3.
U RSA kriptosustavu s javnim kljucem (n;e), gdje je n = 86267 = 281 * 307
i e = 65537 = 2^16+1, sifrirajte otvoreni tekst x =1245.
Odredite pripadni tajni kljuc d.

---
y=?
d=?

phi(n)=(p-1)*(q-1)
d*e = 1 (mod phi(n))

Provede se Euklidov algoritam i dobije d.

y = x^e (mod n)

e se zapise u binarnom zapisu, te se zatim provede metoda "kvadriraj i mnozi" i dobije y

---

4.
Otvoreni je tekst na hrvatskom jeziku sifriran pomocu RSA kriptosustava, ciji je javni kljuc (n;e)= (30967, 17). Najprije su slovima pridruzene odgovarajuce brojevne vrijednosti: A=0, B=1, C=2, Č=3, ..., Z=28, Ž=29. Potom su tri po tri susjedna slova otvorenog teksta "kodirana" kao elementi od Zn, kao sto pokazuju ovi primjeri:
DAN =5*30^2 + 0*30 + 18 = 4518,
PUT =21*302 + 26*30 + 25 = 19705.
Konacno su ovako dobiveni elementi od Zn sifrirani pomocu RSA kriptosustava s gore navedenim parametrima n i e.
Faktorizirajte broj n (poznato je da je produkt dvaju "bliskih" prostih brojeva), te desifrirajte sifrat:
y1 = 23144, y2 = 14420, y3 = 19603, y4 = 27580.

---

p = ? q = ?
x1, x2, x3, x4 = ?
---

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
a b c č ć d dž đ e f g h i j k
15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
l lj m n nj o p r s š t u v z ž

```
p = floor(sqrt(n))
while (n/p != cijeli broj) {
        p = p – 1
}
q = n / p
```

phi(n)=(p-1)*(q-1)
d*e = 1 (mod phi(n))

Provede se Euklidov algoritam i dobije d.

x = y^d (mod n)

d se zapise u binarnom zapisu, te se zatim provede metoda "kvadriraj i mnozi" i dobije x.

Dobiveni x se podijeli s 30^2=900 te je kvocijent prvi znak. -> a1
Od dobivenog broja se oduzme taj kvocijent pa pomnozi s 30. kvocijent-> a2
Od dobivenog broja se oduzme taj kvocijent pa pomnozi s 30. Preostali broj -> a3

5.
Alice je poslala istu poruku m nekolicini agenata. Eva je presrela sifrate c1, c2, c3 za trojicu agenata ciji su javni kljucevi n1, n2 i n3. Poznato je da Alice i agenti koriste RSA kriptosustav s javnim eksponentom e = 3. Za zadane
n1 =407, c1 =356;
n2 =533, c2 =281;
n3 =551, c3 =468:
pokazite kako ce Eva otkriti poruku m (bez poznavanja faktorizacije modula n1, n2, n3).

---

m = ?

Tri jednadzbe oblika:
x = ci (mod ni)

Rjesi se taj sustav kongruencija CRT-om i dobije se:

x = c (mod n1*n2*n3)

m = x^(1/e) = x^(1/3)
m mora biti cijeli broj, inače se dogodila greška.

6.
Neka je (n;e)=(7478291; 4395713) Bobov javni RSA kljuc. Poznato je da tajni eksponent d zadovoljava nejednakost d< (1/3)*(n^(1/4)). Odredite d (Bobov tajni RSA kljuc).

---

d = ?

---

e/n se zapise u obliku veriznog razlomka (nije potrebno do kraja provesti Euklidov algoritam jer postoji nejednakost d< (1/3)*(n^(1/4)))

k/d je konvergenta veriznog razlomka e/n.

Imamo (n,e) = (7478291,4395713)
Znamo da je d <1/4 četvrti korijen od 7478291
--> d < 17.4
Postupak krece ovako:
Moramo razviti e/n u verižni razlomak (Napomena: ne treba se raditi do kraja)
7478291 = 4395713 * **1** + 3082578
4395713 = 3082578 * **1** + 1313135
3082578 = 1313135 * **2** + 456308
1313135 = 456308 * **2** + 400519
456308 = 55789 * 7 + 9996
e/n = [0; 1,1,2,2,7,...] (prva je 0 jer je e < n)
Ovo nam je dosta, pokazat ce nam tablica kasnije.
Sad racunamo konvergente, konvergenta je oblika p/q (skripta, str. 44,47)

n	-1	0	1	2	3	4	5
a	_	0	1	1	2	2	1
p	1	0	1	1	3	7	10
q	0	1	1	2	5	12	17

Kad se dobije ovaj q = 17, znamo da dalje ne moramo jer nam uvjet tako kaže
konvergente su: 1/2, 3/5, 7/12, 10/17
To je ustvari oblik k/d prema str.91
I sad uvrštavamo jednu po jednu konvergentu. Ja cu pokazati za 10/17.
Znači k = 10, d = 17.
Imamo formulu
(p+q)/2 = (pq - (ed - 1)/k +1)/2
(p+q)/2 = 2790
Iz formule
((p+q)/2)^2-pq=((q-p)/2)^2 --> (q-p)/2 = 553
Iz cega mozemo dobiti p=2237, q=3343 i provjeriti da li je pq=n.

7.
U Rabinovom kriptosustavu s parametrima (n;p;q) = (3713; 47; 79), desifrirajte sifrat y = 1512. Poznato je da je otvoreni tekst prirodan broj x<n kojem su zadnja cetiri bita u binarnom zapisu medusobno jednaka.

---

x = ?

Zadnjih n bita u binarnom zapisu su medusobno jednaka znaci da vrijedi:
x = 0 (mod 2^n) ili x = 2^n-1 (mod 2^n) = -1 (mod 2^n)

Ako je p = 3 (mod 4) (a najcesce jest) onda se izracuna a
y^((p+1)/4) = y (mod p)

Identicno vrijedi i za q.

Dobije se 4 sustava kongruencija para jednadzbi.
x = +-a (mod p)
x = +-b (mod q)

u * p + v * q = 1
Euklidovim algoritmom se dobiju u i v pa se uvrstavaju u ovu jednadzbu mijenjajuci predznak a-u i b-u.

x = u*p*b + v*q*a (mod p*q)

8.
Neka je u Diffe – Hellmanovom protokolu G = Z*p, p =87671, te g = 2, a =1234, b = 4321. Odredite kljuc K = g^(a*b).

K = ?

Izracuna se a*b i zapise u binarnom zapisu te se provede algoritam "kvadriraj i mnozi".

9.
Neka je u ElGamalovom kriptosustavu p =1777, alfa =6, a =1009.
a) Sifrirajte otvoreni tekst x =1483, uz pretpostavku da je jednokratni kljuc k =701.
b) Desifrirajte sifrat(1664; 1031).

---

a) y = ?
b) x = ?

---

a)
beta = alfa^a (mod p)

y = eˇK = (alfa^k mod p, x*beta^k mod p)

b)
(y1, y2)

x = dˇK (y1, y2) = y2 * (y1^a)^-1 (mod p)

10.
Zadan je Merkle-Hellmanov kriptosustav s parametrima
v =(2; 5; 13; 27; 55; 119; 223); p =449; a =307;
t =(165; 188; 399; 207; 272; 164; 213).

Desifrirajte sifrat y =1021.

---

n = 7
(x1, x2, x3, x4, x5, x6, x7) = ?
Opcenito:
(x1, … xn) = ?
xi su 0 ili 1.

---

y = eˇK(x1,…,xn) = suma (i=1 do n) xi*ti

z = a^-1*y (mod p)

Od tog z-a se oduzimaju clanovi iz skupa v i za njih vrijedi 1 (tj. da se nalaze u tom skupu).