I ÜLDMÕISTED, ETTEVALMISTUSTÖÖD

SAMAS-SALAKIRJA KASUTUSALA

1. SAMAS-salakiri oli algselt mõeldud kasutamiseks konspiratiivsetes tingimustes salasõnumite ning vajalike signaalide vahetamiseks organiseeritud vastupanuliikumise eri gruppide vahel ning rahvusvaheliste usalduslike sidemete pidamiseks, sealjuures ka kodu- ja pagulaskeskuste vahel.
2. SAMAS-salakiri võimaldab eluliselt tähtsaid salasõnumeid, nimesid, aadresse, telefoninumbreid ja kõikvõimalikke operatiivteateid peita avalikesse telefonikõnedesse, telegrammidesse ning tsenseeritavasse kirjavahetusse.
3. Totalitaarse võimu tingimustes ja kõige ekstreemsemates oludes võimaldab korralikult omandatud SAMAS-salakirja süsteem pidada salastatud sõnumivahetust ilma kaasaskantavate lisavahendite ja kooditabelite vajaduseta; ning teha vajalikke maskeeritud ülestähendusi vaid endale teadaoleval viisil.
4. Salakirja harrastajatele võimaldab SAMAS-salakiri põnevat mängu. Sellesse raamatusse koondatud SAMAS-salakirja variandid ei ammenda kaugeltki kogu süsteemi võimalusi ning nutikas salakirjahuviline saab rakendada oma jõudu ja fantaasiat SAMAS-süsteemi edasiarendamisel ning uute maskeerimisviiside leiutamisel. Et anda algteadmisi ja luua eeldusi uute salakirjaideede tekkeks on käesolevas õpikus mitmel matemaatika ja keeleteaduse lõigul peatutud põhjalikumalt, kui seda vajanuks "puust ette tehtud" salakirjavariantide maketid.
5. Salakirjaõpik sisaldab ohtrasti harjutusi ja ülesandeid, millega kinnistada metoodika omandamist ja teritada hambaid lihtsate-keerulisemate pähklite järamisel.

SAMAS-SALAKIRJA PÕHIIDEE (SAMAS = SA -salastamine + MAS-maskeerimine)
Salastatav sõnum salastatakse (õifreeritakse) – sõnumi tähed muudetakse vastavalt valitud variandile mingi arvsüsteemi arvudeks, mis siis järgnevalt maskeeritakse (peidetakse) originaalsel viisil kas tavalisse kirjavahetusse või visuaalsete nippidega joonistesse.

ESIMENE ÕPPETUND

- **Ekskursioon matemaatikasse: erinevad arvusüsteemid, opereerimine mitmekohaliste eri süsteemi arvudega**
- **Harjutused ja ülesanded**

SAMAS-salakirja põhiideeks on kümnendsüsteemist erinevate arvsüsteemide kasutamine sõnumi salastamisel (õifreerimisel). Seepärast pole liigne lähemalt tutvuda eri arvsüsteemidega ning õppida opereerima mitmekohaliste eri süsteemi arvudega

MEIE IGAPÄEVANE KÜMNENDSÜSTEEM

Kümnendarvusüsteem tekkis Hiinas 4. sajandil e.m.a. ja 5. sajandil Indias, kust ta 8. sajandil levis araabiamaadele. Hispaania kaudu jõudis kümnendsüsteem Euroopasse alles 16. saj. ja on tänapäeval kahtlemata levinuim arvusüsteem. 10ndsüsteemile tugineb ka enamik mõõtühikute süsteeme, mida me kasutame. Oleme selle süsteemiga niivõrd harjunud, et arvame temast teadvat kõike. Võib-olla seepärast ongi kergem tema põhjal teha mõningaid üldistusi enne teiste arvusüsteemide juurde asumist. Kümnendsüsteemi aluseks on arv 10, mis tähendab, et selles süsteemis kasutatakse kümmet erinevat numbrit. Need on: 0, 1, 2, 3, 4, 5, 6, 7, 8 ja 9. Paneme tähele ka asjaolu, et suurim number on siin 9, s.t. ühe võrra väiksem süsteemi alusest. Kümnendsüsteem on mitmekohaliste arvude, ehk nn. positsiooniline arvusüsteem, kus numbrite väärtus sõltub nende asukohast mitmekohalises arvus.

Näiteks viiekohalises arvus 27456 on 6 ühelist, 5 kümnelist, 4 sajalist, 7 tuhandelist ja 2 kümnetuhandelist. Teisi sõnu on see kümnendarv esitatav järgmise summana:

27456 = 20000 + 7000 + 400 + 50 + 6, ehk kasutades aluse 10 astmeid:

$= 2\cdot10^4 + 7\cdot10^3 + 4\cdot10^2 + 5\cdot10^1 + 6\cdot10^0$, ehk kuna $10^1=10$ ja $10^0=1$:

$= 2\cdot10^4 + 7\cdot10^3 + 4\cdot10^2 + 5\cdot10 + 6\cdot1$

Niipalju siis kümnendsüsteemist.

MILLISEID ARVUSÜSTEEME ME VEEL TEAME?

Kuuekümnendsüsteem (seksagesimaalsüsteem) on vanim teadaolev positsiooniline arvusüsteem, mida kasutati Babüloonias juba 4000 aastat tagasi. 60ndsüsteemi mõju võime leida tänapäevaste nurga- ja ajamõõtühikute juures: ühes tunnis on 60 minutit ja 60·60 sekundit, üks nurgakraad sisaldab samuti 60 minutit ja 3600 sekundit.

Nulli lugu

Babüloonlased on andnud meile ka arvu "null", millega nad 60ndsüsteemis hakkasid tähistama puuduvat järguühikut. Kreeklased olid aga arvatavasti esimesed, kes hakkasid millegi puudumist tähistama tähega "omikron" - 0. Tänapäevase tähistuse on nullile andnud kuulsad prantsuse matemaatikud A.Girard ja R.Descartes alles 17.saj.

Kuueteistkümnendsüsteem (seksadetsimaalsüsteem) on põhiliselt kasutamist leidnud arvutites. 16ndsüsteemi aluseks on arv 16, mis tähendab, et süsteemis kasutatakse 16 sõltumatut numbrit. Nendeks on võetud kümme 10ndsüsteemi numbrit 0, 1, 2, 3, 4, 5, 6, 7, 8 ja 9 ning lisatud kuus tähte: A, B, C, D, E ja F, mis vastavad 10ndsüsteemi arvudele 10, 11, 12, 13,14 ja 15.

Muuseas, kuna arvutites on põhikeeleks kahendsüsteem ja 16ndsüsteemi alus 16 kujutab endast arvu 2 neljandat astet: 2·2·2·2=16, siis väljendataksegi seal igat 16ndarvu neljakohaliste kahendarvudega.

10ndsüsteemist kõrgemate arvusüsteemide hulka võiks nimetada veel ka **kaheteistkümnendarvusüsteem** (duodetsimaalsüsteem). See kuulub osana iidse 60ndsüsteemi juurde. Positsioonilise arvusüsteemina praktiliselt ei kasutata, sest tal puuduvad numbrimärgid ja arvsõnad kõigi 12 numbri märkimiseks. 12ndsüsteemi kasutatakse siiski näiteks loendamisel (12 – tosin) ja mõningates mõõtühikute süsteemides.

KÜMNENDSÜSTEEMIST MADALAMAD ARVUSÜSTEEMID

Selliseid arvusüsteeme on kaheksa ja mitmedki neist on kasutatavad SAMAS-salakirja juures. Analoogiliselt eelpoolvaadeldud kümnendsüsteemiga on temast madalamate arvusüsteemide numbrid järgmised:
9ndsüsteemi numbrid on: 0, 1, 2, 3, 4, 5, 6, 7 ja 8 – kokku 9 ja suurim number – 8
8ndsüsteemi numbrid on: 0, 1, 2, 3, 4, 5, 6 ja 7– kokku 8 ja suurim number – 7
7ndsüsteemi numbrid on: 0, 1, 2, 3, 4, 5 ja 6 – kokku 7 ja suurim number – 6
6ndsüsteemi numbrid on: 0, 1, 2, 3, 4 ja 5 – kokku 6 ja suurim number – 5
5ndsüsteemi numbrid on: 0, 1, 2, 3 ja 4 – kokku 5 ja suurim number – 4
4ndsüsteemi numbrid on: 0, 1, 2 ja 3 – kokku 4 ja suurim number – 3
3ndsüsteemi numbrid on: 0, 1 ja 2 – kokku 3 ja suurim number – 2
2ndsüsteemi numbrid on: 0 ja 1 – kokku 2 ja suurim number – 1

Vaadeldud erinevatest arvusüsteemidest saab teha üldistuse, et igas arvsüsteemis (tähistusega K) on täpselt niimitu erinevat numbrimärki nagu näitab süsteemi alus K ja suurim number nendest on ühe võrra väiksem süsteemi alusarvust, seega K–1

Kas eksisteerib ka 1ndsüsteem?
Sellisel "süsteemil" oleks siis ainult üks number, mis aga ei võimalda koostada mitmekohalisi arve. Kõik numbrid oleksid ühese väärtusega, ükskõik millisel kohal nad ka sellises arvus oleks. Seepärast pole ühendsüsteemist kui süsteemist mõtet rääkida. Tema ühe märgiga ei saa moodustada süsteemseid arve ning üheliste märkide jada kujutaks endast paremal juhul mingit primitiivset loetelu.
Seega on kõige lihtsamaks arvusüsteemiks kahendsüsteem.

KUIDAS ESITATAKSE ARVE ERINEVATES ARVSÜSTEEMIDES?

Kümnendsüsteemi mitmekohaliste arvude juures õppisime neid välja kirjutama arv 10 astmete summana.
Analoogiliselt võib kujutada ka teiste arvsüsteemide mitmekohalisi arve, kusjuures mingi K-süsteemi arvu numbreid korrutatakse selle numbri positsioonist sõltuvalt vastava K astmega:
Näiteks viiekohaline K-süsteemi arv abcde näeb välja nii:
$abcde_k = a \cdot K^4 + b \cdot K^3 + c \cdot K^2 + d \cdot K + e$

KUIDAS PRAKTILISELT ÜLE MINNA ÜHELT ARVSÜSTEEMILT TEISELE?

TEISTE ARVSÜSTEEMIDE ARVUD → KÜMNENDSÜSTEEMI ARVUDEKS

Mistahes10ndsüsteemist erinevate arvude teisendamisel 10ndarvuks tuleb lähtuda viimatitoodud valemist. Olenevalt sellest, mitmekohaline arv on, leiame arvu süsteemi aluse K vastavad astmed ning arvutame summa, liites arvu moodustavate numbrite ja vastavate K astmete korrutised.

Need kohakoefitsendid ehk arvusüsteemi aluste astmed kuni 6-kohalistele arvudele on toodud järgmises tabelis 1.

Tabel 1

Arvu-süsteemi alus K	numbri positsioon mitmekohalises arvus ja vastav K aste					
	6	5	4	3	2	1
	K^5	K^4	K^3	K^2	K	$K^0=1$
K=9	59049	6561	729	81	9	1
K=8	32768	4096	512	64	8	1
K=7	16807	2401	343	49	7	1
K=6	7776	1296	216	36	6	1
K=5	3125	625	125	25	5	1
K=4	1024	256	64	16	4	1
K=3	243	81	27	9	3	1
K=2	32	16	8	4	2	1

Näited: Muudame mitmekohalised eri süsteemi arvud kümnendarvudeks

$\boxed{2} \rightarrow \boxed{10}$ $110010_2 = 1\cdot32 + 1\cdot16 + 0 + 0 + 1\cdot2 + 0 = 50_{10}$

$\boxed{3} \rightarrow \boxed{10}$ $2011_3 = 2\cdot27 + 0 + 1\cdot3 + 1 = 58_{10}$

$\boxed{4} \rightarrow \boxed{10}$ $2302_4 = 2\cdot64 + 3\cdot16 + 0 + 2 = 178_{10}$

$\boxed{6} \rightarrow \boxed{10}$ $2145_6 = 2\cdot216 + 1\cdot 36 + 4\cdot6 + 5 = 497_{10}$

$\boxed{8} \rightarrow \boxed{10}$ $126_8 = 1\cdot64 + 2\cdot8 + 6 = 86_{10}$

10-NDSÜSTEEMI ARVUD → TEISTESSE SÜSTEEMIDESSE

Mingi kümnendarvu teisendamisel mõnda teise arvusüsteemi talitame järgmiselt: Kõigepealt leiame ühelised jagades antud kümnendarvu soovitud süsteemi alusega K – jääk näitabki K-süsteemi arvu ühelisi. Seejärel võtame eelmise jagatise täisarvulise osa ja jägame uuesti K-ga – selle jagatise jääk annab teise koha numbri. Jne. Toimingut kordame seni kuni arv on jagatud. Kirjeldatud toimingut on kergem omandada järgmiste näidete varal.

Näited:

$\boxed{10} \rightarrow \boxed{3}$ Muudame kümnendarvu 77 kolmendarvuks.
Jagame 77:3 saame 25 ja jääk 2 annab meile ühelised. Võtame eelmise jägatise täisarvulise osa ja jagame uuesti 3-ga 25:3 saame 8 ja jääk 1 annab teise koha arvu. Jagades eelmise täisarvulise jägatise uuesti 3-ga saame 2 ja jääk 2 näitab kolmanda koha numbri. Kuna viimase jagatise täisosa enam 3-ga ei jagu, moodustab ta kolmendarvu neljanda koha. Seega: $77_{10} = 2212_3$
Tehet võiks sooritada järgmisel moel:

77 : 3 = 25 : 3 = 8 : 3 = **2**
6 24 6
17 **1** **2**
15
2

$\boxed{10} \rightarrow \boxed{4}$ Muudame 53 neljandarvuks. Peale jagamisi saame: $53_{10} = 311_4$

53 : 4 = 13 : 4 = **3**
4 12
13 **1**
12

1

10 → 2 Muudame 47 kahendarvuks. Jagamisega saame: $47_{10} = 101111_2$

47 : 2 = 23 : 2 = 11 : 2 = 5 : 2 = 2 : 2 = **1**

4	2	10	4	2
7	3	**1**	**1**	**0**
6	2			
1	**1**			

10 → 8 Muudame 33 kaheksandarvuks. Peale tehingut: $33_{10} = 41_8$

33 : 8 = **4**

32
1

KUIDAS ILMA VAHEARVUTUSTETA VäLJA KIRJUTADA ERINEVATE ARVUSÜSTEEMIDE MITMEKOHALISTE ARVUDE RIDA JA MITUT 10NDSÜSTEEMI KOHTA NAD KATAVAD?

Hiljem näeme vajadust salastamislükatile kanda mitmekohalisi eri süsteemi arve. Sel juhul võib otsekohe hakata arve välja kirjutama alustades 0-st. Eelnevast me teame, et mistahes arvusüsteemis K on suurim number ühe võrra väiksem (K-1) ja arvu väärtusel K muutub arvu järk, ühelised aga algavad uuesti 0-st. Näiteks 10ndsüsteemis peale 9-t muutub arv kahekohaliseks:10; 5ndsüsteemis peale 4 järgneb 10 jne.

Näiteks kahekohaliste kuuendarvude rida algab 00-st ja suurim number on 55 (järgmine arv oleks juba kolmekohaline: 100). Näeme ka, et see kahekohaliste kuuendarvude rida hõlmab 36 10ndsüsteemi kohta. Üldjuhul, kui meil on tegemist K-süsteemi n-kohalise arvuga, siis kataks see n-kohaliste arvude rida 10ndsüsteemis K^n kohta.

Näiteks: Kolmekohaliste 4ndarvude rida näeb välja nii: 000, 001, 002, 003, 010, 011, 012, 013, 020, …jne viimane kolmekohaline 4ndarv on 333. Kogu kolmekohaliste neljandarvude rida aga katab 10ndsüsteemis $4^3 = 4 \cdot 4 \cdot 4 = 64$ kohta.

Arvutused kuni 6-kohaliste eri süsteemi arvudele on toodud tabelis 2.

TABEL2 näitab mitmekohaliste eri arvsüsteemide kasutamisvõimalusi, mitut 10ndsüsteemi kohta (tähekohta) nad suudavad katta:

Arvusüsteem K	**n-kohaline arv**				
	n=2	n=3	n=4	n=5	n=6
2nd-süsteem	4	8	16	**32**	**64**
3nd-süsteem	9	**27**	**81**	243	729
4nd-süsteem	16	**64**	256	1024	4096
5nd-süsteem	25	125	625	3125	15625
6nd-süsteem	**36**	216	1296	7776	46656
7nd-süsteem	49	343	2401	16807	117649
8nd-süsteem	**64**	512	4096	32768	262144
9nd-süsteem	81	729	6561	59049	531441
10nd-süsteem	100	1000	10000	100000	1000000

HARJUTUSED JA üLESANDED

1. Mis arvusüsteemis toimuvad järgmised tehted?

A.
$$\begin{array}{r} 344 \\ + \\ 411 \\ + \\ \underline{203} \\ 2013 \end{array}$$

B.
$$\begin{array}{r} 201 \\ - \\ \underline{112} \\ 67 \end{array}$$

C.
$$\begin{array}{r} 22 \\ \times \\ \underline{11} \\ 22 \\ \underline{22\ .} \\ 302 \end{array}$$

D.
$$\begin{array}{r} 32130 : 213 = 130 \\ \underline{213} \\ 1043 \\ \underline{1043} \end{array}$$

2. Kontrollida kas järgmised tehted on õiged?

A. $401_6 + 233_6 + 102_6 = 1140_6$ B. $20200_3 + 1123_4 - 134_5 = 1015_6$ C.

3. Milliste eri arvusüsteemide puhul kehtivad järgmised võrdused?

A. 13 = 31 = 23 B. 11111 = 321 C. 2014 = 121101 D. 1121 + 302 = 2120

SAMAS-SALAKIRJA PRAKTILISTE VARIANTIDE KLASSIFIKATSIOON

Tabelis 1 poolpaksus kirjas ja allakriipsutatud variandid on leidnud rakendust SAMAS-salakirja käsiraamatus. Iga variant on saanud omale nime vastavalt sellele, mitmekohalisi ja millise arvusüsteemi arve õifreerimisel kasutatakse. Igal SAMAS-salakirja variandil on omad head ja vead ning optimaalne kasutamispiirkond.

TABEL 2 SAMAS-salakirja variantide võrdlus

Nimetus	kirjeldav arv	tähekohti kokku	kohti ühe tähe salastamiseks	parim maskeerimisviis
VIKA	viiekohaline kahendarv	32	5	kirjas
KUKA	kuuekohaline kahendarv	64	6	kirjas
KOKO	kolmekohaline kolmendarv	27	3	kirjas visuaalne
NEKO	neljakohaline kolmendarv	81	4	kirjas visuaalne
KONE	kolmekohaline neljandarv	64	3	(kirjas) visuaalne
KAKU	kahekohaline kuuendarv	36	2	sõnastik visuaalne
KAKA	kahekohaline kaheksandarv	64	2	visuaalne

TÄHESTIK

Käsiraamatus on lähtutud põhiliselt kahest eesti tähestikust:
24-täheline eesti tähestik:
A, B, D, E, F, G, H, I, J, K, L, M, N, O, P, R, S, T, U, V, Õ, Ä, Ö, Ü
32-täheline võõrtähtedega eesti tähestik (nagu see on antud ka “Õigekeelsuse sõnaraamatus”, Tallinn 1960):
A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, Đ, Z, Œ, T, U, V, W, Õ, Ä, Ö, Ü, X, Y
Muukeelsetest tähestikest on vaadeldud 32-tähelist vene tähestikku, kus T=?:
F < D U L T : P B Q R K V Y J G H C N E A X W X I O } S M ò > ó

SÕNUMI KOOSTAMINE

Edastamisele kuuluv informatsioon tuleb enne õifreerimisele asumist korrastada ja koondada SÕNUMIKS. Ühelt poolt tuleb sõnumi sisu esitada võimalikult kokkusurutult, lühendite ja vihjetega. Teisalt aga peab hoolikalt kokkupandud sõnum olema üheselt mõistetav ka ühte tähejorusse ning ilma tähevahedeta väljakirjutatult. Seepärast tuleb enne salastamisele asumist veelkordselt ise veenduda, kas koostatud SÕNUM vastab neile tingimustele.

VÕTME KASUTAMINE

Sõnumi salastamiskindluse tõstmiseks kasutatakse kokkuleppelisi VÕTMEID.
Kuivõrd hoolikad ja konspiratiivnõudeid järgivad me ka poleks, varem või hiljem satub SAMAS-süsteemi kirjeldus ja metoodika vaenlase kätte. Siis on oskuslikult valitud ja hoolikalt saladuses hoitud võtme olemasolu otsustavaks kaitseks salasõnumi soovimatu deõifreerimise vastu. Võtme moodustamisel peaks silmas pidama soovitust, et selleks ei sobi liiga lühikesed sõnad ega tuntud kirjanduslikud tekstid. Soovitatakse järgmist VÕTME moodustamise korda: partnerid moodustavad ja õpivad pähe (või märgivad üles ainult endale teadaoleval viisil) mingi omaloomingulise (vähemalt kümnesõnalise) hästi meeldejääva VÕTMELAUSE. Võtmelausest aga moodustavad vahetult õifreerimise-deõifreerimise toimingu käigus sõnumi pikkuse VÕTME, näiteks algul välja kirjutades sõnade esitähed, siis teised ja siis kolmandad, vastavalt omavahelisele kokkuleppele. Kui võtmelause on hästi pähe õpitud, pole võtme kohene

tähekaupa väljakirjutamine raske. Juhul, kui mõni võtmelause sõna on lühem (näiteks kahetäheline), siis alustatakse teda vajaduse korral uuesti.

SALASTAMISLÜKATID SÕNUMI ÐEŠIFREERIMISEKS
Abilükat sõnumi õifreerimiseks koosneb ALUSEST ja liikuvast KEELEST.

SALASTAMISLÜKATI ALUSE moodustab ruudustik, mis mahutab igale SAMAS-variandile vastava tähekohtade arvu. Teda võib esitada ühe realisena nagu näites 1 (vt. lk. 8) Käsiraamatus soovitatakse moodustada ALUS mitmerealise tabeli kujul, mille ridade arv sõltub kasutatavast arvsüsteemist. Tabeli read nummerdatakse vasakul ja alt üles kasutatava arvsüsteemi numbritega. Veergude numeratsioon kirjutatakse kas vahetult tabeli alla või jättes keele laiuseline teatud vahemaa. Seega on lükati alusel oleva tabeli iga lahter (tähekoht) väljendatav mitmekohalise kasutatava arvsüsteemi arvuga, mille esimene koht (esimesed kohad) vastab reale, millel too täht asub ning teised arvkohad vastava veeru all olevaletele numbritele.

SALASTAMISLÜKATI KEELE ruudustiku laius on sama, mis alusel ja mahutab kasutatava tähestiku kas ühes või mitmes reas. Keelelolev tähestik (ruudustik) dubleeritakse. Ruudustike esimene ruut tähistatakse noolekestega. Dubleerimisest võib ka loobuda, jättes aga alles noolekese esimesel ruudul dubleeritud tähestiku kohal.

VIKA salastamislükat

alus sisaldab 32 lahtrit, kasutatakse 32-tähelist eesti tähestikku

1	Q	R	S	Đ	Z	Œ	T	U	V	W	Õ	Ä	Ö	Ü	X	Y
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	00	**00**	**00**	**00**	**01**	**01**	**01**	**01**	**10**	**10**	**10**	**10**	**11**	**11**	**11**	**11**
	00	**01**	**10**	**11**	**00**	**01**	**10**	**11**	**00**	**01**	**10**	**11**	**00**	**01**	**10**	**11**

keel

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	Đ	Z	Œ	T	U	V	W	Õ	Ä	Ö	Ü	X	Y

KUKA salastamislükat

alus sisaldab 64 lahtrit, kasutatakse 32-tähelist eesti tähestikku ja numbreid 0-31

11	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
01	Q	R	S	Đ	Z	Œ	T	U	V	W	Õ	Ä	Ö	Ü	X	Y
00	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	00	**00**	**00**	**00**	**01**	**01**	**01**	**01**	**10**	**10**	**10**	**10**	**11**	**11**	**11**	**11**
	00	**01**	**10**	**11**	**00**	**01**	**10**	**11**	**00**	**01**	**10**	**11**	**00**	**01**	**10**	**11**

keel

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	Đ	Z	Œ	T	U	V	W	Õ	Ä	Ö	Ü	X	Y

KOKO salastamislükat

alus sisaldab 27 lahtrit, kasutatakse 24-tähelist eesti tähestikku ja 3 lisamärki

2	U	V	Õ	Ä	Ö	Ü	+	–	NB!
1	K	L	M	N	O	P	R	S	T
0	A	B	D	E	F	G	H	I	J
	00	**01**	**02**	**10**	**11**	**12**	**20**	**21**	**22**

keel

A	B	D	E	F	G	H	I	J
K	L	M	N	O	P	R	S	T
U	V	Õ	Ä	Ö	Ü			

N EKO salastamislükat

alus sisaldab 81 lahtrit, kasutatakse 32-tähelist tähestikku ja numbreid 0-49

II SALASTAMINE (ĐIFREERIMINE)

VIIES OSA:
HARJUTUSI JA MÕNINGAID SALAKIRJAÜLESANDEID NUPUTAMISEKS

(HARJUTUSED)
Nii harjutusi kui ka ülesandeid on otstarbekas teha ja lahendada kahekesi. Kuigi ei ole paha osata mingeid salajasi andmeid vajaduse korral ainult endale teadaoleval viisil ära peita. Partneriga koos süsteemi harjutamine on aga alati efektiivsem. Leppige kokku ühised süsteemid, võtmelaused ja tingimused – ja saatke vastastikku üksteisele sõnumeid ning püüdke neid deõifreerida.

HARJUTUS 1 : MASKEERIMINE TAVALISSE KIRJA – DEMASKEERIMINE
Näites nr.1 toodud Leenu kirjast oma õele püüdke ilmutada sinna peidetud numbrid, kasutades samu maskeerimiskaste. Võrrelge tulemust näites salastamisel saadud numbritega.

HARJUTUS 2 : MASKEERIMINE TAVALISSE KIRJA – DEMASKEERIMINE
Võtke näites nr.1 salastamisel saadud arvuderida ja püüdke see peita tavalisse kirja, kasutades näites antud maskeerimiskaste. Järgige soovitust: paigutades numbrid vertikaalselt üksteise alla, nii hõlbustub maskeerimistoiming tunduvalt, väheneb eksimuste võimalus, kerge on teha parandusi ja muudatusi kui mõni lause ummikusse jookseb, paraneb kontroll tehtu üle.

HARJUTUS 3 : MASKEERIMINE KIRJA OTSESEL MEETODIL – DEMASKEERIMINE
Kasutades maskeerimise otsest meetodit, jätkake siin alustatud kirja kirjutamist, kuni kõik arvud on kirja peidetud.

HARJUTUS 4 : MASKEERIMINE TELEGRAMMI KOMBINEERITUD MEETODIL - DEMASKEERIMINE

HARJUTUS 5 : DEÐIFREERI TELEGRAMM kasutades näitesnr.1 toodud VIKA-süsteemi maskeerimiskaste ja salastamislükatit. Kasutades näites toodud võtmelauset, moodusta võti tingimustel 2-3-1, s.t. välja kirjutades algul sõnade teised, siis kolmandad ja lõpuks, kui vaja ka esimesed tähed.

(ÜLESANDED)
Nüüd on nuputamishuvilisel salakirjalahendajal võimalus end seada ühe kurja tsensori asemele, kelle töölauale on kuhjatud poliitiliste laagrivangide kirjavahetus oma perekondadega ja sõpradega. Kirju on palju ja teid lohutab vähe teadmine, et suurem osa kirjavahetust on eeltsensuurist kergemalt läbi lastud. Teie lauale on toodud sisult või vormilt juba kahtlust äratanud kirjad ja nende vangide kirjad, kelle nimed on eriti ohtlike poliitvangide nimekirjas ning kelle kirjavahetus lihtsalt **peab** sisaldama (ja tõenäoliselt sisaldabki) keelatud salasõnumeid. Teie käsutuses on ka KGB operatiivosakondade poolt kogutud lisamaterjalid, mis kujutavad endast dissidentide ja laagrivangide juures aegajalt läbiotsimistel leitud märkmeid, telefonide pealtkuulamisel ja tunnistajate ülekuulamisel saadud vihjeid, ning muidugi nuhkide ettekannnetest kogutud andmeid. Teie ülesandeks on sellest kirjade hulgast leida need, mis kindlalt sisaldavad peidetud sõnumeid - ja need deõifreerida. Sõelale on jäänud viis kirja.

ÜLESANNE NR.1