, 348) = 2
ord(18^k) = ord(18^2) = 174
```

```
-----
k = 3
18^k = 18^3 = 80
gcd(k, 348) = 3
ord(18^k) = ord(18^3) = 116
```

```
-----
k = 4
18^k = 18^4 = 313
gcd(k, 348) = 4
ord(18^k) = ord(18^4) = 87
```

```
-----
k = 5
18^k = 18^5 = 168
gcd(k, 348) = 1
ord(18^k) = ord(18^5) = 348
```

```
=====
The value of k is: 5, and the order of 18^5 is: 348 (mod 349)
=====
```

b = 29

We are going to find the value of k such that $\text{ord}(18^k) = 29 \pmod{349}$

We are going to find that by the formula: $\text{ord}(a^k) = |G|/\text{gcd}(k, |G|)$

k = 2

$$18^k = 18^2 = 324$$

$$\text{gcd}(k, 348) = 2$$

$$\text{ord}(18^k) = \text{ord}(18^2) = 174$$

k = 3

$$18^k = 18^3 = 80$$

$$\text{gcd}(k, 348) = 3$$

$$\text{ord}(18^k) = \text{ord}(18^3) = 116$$

k = 4

$$18^k = 18^4 = 313$$

$$\text{gcd}(k, 348) = 4$$

$$\text{ord}(18^k) = \text{ord}(18^4) = 87$$

k = 5

$$18^k = 18^5 = 168$$

$$\text{gcd}(k, 348) = 1$$

$$\text{ord}(18^k) = \text{ord}(18^5) = 348$$

k = 6

$$18^k = 18^6 = 313$$

$$\text{gcd}(k, 348) = 6$$

$$\text{ord}(18^k) = \text{ord}(18^6) = 58$$

k = 7

$$18^k = 18^7 = 301$$

$$\text{gcd}(k, 348) = 1$$

$$\text{ord}(18^k) = \text{ord}(18^7) = 348$$

k = 8

$$18^k = 18^8 = 171$$

$$\text{gcd}(k, 348) = 4$$

$$\text{ord}(18^k) = \text{ord}(18^8) = 87$$

k = 9

$$18^k = 18^9 = 224$$

$$\text{gcd}(k, 348) = 3$$

$$\text{ord}(18^k) = \text{ord}(18^9) = 116$$

```
k = 10
18^k = 18^10 = 88
gcd(k, 348) = 2
ord(18^k) = ord(18^10) = 174
-----
k = 11
18^k = 18^11 = 41
gcd(k, 348) = 1
ord(18^k) = ord(18^11) = 348
-----
k = 12
18^k = 18^12 = 280
gcd(k, 348) = 12
ord(18^k) = ord(18^12) = 29
-----

=====
The value of k is: 12, and the order of 18^12 is: 29 (mod 349)
=====
```


ג.

נחשב את $L_{18}(7), L_{18}(11), L_{18}(3)$.

$$\begin{cases} 18^{54} = 27 = 3^3 \mod 349 \\ 18^{211} = 33 = 3 \times 11 \mod 349 \\ 18^{284} = 77 = 7 \times 11 \mod 349 \end{cases}$$

$$\Rightarrow \begin{cases} 54 = 3L_{18}(3) \mod 348 \\ 211 = L_{18}(3) + L_{18}(11) \mod 348 \\ 284 = L_{18}(7) + L_{18}(11) \mod 348 \end{cases}$$

$$L_{18}(3): 18 = L_{18}(3) \mod 116$$

$$18 \mod 116$$

$$18 + 116 = 134 \mod 116$$

$$134 + 116 = 250 \mod 116$$

$$L_{18}(3) = 18, 134, 250 \mod 348$$

נבדוק איזה ערך ייתן את $L_{18}(3)$:

$$18^{18} = 17 \mod 348$$

$$18^{134} = 329 \mod 348$$

$$18^{250} = 3 \mod 348$$

$$L_{18}(3) = 250, \text{ לכן}$$

$$\Rightarrow \begin{cases} 250 = L_{18}(3) \mod 348 \\ 211 = L_{18}(3) + L_{18}(11) \mod 348 \\ 284 = L_{18}(7) + L_{18}(11) \mod 348 \end{cases}$$

$$\Rightarrow \begin{cases} 250 = L_{18}(3) \mod 348 \\ 309 = L_{18}(11) \mod 348 \\ 284 = L_{18}(7) + L_{18}(11) \mod 348 \end{cases}$$

$$\Rightarrow \begin{cases} 250 = L_{18}(3) \mod 348 \\ 309 = L_{18}(11) \mod 348 \\ 323 = L_{18}(7) \mod 348 \end{cases}$$

$$\underline{\underline{\text{לסיכום, } L_{18}(7) = 323, L_{18}(11) = 309, L_{18}(3) = 250.}}$$

.ד

נחשב את $L_{18}(100)$.

$$100 \times 18^3 = 21 = 3 \times 7 \mod 349$$

$$\Rightarrow L_{18}(100) + 3 \equiv L_{18}(3) + L_{18}(7) \mod 348$$

$$\Rightarrow L_{18}(100) + 3 \equiv 250 + 323 \mod 348$$

$$\Rightarrow L_{18}(100) + 3 \equiv 225 \mod 348$$

$$\Rightarrow L_{18}(100) \equiv 222 \mod 348$$

$$L_{18}(100) \equiv 222 \Leftarrow$$

We are solving the discrete log problem with shanks algorithm.

The order of the group is 348 and $m = \text{ceil}(\sqrt{348}) = 19$

Now we are looking for $0 \leq i, j \leq 19$ such that:

$$18^{(i+19*j)} \mod 349 \Leftrightarrow 18^i = 202 \times (18^{(-19)^j} \mod 349)$$

Let's calculate the values of $18^i \mod 349$ for $0 \leq i \leq 19$:

i = 0: $18^0 \mod 349 = 1$
i = 1: $18^1 \mod 349 = 18$
i = 2: $18^2 \mod 349 = 324$
i = 3: $18^3 \mod 349 = 248$
i = 4: $18^4 \mod 349 = 276$
i = 5: $18^5 \mod 349 = 82$
i = 6: $18^6 \mod 349 = 80$
i = 7: $18^7 \mod 349 = 44$
i = 8: $18^8 \mod 349 = 94$
i = 9: $18^9 \mod 349 = 296$
i = 10: $18^{10} \mod 349 = 93$
i = 11: $18^{11} \mod 349 = 278$
i = 12: $18^{12} \mod 349 = 118$
i = 13: $18^{13} \mod 349 = 30$
i = 14: $18^{14} \mod 349 = 191$
i = 15: $18^{15} \mod 349 = 297$
i = 16: $18^{16} \mod 349 = 111$
i = 17: $18^{17} \mod 349 = 253$
i = 18: $18^{18} \mod 349 = 17$

Now let's calculate the values of $18^{(-19)^j} \mod 349$ for $0 \leq j \leq 19$ until we find a match in the i values:

j = 0:
 $202 \times 18^{(-19)^0} \mod 349 = 202$
202 is not in the i values

j = 1:
 $202 \times 18^{(-19)^1} \mod 349 = 44$

=====
We found a match in the i values: $44 = 18^7 \mod 349$
 $202 \times (18^{(-19)^1}) = 18^7 \mod 349$
 $\Leftrightarrow 202 = 18^{7+19*1} = 18^{26} \mod 349$

- Therefore the discrete log of 202 in base 18 mod 349 is 26

=====

.4

.א

```
We are going to send a symmetric key  $k = 111$  using the following
algorithm:
-----

1. Alice generates a random number 'a' from 'Z*_2002'.
a = 1229
 $a^1 = 821$ 

2. Bob generates a random number 'b' from 'Z*_2002' to.
b = 795
 $b^1 = 345$ 

3. Alice calculates  $K_1 = (k^a) \bmod p = (111^{1229}) \bmod 2003 = 1059$ 
And then sends  $K_1$  to Bob.

4. Bob calculates  $K_2 = (K_1^b) \bmod p = (1059^{795}) \bmod 2003 = 1700$ 
And then sends  $K_2$  to Alice.

5. Alice calculates  $K_3 = (K_2^{-a}) \bmod p = (1700^{-1229}) \bmod 2003 = 1059$ 
And then sends  $K_3$  to Bob.

6. Bob calculates  $K_4 = (K_3^{-b}) \bmod p = (1059^{-795}) \bmod 2003 = 111$ 
And then sends  $K_4$  to Alice.

=====
final we have  $K_4 = 111$  which is the symmetric key  $k = 111$ .
 $K_4 = 111, k = 111$ 
=====
```

ב.

נציג מתקפה מסוג "man in the middle" עבור הפרוטוקול הזה, שהתוצאה של המתקפה היא שאליס חושבת שהיא שולחת את K לבוב אבל בסוף ההתקפה התוקף מלורי מקבל את K ובוב מקבל בסוף מפתח K' שנקבע על ידי מלורי.

ההתקפה:

אליס שולחת לבוב את $K_1 = K^a \bmod p$.

מלורי שנמצאת באמצע בוחרת $C \in \mathbb{Z}_{p-1}^*$ הופכי, ומוסיפה ללא ידיעת אליס ובוב את $K_1' = K_1^C = K^{ac} \bmod p$ ושולחת את K_1' לבוב, ללא ידיעת אליס ובוב.

בוב מחשב את $K_2' = (K_1')^b = K^{abc}$ למרות שהוא ואליס חושבים שהוא מחשב את: $K_2 = K_1^b = K^{ab}$.

לאחר מכן אליס מחשבת את: $K_3' = (K_2')^{-a} = K^{bc}$.
ובוב מחשב את: $K' = K_4' = (K_3')^{-b} = K^c$.

כעת לבוב יש את: $K' = K^c$.

מלורי מחשבת כעת את: $K = K'^{-c} = (K_4')^{-c} = K$.

ולסיכום: לבוב יש את בסוף האלגוריתם את: $K' = K^c$.
ולמלורי יש בסוף האלגוריתם את: K .

