**מבוא להצפנה – תרגיל 4**

In this capter 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 (mod 16157)

Calculate 11671^-1:

First we need to calculate the inverse of 11671: 11671^-1 = 11671^-1 (mod 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 = 8734^1 (mod 16157):

using the square and multiply algorithm:

1 in binary is [1]

-----------------------------

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*8734 = 8734\*8734 = 8734 (mod 16157)

-----------------------------

And we got that 11671^-1 = 8734 (mod 16157)

============================

Now we calculate:

7224^2 = (mod 16157)

2 in binary is [1, 0]

-----------------------------

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*7224 = 7224\*7224 = 7224 (mod 16157)

-----------------------------

i = 1

e\_i = 0

z^2 = 1^2 = 15223 (mod 16157)

-----------------------------

And we got that 7224^2 = 15223 (mod 16157)

============================

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

============================

In this capter 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 (mod 16157)

Calculate 11449^-1:

First we need to calculate the inverse of 11449: 11449^-1 = 11449^-1 (mod 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\*(24) + 16157\*(-17)

-----------------

So:

The value of s is 24

The value of t is -17

-----------------

The inverse of 11449 is 24 (mod 16157)

11449^-1 = 24 = 24 (mod 16157)

Now we calculate 11449^-1 = 24^1 (mod 16157):

using the square and multiply algorithm:

1 in binary is [1]

-----------------------------

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*24 = 24\*24 = 24 (mod 16157)

-----------------------------

And we got that 11449^-1 = 24 (mod 16157)

============================

Now we calculate:

13910^2 = (mod 16157)

2 in binary is [1, 0]

-----------------------------

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*13910 = 13910\*13910 = 13910 (mod 16157)

-----------------------------

i = 1

e\_i = 0

z^2 = 1^2 = 8025 (mod 16157)

-----------------------------

And we got that 13910^2 = 8025 (mod 16157)

============================

The message is: 8025X24 = 14873 (mod 16157)

============================

To check if 18 is a creator of the group Z\_349 we will calculate the following:

=============================

2. 18^2 = 5832 mod 349 = 324

3. 18^3 = 4464 mod 349 = 248

4. 18^4 = 4968 mod 349 = 276

5. 18^5 = 1476 mod 349 = 82

6. 18^6 = 1440 mod 349 = 80

7. 18^7 = 792 mod 349 = 44

8. 18^8 = 1692 mod 349 = 94

9. 18^9 = 5328 mod 349 = 296

10. 18^10 = 1674 mod 349 = 93

11. 18^11 = 5004 mod 349 = 278

12. 18^12 = 2124 mod 349 = 118

13. 18^13 = 540 mod 349 = 30

14. 18^14 = 3438 mod 349 = 191

15. 18^15 = 5346 mod 349 = 297

16. 18^16 = 1998 mod 349 = 111

17. 18^17 = 4554 mod 349 = 253

18. 18^18 = 306 mod 349 = 17

19. 18^19 = 5508 mod 349 = 306

20. 18^20 = 4914 mod 349 = 273

21. 18^21 = 504 mod 349 = 28

22. 18^22 = 2790 mod 349 = 155

23. 18^23 = 6246 mod 349 = 347

24. 18^24 = 5634 mod 349 = 313

25. 18^25 = 900 mod 349 = 50

26. 18^26 = 3636 mod 349 = 202

27. 18^27 = 2628 mod 349 = 146

28. 18^28 = 3330 mod 349 = 185

29. 18^29 = 3402 mod 349 = 189

30. 18^30 = 4698 mod 349 = 261

31. 18^31 = 2898 mod 349 = 161

32. 18^32 = 1908 mod 349 = 106

33. 18^33 = 2934 mod 349 = 163

34. 18^34 = 2556 mod 349 = 142

35. 18^35 = 2034 mod 349 = 113

36. 18^36 = 5202 mod 349 = 289

37. 18^37 = 5688 mod 349 = 316

38. 18^38 = 1872 mod 349 = 104

39. 18^39 = 2286 mod 349 = 127

40. 18^40 = 3456 mod 349 = 192

41. 18^41 = 5670 mod 349 = 315

42. 18^42 = 1548 mod 349 = 86

43. 18^43 = 2736 mod 349 = 152

44. 18^44 = 5274 mod 349 = 293

45. 18^45 = 702 mod 349 = 39

46. 18^46 = 72 mod 349 = 4

47. 18^47 = 1296 mod 349 = 72

48. 18^48 = 4482 mod 349 = 249

49. 18^49 = 5292 mod 349 = 294

50. 18^50 = 1026 mod 349 = 57

51. 18^51 = 5904 mod 349 = 328

52. 18^52 = 5760 mod 349 = 320

53. 18^53 = 3168 mod 349 = 176

54. 18^54 = 486 mod 349 = 27

55. 18^55 = 2466 mod 349 = 137

56. 18^56 = 414 mod 349 = 23

57. 18^57 = 1170 mod 349 = 65

58. 18^58 = 2214 mod 349 = 123

59. 18^59 = 2160 mod 349 = 120

60. 18^60 = 1188 mod 349 = 66

61. 18^61 = 2538 mod 349 = 141

62. 18^62 = 1710 mod 349 = 95

63. 18^63 = 5652 mod 349 = 314

64. 18^64 = 1224 mod 349 = 68

65. 18^65 = 3186 mod 349 = 177

66. 18^66 = 810 mod 349 = 45

67. 18^67 = 2016 mod 349 = 112

68. 18^68 = 4878 mod 349 = 271

69. 18^69 = 6138 mod 349 = 341

70. 18^70 = 3690 mod 349 = 205

71. 18^71 = 3600 mod 349 = 200

72. 18^72 = 1980 mod 349 = 110

73. 18^73 = 4230 mod 349 = 235

74. 18^74 = 756 mod 349 = 42

75. 18^75 = 1044 mod 349 = 58

76. 18^76 = 6228 mod 349 = 346

77. 18^77 = 5310 mod 349 = 295

78. 18^78 = 1350 mod 349 = 75

79. 18^79 = 5454 mod 349 = 303

80. 18^80 = 3942 mod 349 = 219

81. 18^81 = 1854 mod 349 = 103

82. 18^82 = 1962 mod 349 = 109

83. 18^83 = 3906 mod 349 = 217

84. 18^84 = 1206 mod 349 = 67

85. 18^85 = 2862 mod 349 = 159

86. 18^86 = 1260 mod 349 = 70

87. 18^87 = 3834 mod 349 = 213

88. 18^88 = 6192 mod 349 = 344

89. 18^89 = 4662 mod 349 = 259

90. 18^90 = 2250 mod 349 = 125

91. 18^91 = 2808 mod 349 = 156

92. 18^92 = 288 mod 349 = 16

93. 18^93 = 5184 mod 349 = 288

94. 18^94 = 5364 mod 349 = 298

95. 18^95 = 2322 mod 349 = 129

96. 18^96 = 4104 mod 349 = 228

97. 18^97 = 4770 mod 349 = 265

98. 18^98 = 4194 mod 349 = 233

99. 18^99 = 108 mod 349 = 6

100. 18^100 = 1944 mod 349 = 108

101. 18^101 = 3582 mod 349 = 199

102. 18^102 = 1656 mod 349 = 92

103. 18^103 = 4680 mod 349 = 260

104. 18^104 = 2574 mod 349 = 143

105. 18^105 = 2358 mod 349 = 131

106. 18^106 = 4752 mod 349 = 264

107. 18^107 = 3870 mod 349 = 215

108. 18^108 = 558 mod 349 = 31

109. 18^109 = 3762 mod 349 = 209

110. 18^110 = 4896 mod 349 = 272

111. 18^111 = 180 mod 349 = 10

112. 18^112 = 3240 mod 349 = 180

113. 18^113 = 1782 mod 349 = 99

114. 18^114 = 666 mod 349 = 37

115. 18^115 = 5706 mod 349 = 317

116. 18^116 = 2196 mod 349 = 122

117. 18^117 = 1836 mod 349 = 102

118. 18^118 = 1638 mod 349 = 91

119. 18^119 = 4356 mod 349 = 242

120. 18^120 = 3024 mod 349 = 168

121. 18^121 = 4176 mod 349 = 232

122. 18^122 = 6066 mod 349 = 337

123. 18^123 = 2394 mod 349 = 133

124. 18^124 = 5400 mod 349 = 300

125. 18^125 = 2970 mod 349 = 165

126. 18^126 = 3204 mod 349 = 178

127. 18^127 = 1134 mod 349 = 63

128. 18^128 = 1566 mod 349 = 87

129. 18^129 = 3060 mod 349 = 170

130. 18^130 = 4824 mod 349 = 268

131. 18^131 = 5166 mod 349 = 287

132. 18^132 = 5040 mod 349 = 280

133. 18^133 = 2772 mod 349 = 154

134. 18^134 = 5922 mod 349 = 329

135. 18^135 = 6084 mod 349 = 338

136. 18^136 = 2718 mod 349 = 151

137. 18^137 = 4950 mod 349 = 275

138. 18^138 = 1152 mod 349 = 64

139. 18^139 = 1890 mod 349 = 105

140. 18^140 = 2610 mod 349 = 145

141. 18^141 = 3006 mod 349 = 167

142. 18^142 = 3852 mod 349 = 214

143. 18^143 = 234 mod 349 = 13

144. 18^144 = 4212 mod 349 = 234

145. 18^145 = 432 mod 349 = 24

146. 18^146 = 1494 mod 349 = 83

147. 18^147 = 1764 mod 349 = 98

148. 18^148 = 342 mod 349 = 19

149. 18^149 = 6156 mod 349 = 342

150. 18^150 = 4014 mod 349 = 223

151. 18^151 = 3150 mod 349 = 175

152. 18^152 = 162 mod 349 = 9

153. 18^153 = 2916 mod 349 = 162

154. 18^154 = 2232 mod 349 = 124

155. 18^155 = 2484 mod 349 = 138

156. 18^156 = 738 mod 349 = 41

157. 18^157 = 720 mod 349 = 40

158. 18^158 = 396 mod 349 = 22

159. 18^159 = 846 mod 349 = 47

160. 18^160 = 2664 mod 349 = 148

161. 18^161 = 3978 mod 349 = 221

162. 18^162 = 2502 mod 349 = 139

163. 18^163 = 1062 mod 349 = 59

164. 18^164 = 270 mod 349 = 15

165. 18^165 = 4860 mod 349 = 270

166. 18^166 = 5814 mod 349 = 323

167. 18^167 = 4140 mod 349 = 230

168. 18^168 = 5418 mod 349 = 301

169. 18^169 = 3294 mod 349 = 183

170. 18^170 = 2754 mod 349 = 153

171. 18^171 = 5598 mod 349 = 311

172. 18^172 = 252 mod 349 = 14

173. 18^173 = 4536 mod 349 = 252

174. 18^174 = 6264 mod 349 = 348

175. 18^175 = 5958 mod 349 = 331

176. 18^176 = 450 mod 349 = 25

177. 18^177 = 1818 mod 349 = 101

178. 18^178 = 1314 mod 349 = 73

179. 18^179 = 4806 mod 349 = 267

180. 18^180 = 4842 mod 349 = 269

181. 18^181 = 5490 mod 349 = 305

182. 18^182 = 4590 mod 349 = 255

183. 18^183 = 954 mod 349 = 53

184. 18^184 = 4608 mod 349 = 256

185. 18^185 = 1278 mod 349 = 71

186. 18^186 = 4158 mod 349 = 231

187. 18^187 = 5742 mod 349 = 319

188. 18^188 = 2844 mod 349 = 158

189. 18^189 = 936 mod 349 = 52

190. 18^190 = 4284 mod 349 = 238

191. 18^191 = 1728 mod 349 = 96

192. 18^192 = 5976 mod 349 = 332

193. 18^193 = 774 mod 349 = 43

194. 18^194 = 1368 mod 349 = 76

195. 18^195 = 5778 mod 349 = 321

196. 18^196 = 3492 mod 349 = 194

197. 18^197 = 36 mod 349 = 2

198. 18^198 = 648 mod 349 = 36

199. 18^199 = 5382 mod 349 = 299

200. 18^200 = 2646 mod 349 = 147

201. 18^201 = 3654 mod 349 = 203

202. 18^202 = 2952 mod 349 = 164

203. 18^203 = 2880 mod 349 = 160

204. 18^204 = 1584 mod 349 = 88

205. 18^205 = 3384 mod 349 = 188

206. 18^206 = 4374 mod 349 = 243

207. 18^207 = 3348 mod 349 = 186

208. 18^208 = 3726 mod 349 = 207

209. 18^209 = 4248 mod 349 = 236

210. 18^210 = 1080 mod 349 = 60

211. 18^211 = 594 mod 349 = 33

212. 18^212 = 4410 mod 349 = 245

213. 18^213 = 3996 mod 349 = 222

214. 18^214 = 2826 mod 349 = 157

215. 18^215 = 612 mod 349 = 34

216. 18^216 = 4734 mod 349 = 263

217. 18^217 = 3546 mod 349 = 197

218. 18^218 = 1008 mod 349 = 56

219. 18^219 = 5580 mod 349 = 310

220. 18^220 = 6210 mod 349 = 345

221. 18^221 = 4986 mod 349 = 277

222. 18^222 = 1800 mod 349 = 100

223. 18^223 = 990 mod 349 = 55

224. 18^224 = 5256 mod 349 = 292

225. 18^225 = 378 mod 349 = 21

226. 18^226 = 522 mod 349 = 29

227. 18^227 = 3114 mod 349 = 173

228. 18^228 = 5796 mod 349 = 322

229. 18^229 = 3816 mod 349 = 212

230. 18^230 = 5868 mod 349 = 326

231. 18^231 = 5112 mod 349 = 284

232. 18^232 = 4068 mod 349 = 226

233. 18^233 = 4122 mod 349 = 229

234. 18^234 = 5094 mod 349 = 283

235. 18^235 = 3744 mod 349 = 208

236. 18^236 = 4572 mod 349 = 254

237. 18^237 = 630 mod 349 = 35

238. 18^238 = 5058 mod 349 = 281

239. 18^239 = 3096 mod 349 = 172

240. 18^240 = 5472 mod 349 = 304

241. 18^241 = 4266 mod 349 = 237

242. 18^242 = 1404 mod 349 = 78

243. 18^243 = 144 mod 349 = 8

244. 18^244 = 2592 mod 349 = 144

245. 18^245 = 2682 mod 349 = 149

246. 18^246 = 4302 mod 349 = 239

247. 18^247 = 2052 mod 349 = 114

248. 18^248 = 5526 mod 349 = 307

249. 18^249 = 5238 mod 349 = 291

250. 18^250 = 54 mod 349 = 3

251. 18^251 = 972 mod 349 = 54

252. 18^252 = 4932 mod 349 = 274

253. 18^253 = 828 mod 349 = 46

254. 18^254 = 2340 mod 349 = 130

255. 18^255 = 4428 mod 349 = 246

256. 18^256 = 4320 mod 349 = 240

257. 18^257 = 2376 mod 349 = 132

258. 18^258 = 5076 mod 349 = 282

259. 18^259 = 3420 mod 349 = 190

260. 18^260 = 5022 mod 349 = 279

261. 18^261 = 2448 mod 349 = 136

262. 18^262 = 90 mod 349 = 5

263. 18^263 = 1620 mod 349 = 90

264. 18^264 = 4032 mod 349 = 224

265. 18^265 = 3474 mod 349 = 193

266. 18^266 = 5994 mod 349 = 333

267. 18^267 = 1098 mod 349 = 61

268. 18^268 = 918 mod 349 = 51

269. 18^269 = 3960 mod 349 = 220

270. 18^270 = 2178 mod 349 = 121

271. 18^271 = 1512 mod 349 = 84

272. 18^272 = 2088 mod 349 = 116

273. 18^273 = 6174 mod 349 = 343

274. 18^274 = 4338 mod 349 = 241

275. 18^275 = 2700 mod 349 = 150

276. 18^276 = 4626 mod 349 = 257

277. 18^277 = 1602 mod 349 = 89

278. 18^278 = 3708 mod 349 = 206

279. 18^279 = 3924 mod 349 = 218

280. 18^280 = 1530 mod 349 = 85

281. 18^281 = 2412 mod 349 = 134

282. 18^282 = 5724 mod 349 = 318

283. 18^283 = 2520 mod 349 = 140

284. 18^284 = 1386 mod 349 = 77

285. 18^285 = 6102 mod 349 = 339

286. 18^286 = 3042 mod 349 = 169

287. 18^287 = 4500 mod 349 = 250

288. 18^288 = 5616 mod 349 = 312

289. 18^289 = 576 mod 349 = 32

290. 18^290 = 4086 mod 349 = 227

291. 18^291 = 4446 mod 349 = 247

292. 18^292 = 4644 mod 349 = 258

293. 18^293 = 1926 mod 349 = 107

294. 18^294 = 3258 mod 349 = 181

295. 18^295 = 2106 mod 349 = 117

296. 18^296 = 216 mod 349 = 12

297. 18^297 = 3888 mod 349 = 216

298. 18^298 = 882 mod 349 = 49

299. 18^299 = 3312 mod 349 = 184

300. 18^300 = 3078 mod 349 = 171

301. 18^301 = 5148 mod 349 = 286

302. 18^302 = 4716 mod 349 = 262

303. 18^303 = 3222 mod 349 = 179

304. 18^304 = 1458 mod 349 = 81

305. 18^305 = 1116 mod 349 = 62

306. 18^306 = 1242 mod 349 = 69

307. 18^307 = 3510 mod 349 = 195

308. 18^308 = 360 mod 349 = 20

309. 18^309 = 198 mod 349 = 11

310. 18^310 = 3564 mod 349 = 198

311. 18^311 = 1332 mod 349 = 74

312. 18^312 = 5130 mod 349 = 285

313. 18^313 = 4392 mod 349 = 244

314. 18^314 = 3672 mod 349 = 204

315. 18^315 = 3276 mod 349 = 182

316. 18^316 = 2430 mod 349 = 135

317. 18^317 = 6048 mod 349 = 336

318. 18^318 = 2070 mod 349 = 115

319. 18^319 = 5850 mod 349 = 325

320. 18^320 = 4788 mod 349 = 266

321. 18^321 = 4518 mod 349 = 251

322. 18^322 = 5940 mod 349 = 330

323. 18^323 = 126 mod 349 = 7

324. 18^324 = 2268 mod 349 = 126

325. 18^325 = 3132 mod 349 = 174

326. 18^326 = 6120 mod 349 = 340

327. 18^327 = 3366 mod 349 = 187

328. 18^328 = 4050 mod 349 = 225

329. 18^329 = 3798 mod 349 = 211

330. 18^330 = 5544 mod 349 = 308

331. 18^331 = 5562 mod 349 = 309

332. 18^332 = 5886 mod 349 = 327

333. 18^333 = 5436 mod 349 = 302

334. 18^334 = 3618 mod 349 = 201

335. 18^335 = 2304 mod 349 = 128

336. 18^336 = 3780 mod 349 = 210

337. 18^337 = 5220 mod 349 = 290

338. 18^338 = 6012 mod 349 = 334

339. 18^339 = 1422 mod 349 = 79

340. 18^340 = 468 mod 349 = 26

341. 18^341 = 2142 mod 349 = 119

342. 18^342 = 864 mod 349 = 48

343. 18^343 = 2988 mod 349 = 166

344. 18^344 = 3528 mod 349 = 196

345. 18^345 = 684 mod 349 = 38

346. 18^346 = 6030 mod 349 = 335

347. 18^347 = 1746 mod 349 = 97

348. 18^348 = 18 mod 349 = 1

349. 18^349 = 324 mod 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

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 ord(18^k) = 29 (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

-----------------------------------

k = 6

18^k = 18^6 = 313

gcd(k, 348) = 6

ord(18^k) = ord(18^6) = 58

-----------------------------------

k = 7

18^k = 18^7 = 301

gcd(k, 348) = 1

ord(18^k) = ord(18^7) = 348

-----------------------------------

k = 8

18^k = 18^8 = 171

gcd(k, 348) = 4

ord(18^k) = ord(18^8) = 87

-----------------------------------

k = 9

18^k = 18^9 = 224

gcd(k, 348) = 3

ord(18^k) = 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)

===================================

נחשב את *, , .*

*נבדוק איזה ערך ייתן את*

*לכן,*

*לסיכום, , , .*

נחשב את *.*

We are solving the discrete log problem with shanks algorithm.

The order of the group is 348 and m = ceil(sqrt(348)) = 19

Now we are looking for 0<=i,j<=19 such that:

18^(i+19\*j) 202 mod 349 <=> 18^i = 202X(18^((-19)^j) mod 349

Let's calculate the values of 18^i mod 349 for 0<=i<=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<=j<=19 antil we find a match in the i values:

-------------------

j = 0:

202 X 18^((-19)^0) mod 349 = 202

202 is not in the i values

-------------------

j = 1:

202 X 18^((-19)^1) mod 349 = 44

===================

We found a match in the i values: 44 = 18^7 mod 349

202X(18^((-19)^1) = 18^7 mod 349

<=> 202 = 18^7+19\*1 = 18^26 mod 349

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

===================

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) mod p = (111^1229) mod 2003 = 1059

And then sends K\_1 to Bob.

4. Bob calculates K\_2 = (K\_1^b) mod p = (1059^795) mod 2003 = 1700

And then sends K\_2 to Alice.

5. Alice calculates K\_3 = (K\_2^(-a)) mod p = (1700^(-1229)) mod 2003 = 1059

And then sends K\_3 to Bob.

6. Bob calculates K\_4 = (K\_3^(-b)) mod p = (1059^(-795)) mod 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

============================================

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

ההתקפה:

אליס שולחת לבוב את .

מלורי שנמצאת באמצע בוחרת הופכי, ומוסיפה ללא ידיעת אליס ובוב *את ושולחת את לבוב, ללא ידיעת אליס ובוב.*

*בוב מחשב את למרות שהוא ואליס חושבים שהוא מחשב את: .*

*לאחר מכן אליס מחשבת את: .*

*ובוב מחשב את: .*

*כעת לבוב יש את: .*

*מלורי מחשבת כעת את: .*

*ולסיכום: לבוב יש את בסוף האלגוריתם את: .*

*ולמלורי יש בסוף האלגוריתם את: .*

בהצפנת אל גמאל בוחרים אקראי.

הצפנה של הודעה היא .

בשתי ההודעות המוצפנות של בוב יש את אותו רכיב ראשון, לכן אנו יודעים כי בוב השתמש באותו רכיב עבור שתי ההודעות.

נסמן ב- את שתי ההודעות לפי הנתון, .

לכן,

*לפי הנתון:*

*ולכן,*

*לסיכום: הפענוח של ההודעה השנייה היא –*