**מבוא להצפנה – תרגיל 3**

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

a = 2

b0 = 2^11799 = 1014 mod 47197

b1 = 1014^2 = 37059 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 2

/////////////////////////////////

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

a = 3

b0 = 3^11799 = 1 mod 47197

47197 is a Strong pseudoprime to base 3

/////////////////////////////////

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

a = 4

b0 = 4^11799 = 37059 mod 47197

b1 = 37059^2 = 31175 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 4

/////////////////////////////////

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

a = 5

b0 = 5^11799 = 40004 mod 47197

b1 = 40004^2 = 11337 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 5

/////////////////////////////////

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

a = 6

b0 = 6^11799 = 1014 mod 47197

b1 = 1014^2 = 37059 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 6

/////////////////////////////////

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

a = 7

b0 = 7^11799 = 34445 mod 47197

b1 = 34445^2 = 19839 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 7

/////////////////////////////////

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

a = 8

b0 = 8^11799 = 9014 mod 47197

b1 = 9014^2 = 26159 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 8

/////////////////////////////////

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

a = 9

b0 = 9^11799 = 1 mod 47197

47197 is a Strong pseudoprime to base 9

/////////////////////////////////

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

a = 10

b0 = 10^11799 = 21833 mod 47197

b1 = 21833^2 = 37386 mod 47197

47197 is not a pseudoprime or a Strong pseudoprime to base 10

/////////////////////////////////

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

a = 2

n = 47197, k = 2, r = 11799

b0 = 2^11799 = 1014 mod 47197

b1 = 1014^2 = 37059 mod 47197

/////////////////////////////////

47197 is composite

gcd(47197, 37059) = 1

/////////////////////////////////

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

a = 3

n = 47197, k = 2, r = 11799

b0 = 3^11799 = 1 mod 47197

/////////////////////////////////

47197 is probably prime

/////////////////////////////////

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

a = 4

n = 47197, k = 2, r = 11799

b0 = 4^11799 = 37059 mod 47197

b1 = 37059^2 = 31175 mod 47197

/////////////////////////////////

47197 is composite

gcd(47197, 31175) = 109

and we found that the composite is 47197 = 109 \* 433

/////////////////////////////////

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

x = 218

x^2 - 47197 = 327

sqrt(x^2 - 47197) = 18.083141320025124

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

x = 219

x^2 - 47197 = 764

sqrt(x^2 - 47197) = 27.640549922170507

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

x = 220

x^2 - 47197 = 1203

sqrt(x^2 - 47197) = 34.68429039204925

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

x = 221

x^2 - 47197 = 1644

sqrt(x^2 - 47197) = 40.54626986542659

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

x = 222

x^2 - 47197 = 2087

sqrt(x^2 - 47197) = 45.68369512200168

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

x = 223

x^2 - 47197 = 2532

sqrt(x^2 - 47197) = 50.3189825016365

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

x = 224

x^2 - 47197 = 2979

sqrt(x^2 - 47197) = 54.58021619598075

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

x = 225

x^2 - 47197 = 3428

sqrt(x^2 - 47197) = 58.54912467321779

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

x = 226

x^2 - 47197 = 3879

sqrt(x^2 - 47197) = 62.281618476080084

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

x = 227

x^2 - 47197 = 4332

sqrt(x^2 - 47197) = 65.81793068761733

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

x = 228

x^2 - 47197 = 4787

sqrt(x^2 - 47197) = 69.18814927427962

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

x = 229

x^2 - 47197 = 5244

sqrt(x^2 - 47197) = 72.41546796092669

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

x = 230

x^2 - 47197 = 5703

sqrt(x^2 - 47197) = 75.5182097245426

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

x = 231

x^2 - 47197 = 6164

sqrt(x^2 - 47197) = 78.51114570556209

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

x = 232

x^2 - 47197 = 6627

sqrt(x^2 - 47197) = 81.40638795573723

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

x = 233

x^2 - 47197 = 7092

sqrt(x^2 - 47197) = 84.2140130857092

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

x = 234

x^2 - 47197 = 7559

sqrt(x^2 - 47197) = 86.94250974063263

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

x = 235

x^2 - 47197 = 8028

sqrt(x^2 - 47197) = 89.59910713840847

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

x = 236

x^2 - 47197 = 8499

sqrt(x^2 - 47197) = 92.19002115196633

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

x = 237

x^2 - 47197 = 8972

sqrt(x^2 - 47197) = 94.72064188971694

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

x = 238

x^2 - 47197 = 9447

sqrt(x^2 - 47197) = 97.19567891629751

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

x = 239

x^2 - 47197 = 9924

sqrt(x^2 - 47197) = 99.61927524329818

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

x = 240

x^2 - 47197 = 10403

sqrt(x^2 - 47197) = 101.99509792141973

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

x = 241

x^2 - 47197 = 10884

sqrt(x^2 - 47197) = 104.32641084595981

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

x = 242

x^2 - 47197 = 11367

sqrt(x^2 - 47197) = 106.61613386350116

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

x = 243

x^2 - 47197 = 11852

sqrt(x^2 - 47197) = 108.86689120205463

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

x = 244

x^2 - 47197 = 12339

sqrt(x^2 - 47197) = 111.0810514894417

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

x = 245

x^2 - 47197 = 12828

sqrt(x^2 - 47197) = 113.26076107814215

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

x = 246

x^2 - 47197 = 13319

sqrt(x^2 - 47197) = 115.40797199500561

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

x = 247

x^2 - 47197 = 13812

sqrt(x^2 - 47197) = 117.52446553803169

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

x = 248

x^2 - 47197 = 14307

sqrt(x^2 - 47197) = 119.61187232043481

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

x = 249

x^2 - 47197 = 14804

sqrt(x^2 - 47197) = 121.67168939404104

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

x = 250

x^2 - 47197 = 15303

sqrt(x^2 - 47197) = 123.70529495538985

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

x = 251

x^2 - 47197 = 15804

sqrt(x^2 - 47197) = 125.71396103854178

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

x = 252

x^2 - 47197 = 16307

sqrt(x^2 - 47197) = 127.69886452118516

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

x = 253

x^2 - 47197 = 16812

sqrt(x^2 - 47197) = 129.66109670984585

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

x = 254

x^2 - 47197 = 17319

sqrt(x^2 - 47197) = 131.6016717219048

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

x = 255

x^2 - 47197 = 17828

sqrt(x^2 - 47197) = 133.52153384379613

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

x = 256

x^2 - 47197 = 18339

sqrt(x^2 - 47197) = 135.42156401400774

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

x = 257

x^2 - 47197 = 18852

sqrt(x^2 - 47197) = 137.30258555467918

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

x = 258

x^2 - 47197 = 19367

sqrt(x^2 - 47197) = 139.16536925542934

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

x = 259

x^2 - 47197 = 19884

sqrt(x^2 - 47197) = 141.01063789657857

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

x = 260

x^2 - 47197 = 20403

sqrt(x^2 - 47197) = 142.83907028540895

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

x = 261

x^2 - 47197 = 20924

sqrt(x^2 - 47197) = 144.65130486794789

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

x = 262

x^2 - 47197 = 21447

sqrt(x^2 - 47197) = 146.4479429695071

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

x = 263

x^2 - 47197 = 21972

sqrt(x^2 - 47197) = 148.22955170950223

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

x = 264

x^2 - 47197 = 22499

sqrt(x^2 - 47197) = 149.9966666296288

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

x = 265

x^2 - 47197 = 23028

sqrt(x^2 - 47197) = 151.74979406905302

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

x = 266

x^2 - 47197 = 23559

sqrt(x^2 - 47197) = 153.48941331570722

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

x = 267

x^2 - 47197 = 24092

sqrt(x^2 - 47197) = 155.21597855890997

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

x = 268

x^2 - 47197 = 24627

sqrt(x^2 - 47197) = 156.9299206652447

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

x = 269

x^2 - 47197 = 25164

sqrt(x^2 - 47197) = 158.63164879682742

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

x = 270

x^2 - 47197 = 25703

sqrt(x^2 - 47197) = 160.3215518886965

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

x = 271

x^2 - 47197 = 26244

sqrt(x^2 - 47197) = 162.0

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

The factors are: x-y and x+y, where x and y are the values from the table above, and n is the number to be factored.

x = 271, y = 162.0, n = 47197

109.0 X 433.0 = (271-162.0)(271+162.0) = 271^2 - 162.0^2 = 47197

ו- .

*שיטת של פולארד מבוססת על העובדה כי אם .*

*אז, אם אינו מחלק את , יש סיכויים טובים ש- .*

*אבל במקרה הזה, עבור ו- , הגורם הראשוני הגדול ביותר הוא 3.*

*ולכן, רק עבור נקבל ש- . ומכוון שגם ואז*

*ולא נצליח לפרק את .*

B = 2 | 2^2! mod15707 = 4         | gcd(2^2!-1 mod15707) = 1)

B = 3 | 2^3! mod15707 = 64        | gcd(2^3!-1 mod15707) = 1)

B = 4 | 2^4! mod15707 = 2140      | gcd(2^4!-1 mod15707) = 1)

B = 5 | 2^5! mod15707 = 14720     | gcd(2^5!-1 mod15707) = 1)

B = 6 | 2^6! mod15707 = 8524      | gcd(2^6!-1 mod15707) = 1)

B = 7 | 2^7! mod15707 = 15143     | gcd(2^7!-1 mod15707) = 113)

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

113 is a prime factor of 15707.

And 15707 = 113 X 139

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

נבחר:

*הפירוק:*

פונקציית ההצפנה היא:

נתון:

נציב:

נחשב:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*ולכן,*

נחשב את המפתח הפרטי על ידי האלגוריתם האוקלידי המורחב.

נתונים:

ראשית, נחשב את :

.

נחשב כעת את - :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

מצאנו בעזרת האלגוריתם האוקלידי המורחב כי:

*המפתח הפרטי הוא:*

נתונים:

נחשב את:

*ע"י הפענוח המהיר.*

*חישוב:*

*.*

*.*

*.*

*.*

*הפענוח הוא:*

נפרק את בעזרת שיטת האקספוננט האוניברסלי.

חישוב:

:

*.*

*הפירוק:*