Kodutöö nr. 15

Joosep Näks ja Uku Hannes Arismaa

1. Uurida Fermat' testi abil, kas 41041, 41071 ja 41081 on alg- või kordarvud.

Lihtsad testid meile nende arvude kohta midagi ei ütle.
Märkame, et $7^{41040} \equiv 29316 \pmod{41041}$, seega 41041 pole algarv.
Märkame, et $7^{41070} \equiv 30659 \pmod{41071}$, seega 41071 pole algarv.
Samas $2^{41080} \equiv 1 \pmod{41081}$,$3^{41080} \equiv 1 \pmod{41081}$,$5^{41080} \equiv 1 \pmod{41081}$,$7^{41080} \equiv 1 \pmod{41081}$, seega on mõitlikult tõenäoline, et 41081 on algarv.

2. Kontrollida eelmise ülesande tulemust Milleri-Rabini testi abil.

Arvude 41041 ja 41071 kohta andis Fermat' test kindla tulemuse et need on kordarvud ehk neid pole vaja kontrollida. Vaatlen arvu $41081 = 5135 \cdot 2^3 + 1$:

n	2^{5135}	$2^{2\cdot 5135}$	$2^{4\cdot 5135}$
41081	1		

n	3^{5135}	$3^{2\cdot 5135}$	$3^{4\cdot 5135}$
41081	1707	38179	-1

n	5^{5135}	$5^{2\cdot 5135}$	$5^{4\cdot 5135}$
41081	1	-1	

Ehk tegu tõenäoliselt tõesti on algarvuga.

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(9379, 277)$, tuvastada digiallkirja õigsus tekstil 71765538043433415340, mille originaal on KAJA KALLAS.

Dekodeerimiseks jagame teksti plokkideks, saame 7176, 5538, 434, 3341, 5340. Tõestes need arvud antud mooduli järgi astmesse 277, saame arvud 1025, 1809, 18, 120, 119, millest saame tähed JYRI RATAS. Tundub, et digiallkiri on ebakorrektne.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi kaheksatäheliste (st. kuueteistnumbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(9727957916830399, 667)$ kodeeritud RSA sõnum

$$1861759116915468769243983439501990264093647399 25.$$

Tegurdades avalikus võtmes arv n, saab $n = 9727957916830399 = 97635481 \cdot 99635479$ ehk $\varphi(n) = (97635481 - 1) \cdot (99635479 - 1) = 9727957719559440$. Kuna salajane astendaja on avaliku astendaja pöördarv mooduli $\varphi(n)$ järgi, saan leida salajase astendaja: $d \equiv 667^{-1} \equiv 5863026991398643 \pmod{9727957719559440}$. Järgmiseks jagan krüpteeritud sõnumi blokkideks ja astendan need salajase astendajaga mooduli n järgi:

$$1861759116915468^{5863026991398643} \equiv 19\ 05\ 05\ 00\ 15\ 14\ 00\ 01 \pmod{9727957916830399}$$
$$7692439834395019^{5863026991398643} \equiv 12\ 12\ 05\ 19\ 00\ 11\ 09\ 18 \pmod{9727957916830399}$$
$$9026409364739925^{5863026991398643} \equiv 22\ 05\ 19\ 00\ 08\ 01\ 08\ 01 \pmod{9727957916830399}$$

Ehk sõnum on "see on alles kirves haha"

5. Te olete salakirjade saatmiseks kokku leppinud loengukonspekti näitega 9.8 sarnase, aga sümmeetrilise ning neljatäheliste blokkidega skeemi, kus arvutused $c = s^d \pmod n$ ja $s = c^e \pmod n$ on asendatud arvutustega $c = s - v \pmod n$ ja $s = c + v \pmod n$, seejuures $n = 98765678$. Salajase võtme v leiate Diffie-Hellmani võtmevahetuse abil, valides rühmaks $\mathbb{Z}_{96168173}$ ja algjuureks arvu 2. Te olete saanud ühissaladuse leidmiseks sõnumi 60848048 ja otsustate võtta oma astendajaks arvu 1794. Dekodeerida salasõnum

30513994214120121341310826402004175430 94.

Esmalt leiame jagatud saladuse. Selleks peame lihtsalt leidma, et $60848048^{1794} \equiv 90403685 \pmod{96168173}$.

Nüüd jagame Algse teksti 8 tähelisteks plokkideks (2 plokki arvutuse kohta) , saades 30513994, 21412012, 13413108, 26402004, 17543094, Liites nendele jagatud numbri ning tähtedesse teisendades saame sõnumi

VOTAME SEEKORD KIRKA

6. Kuidas murda RSA kodeeringut *ilma algteguriteks lahutamist kasutamata*, kui mooduli $n = pq$ jaoks on teada Euleri funktsiooni väärtus $\varphi(n)$ (aga arvud p ja q on ikkagi veel salajased)? Kasutage seda meetodit ülesande 4 salasõnumi dekodeerimiseks teades, et $\varphi(n) = 9727957719559440$.

Võrranditest $n = pq$ ja $\varphi(n) = (p-1)(q-1)$ saab avaldada $q^2+q(\varphi(n)-n-1)+n = 0$ ehk ruutvõrrandi lahendades saab $q = \dfrac{n+1-\varphi(n) \pm \sqrt{(\varphi(n)-n-1)^2-4n}}{2}$ ehk $q_1 = 97635481$ ja $q_2 = 99635479$. Ning kontrollides $97635481 \cdot 99635479 = 9727957916830399 = n$ ehk ma olen leidnud p ja q väärtused ning edasi saab sõnumi leida sama moodi nagu ülesandes 4.