Criptografie - Exerciţii

1. Varianta de RSA în care cele două numere prime p şi q sunt alese de aproximativ aceeaşi dimensiune poartă numele de RSA balansat şi este varianta recomandată şi utilizată în practică. Shamir a propus utilizarea unei variante de RSA numită RSA nebalansat care are rezistenţă mult mai mare decât RSA balansat împotriva factorizării şi are aceeaşi viteză de criptare/decriptare (sau invers spus, la acelaşi nivel de securitate cu RSA balansat permite o decriptare mult mai rapidă). RSA nebalansat presupune utilizarea unui număr prim p relativ mic (câteva sute de biţi) şi a unui număr prim q relativ mare (câteva mii de biţi) urmând ca criptarea să se facă pentru mesaje mai mici decât p iar decriptarea se va face modulo p (evident doar de către posesorului cheii private care îl cunoaste pe p). Pentru a facilita criptarea corectă se face publică o limită l de care mesajele nu au voie să treacă (publicarea acestei valori nu face schema nesigură deoarece ea se alege suficient de departe de valoare lui p, de ex. poate fi fixată la 256 biţi în timp ce p are 512 biţi, etc.). De exemplu:

Generare cheie:

$$p = 541, q = 104729, e = 7, l = 200$$
$$\Rightarrow n = 56658389, \phi(n) = (p-1)(q-1) = 56553120,$$
$$d = e^{-1} \bmod (p-1) = 463$$

Criptare:

$$m = 300 \Rightarrow c = 300^7 \bmod 56658389 = 18157376$$

Decriptare:

$$m = 18157376^{463} \bmod 541 = 300$$

Explicati si exemplificati pentru cheia publica si privata de mai sus cum in urma unui atac de tip CCA2 (Chosen Ciphertext Attack) un adversar ar putea sa factorizeze modulul.

2. Un distribuitor de cheie RSA de încredere decide că pentru a economisi timp de calcul este preferabil să folosească acelaşi modul pentru mai mulţi utilizatori şi să schimbe în certificatul acestora doar valoarea exponenţilor. De exemplu fie următoarele două perechi de chei:

$$K_1 : \{n = 837210799, e = 7, d = 478341751\}$$
$$K_2 : \{n = 837210799, e = 13, d = 579529429\}$$

Explicaţi de ce această decizie nu este corectă şi exemplificaţi cum plecând de la una din cheile de mai sus puteţi afla exponentul privat d al cheii de mai jos:

$$K_3 : \{n = 837210799, e = 17, d = ?\}$$

3. Demostraţi echivalenţa între decriptarea de la criptosistemul Rabin si problema factorizării întregilor.

4. Un tânăr cripograf doreşte să cripteze o cheie secretă pentru ca ea să poată fi alfată doar cândva în viitor când cineva reuşeşte să spargă nişte module RSA. Pentru aceasta el se gândeşte să folosească două module RSA de pe site-ul RSA oferite ca challenge http://www.rsasecurity.com/rsalabs/node.asp?id=2093 despre acestea ştiindu-se că au factorizarea necunoscută dar comunitatea ştiinţifică va lucra să le spargă (compania RSA oferea în trecut chiar şi sume de bani pentru spargerea modulelor de mai jos). Tânărul criptograf alege modulele de 1536 şi respectiv 2048 de biti.

n1=
1847699703211741474306835620200164403018549338663410171471785774910651696711161249859337684305435744585616061544571794052229717732524660960646946071249623720442022269756756687378427562389508764678440933285157496578843415088475528298186726451339863364931908084671990431874381283363502795470282653297802934916155811881049844908319545009848393775227257052578591944993870073695755688436933812779613089230392569695253261620823676490316036551371447913932347169566988069

n2=
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

După ce a selectat modulele el se gândeşte să cripteze mesajul său secret calculând $c_1 = m^2 \bmod n_1$ şi $c_2 = m^2 \bmod n_2$ (acest sistem se numeşte criptosistem Rabin şi este corect şi sigur atunci când este folosit corect). Unde a greşit tânărul criptograf? Se poate afla valoarea mesajului său dacă rezultatele criptărilor sunt următoarele?

c1=
1720824975522517857539467309146518060382842270514896093391979291030656292239729144665403513685944626690514052214759764494443164349805757586202347941324566382604120964935386258122499988803617571634095970180011900017447474052409657500820140866171389821089899978493473235156488326073675749875367732149010528924410410906444433597348845088236450378514333879924861416351842847760894046996788495712068878608786899270756395075310915351872142911403786029148987183447449947

c2=
4561642280956381246774642331705575104523442518306294887033201504008906454855887855514597265790895675977553974797919773779776892655441870273897525131894871022585204433581044093255080732213955457653190810418341335\
5699127548110113873635190699932165850542152382657518899992710162713201334532551245793969597202669219115740003607047862007490749311954754246585281919237018449235669417865766985783275606492993022302403623307723420\
2072322881876285807865893832282346294300028016342171410187938861009812975635715641457865781951720724292241356964611155195796118428665614605770428732914664423921593531374184814778240252956844983980

5. Într-unul din exerciţiile anterioare am arătat că, având un modul RSA $n = p \cdot q$, dacă se cunoşte suma factorilor săi $S = p + q$ putem factoriza modulul şi deci sparge criptosistemul RSA. Următorul fapt matematic este considerat un paradox: dacă avem un modul $n = p \cdot q$ putem calcula pentru $\forall x$ valoarea lui $x^{p+q} \bmod n$ cu toate ca nu ştim cât este $S = p + q$. Se cere pentru $n = 323$ şi $x = 2$ calculaţi valoarea lui $x^{p+q} \bmod n$ fără a folosi factorizarea lui . Justificaţi matematic generalitatea calculului efectuat.

6. Factorizaţi numărul $n = 279841$. Care este numărul maxim de paşi în care poate fi factorizat un întreg de formă similară. Propuneţi o transformare matematică elementară care aplicată numărului l-ar face să numai poată fi factorizat.

7. Pentru verificarea a k semnături RSA, pentru a economisi timp de calcul, a fost propus ca verificarea să aibă loc prin testarea egalităţii $\left(\prod_{i=1}^{k} s_i \right)^e = \prod_{i=1}^{k} h(m_i)$. Această metodă este considerată nesigură din mai multe puncte de vedere, unul dintre ele este acela că un utilizator poate primi un set de semnături $\{s_0, s_1, ..., s_k\}$ care cu toate că verifică egalitatea de mai sus, nu sunt semnăturile corecte pentru mesajele $\{m_0, m_1, ..., m_k\}$. Explicaţi cum este posibil acest lucru folosind un exemplu numeric.

8. Având cele trei probleme computaţionale RSA-Cheie, Euler-Phi şi Factorizarea întregilor, exemplificaţi folosind un exemplu numeric dacă ele sunt sau nu echivalente.

9. Un tânăr fără experienţă în criptografie trăieşte cu spaima că AES ar putea fi spart şi vrea să îi recomandaţi câteva sugestii pentru a construi un criptosistem simetric mai sigur. Explicaţi în maxim 5 rânduri care este recomandarea dumneavoastră.