Lab 2 Seguridad y Criptografía

Course code:	MC1003
Due:	**Friday**, July 15, 2022 at 23:59 (Central Standard Time)
Total points:	8 points

1. **Bad Randomness** *(2 points)*

   Similar to what you already saw in the first lab assignment, randomness is very important when generating a public/private key pair for RSA.

   (a) (1 point) Consider two public keys, $\mathsf{pk}_1 = (N_1, e = \texttt{0x10001})$ and $\mathsf{pk}_2 = (N_2, e = \texttt{0x10001})$, where N_1 and N_2 share a common prime number due to bad randomness.

   How can you now recover the private keys sk_1 and sk_2? Explain.

   (b) (1 point) Let

   $$N_1 = 31911268879726153592906144654237027376295605122244213622922186521905706566982029803162058645560935018590239228741916856548386908451480921197559002999923682112215351653191056500861642292092542289871863948919769102322109592410256330920289755738830113897223085997490143812504556443250361624670954182290699884363278896117260513728011714272216191623720025058574339391161134427455844173649966802001084085434015788604264018240837235540669979791159665641798142182641260977245871174011676056877150506997452523149677619595362184722427839973069792800511461097543016106605185768856201137690019195422872853821674569617291045348689$$

   and

   $$N_2 = 29749098234544950722553728915487736889032000866235439990224672856459603959762999494308747194494532325885995604229460732526748468701949483147742529416082853014150724439501812137763248341553329886209455926895906389466393931259187179345819618331695383131697541789713809171851909036255858913738517079097328136385803271665213396401797666719326659871515268852958442081564695126076615593690544933101179315724715313978155339567027899545964999201565586503260559560324485135168632732813082657924153077728565345736780910658086015188197891329991073146601336884478114205134885359752069712996903473839150213862565214367526184271213.$$

   Factor both numbers N_1 and N_2.

2. **More Bad RSA Keys** *(2 points)*

Another way that public/private key pair is badly generated is when the prime numbers p and q are too close to each other.

(a) (1 point) Consider a public keys using

$$N = p \cdot q$$
$$= 31401612687528177930215943148848809311518904648412623648220491560999134047133387404035404234173305721880604143039585486515317194864906548211258721186428317259772943399041454221743407594470620073977936497501994583009883533841277596103728165846101737491816806690067221463676885724449939022899923184989892421727241280596606832207507590947098792683744805374463880959093833448789884820082010758605737868798783718156918838115514573328254935242993005433365126264477751444026310666237744475957277386209631579355243316171072969461456495192594930326864442956512077580367920523056765040638774009742519469467742782525619657333117$$

where $p - q$ is very small.

Recover the private prime factors p and q of N.

Hint: Search online for Fermat's factorization method.

(b) (1 point) Extend Fermat's factorization method to factor

$$N = p \cdot q$$
$$= 61875236400720759128410941215016479453613282123198667331377016766603927665997397163220426786915195151825369038630953400078667423845632404763981470343566987098498301753730390857612122297550835849654828364670609996817002624295909462920344292561541752528241785063166635968063122355255895282785698082420903775939588824604266016368789475208111017418832511525901028776125518692455909759651215198842914354567118078839820318099544062552917457076588143545635889643240338175499881747347651885094368832196081331569182199150838190049066538477263421447352318440084507237101708052929374849609757243460785313196143175160485430252643$$

where $2p - q$ is very small.

Recover the private prime factors p and q of N.

3. **Wiener's Attack** *(4 points)*

Read §15.4.3 from "Cryptography Made Simple" or read the paper "The Wiener Attack on RSA Revisited: A Quest for the Exact Bound" by Susilo, Tonien, and Yang.

Recover the private exponent d from the public key

$$\mathsf{pk} = (N, e)$$

$$= (3157225366894622336834015710072198776674621846373682478350563513192105388039874132064487542132950421793341642233691841626340853895217798650899417559118276895020714733618843245512466751420186737690922778813494132355590249504923360128769645681638545590772503288656205145432246866821462561231710999307862052963977461651844367780439140889164190317553684768603021163252366078203721344708847913126956520428232466351742170604840291065109974497405678672781299119217697705073947140336942161716000377228904826780902246991592456938594256902217877422583416557105365720012940105276412002087731398340900493257163000465667849155403 3,$$

$$708421519444359916033961432113892898321436226966440050799025869198623456734737953280970023225680571566989943512545558976639560041353350357382298910282387882654003631784824549183476346069329941201161921082731158750031165762143989314781558284481474865094218644978706115082775395822531937816416908572452195044551681639244339283594605736217573353855619241199450585859261266280571171444914589954416635466046579456757046856303481916610910579819493641654914986441221870901786452681012286215585782660157430265944226066664306611422137485210442842550313537398556949983825138180255904773581683859622065345492125790029659070008 9).$$