**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

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