CRYPTOGRAPHY PROBLEM SET

Question 1: Compute $\phi(m)$ (Euler's Phi Function) for $m = 20, 2401, 8800, 7746289204980135457$.

Question 2: Compute $2^{2015} \pmod 7$ by hand, and $2^{2015} \pmod{103}$ using a calculator.

Question 3: Using successive squaring, compute $7^{7386} \pmod{7387}$.Why can't 7387 be prime?

Question 4: Solve the congruence $x^{113} \equiv 347 \pmod{463}$.

Question 5: Encrypt the following message: "Math is fun" using $m = 163276871, k = 79921$.

Question 6: Decode the following message, using the modulus $m = 7081$ and exponent $k = 1789$:

$$5192, 2604, 4222$$

Question 7: You intercept the following message, which you know has been encoded using the modulus and exponent

$$m = 95633199200784355265260442503137669036 7, k = 12398737$$

Break the code and decipher the message (where is the quote from?):

$$821566670681253393182493050080875560504,$$
$$870741731290463997209497869585113910 52,$$
$$552100909946781566365272088688468880029,$$
$$491078995197839451033115784866534122828,$$
$$172219665767314444215921020847762293421.$$

Just for fun: Read the following article: http://www.wsj.com/articles/SB124648494429082661 .

Bonus: Decrypt the text below without using an online decoder (so provide a thorough explanation about your method).

ctcrsurtkhlqynkqtboqoscmcojtkntbcrlwlqitkknnoqmoqrkjlgkqrsbkglqgyskhhojtkjtbojltuqoljitboicqo stckjkngctoqltuqolttbcrmlqtcsuglqtchobkwovoqctbcjfctwkugieo woggtkskjrcioqtbobcabiut- corljitbo qormkjrcecgctcorkntbohlfoqrkngctoqltuqorusbcrtbomqortcaokntbojkeoglwlqiljikntbcrmglsowboqo crtljit-blclhchmoggoijkt tkrpuolfgcfolaqltonugljilmkgkaotcshkuroeuttkqklqgcfol- gckjkutknmqciocjhymqknor-rckjljicjtboaqoltljiakkihoj wbkblvomqlstcsoicttbqkuabt- bolaorgctoqltuqowlrjktmqkhugaltoieylml-goljiohlrsugltoisqctcslgmqcortbkkircjacja tbocqgctljcorcjohmtysbuqsborjkqcrctlalhonkqtbosgkcrtoqoio-gosttbotcjbkqjhojicsljtrkngkwslgkqcoiormlcqgctoqltuqo crlrkgilrrmoosbctaqowkutknbuhljjooinkqctljict-blrjktsbljaoioxsomttkeoskhohkqojooioitbor girtboelqirtbowqctoqrlqoj ktromlqltoljioxsgurcvonqkhtbo eoacjjcja tbocqnujstckjrtbocqiutcortbocqqormkjrcecgctcor- blvoeoojiosqooieykuqrmoscor