Peatükk 1

Klassikalised krüptosüsteemid

1.1 Algus

Krüptograafia põhieesmärgiks on võimaldada kahe inimese (tavaliselt tuntud kui Alice ja Bob) suhtlust kaitsmata (*unsecure*) kanalil (näiteks arvutivõrk, läbi telefoni), nii et 'kurikael' Oskar ei suudaks tekstist aru saada, ammugi seda võltsida.

Konkreetsemalt püstitakse ülesanne järgmiselt: Alice soovib saata Bobile mingi sõnumi (*avatekst*), mis võib olla suvalisel kujul (arvud, inglise-, eesti- või setukeelne tekst). Enne saatmist *šifreerib* (*encrypt*) ta selle teksti vaid talle ja Bobile teadaoleva *salavõtme* abil. Bob *dešifreerib* (*decrypt*) saadud **krüptogrammi**. Kuna Oscar ei tea salavõtit, siis ei suuda ta teksti dešifreerida.

Definitsioon 1.1.1 . ***Krüptosüsteemiks*** *nimetatakse viisikut*

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}),$$

kus

1. $\mathcal{P}$ *on kõikvõimalike* ***avatekstide*** *lõplik hulk*
2. $\mathcal{C}$ *on kõikvõimalike* ***krüptogrammide*** *lõplik hulk*
3. $\mathcal{K}$ *on kõikvõimalike* ***võtmete*** *lõplik hulk*
4. *Iga* $K \in \mathcal{K}$ *jaoks leidub* ***šifreerimisreegel*** $E_K \in \mathcal{E}$ *ja vastav* ***dešifreerimisreegel*** $D_K \in \mathcal{D}$*, kus* $E_K : \mathcal{P} \to \mathcal{C}$ *ja* $D_K : \mathcal{C} \to \mathcal{P}$ *on sellised funktsioonid, et iga* $x \in \mathcal{P}$ *korral* $D_K(E_K(x)) = x$.

Siin tingimus 4 esitab nõude, et kui avatekst šifreeritakse reegliga E_K, siis tekkinud krüptogrammi dešifreerimisel reegliga D_K saame tagasi meie originaalse avateksti.

Mingi spetsiifilise krüptosüsteemi järgimiseks tuleb täita järgnevad sammud: kõigepealt valivad Alice ja Bob juhusliku võtme $K \in \mathcal{K}$ (mille vahetamiseks neil *peab* olema turvaline kanal). Edasises oletagem, et Alice tahab Bob'ile edastada stringi

$$x := x_1 x_2 \dots x_n,$$

kus $n \geq 1$ ning iga i korral $x_i \in \mathcal{P}$. Peale krüptosüsteemi lepivad Alice ja Bob eelnevalt kokku ka *töörežiimis*, st. viisis, kuidas sõltuvad üksteisest järjestikused avateksti elementide šifreeringud. Toome siinkohas ära kahe lihtsama režiimi kirjeldused (dešifreerimisprotsess on kummalgi juhul triviaalselt tuletatav šifreerimisreeglitest):

- Kõige lihtsam, **koodiraamatu režiim** (ECB, *electronic codebook*):

$$(\forall i) y_i := E_K(x_i)$$

- **Ahelrežiim** (CBC, *cipher block chaining mode*):

$$\begin{aligned} y_0 &:= E_K(x_0) \\ y_{i+1} &:= E_K(x_{i+1} \oplus y_i) \end{aligned}$$

Seega stringi x šifreering sõltub

1. kasutatavast krüptosüsteemist,
2. töörežiimist.
3. salajasest võtmest K.

Alice šifreerib x'i ning saadab Bobile stringi

$$y := y_1 y_2 \dots y_n.$$

Bob dešifreerib saadud krüptogrammi, kasutades sama krüptosüsteemi, töörežiimi ja võtit.

Šifreerimisreegel E_K peab olema injektsioon, sest vastasel juhul ei oleks dešifreerimine teostatav üheselt (kui $x_1 \neq x_2$ ning $E_K(x_1) = E_K(x_2) =: y$, siis ei oska Bob sõnet y dešifreerida). Siit järeldub, et juhul $\mathcal{C} = \mathcal{P}$ on reeglid E_K hulga $\mathcal{P}$ permutatsioonid.

Igal praktikas kasutataval krüptosüsteemil peab olema kaks omadust:

1. Iga (de)šifreerimisreegel E_K (D_K) peab olema efektiivselt arvutatav (siin ei rahulduta üldjuhul ainult faktiga, et vastavad funktsioonid on polünomiaalselt arvutatavad: praktika nõuab oma). NB! *Praktikas eeldatakse, et nii krüptosüsteem kui ka töörežiim on avalikud.*

2. Oskari jaoks on *raske* ainuüksi krüptogrammi järgi välja arvutada võtit K ja/või avateksti.

Siin teine omadus defineerib väga ebamäärasel moel seda, mida me intuitiivselt mõistame turvalisuse all. Võtme ja/või avateksti leidmisega tegeleb **krüptoanalüüs**. **Krüptoloogia** on krüptograafia ja krüptoanalüüsi ühend.

1.2 Lihtšifrid

Enamus krüptosüsteeme baseeruvad aritmeetikal lõplikes arvuvaldades, tüüpiliselt on selleks vallaks hulk $\mathbb{Z}_n$ (koos standardliitmise või -korrutamisega), kuid vaadeldakse ka aritmeetikat üle Galois' korpuste ning elliptiliste kõverate.

Tüüpkasutuses olevaid lihtšifreid võib jaotada kahte alamliiki: substitutsiooni- ja permutatsioonišifrid.

Krüptosüsteem 1.2.1 (substitutsioonišiffer) .

Olgu $\mathcal{P} := \mathcal{C} := \mathbb{Z}_{32}$ *ning* $\mathcal{K} := \mathcal{S}_{32}$. *Iga substitutsiooni* $\pi \in \mathcal{K}$ *jaoks defineerime*

$$E_\pi(x) := \pi(x) \text{ ning}$$
$$D_\pi(x) := \pi^{-1}(x).$$

Nii üldise ülesandepüstituse korral $|\mathcal{K}| = 32!$ ning seega on brutaalne jõumeetod krüptoanalüüs raskendatud.

Hulk $\mathbb{Z}_{32}$ on valitud siin seetõttu, et eesti tähestikus on 32 tähte. Defineerime kujutuse μ Eesti tähtede hulkast antud hulka järgmiselt: $\mu(\mathtt{A}) = 0$, $\mu(\mathtt{B}) = 1$ jne (vt joonis 1.1).

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

Joonis 1.1: Eesti tähed

Vaatleme järgnevalt mõnda substitutsioonišifri erijuhtu.

Krüptosüsteem 1.2.2 (nihkešiffer) . *Olgu* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{32}$. *Olgu* $K \in \{0, \ldots, 31\}$, *defineerime*

$$E_K(x) = x + K \pmod{32}$$

ning

$$D_K(y) = y - K \pmod{32}.$$

Näide 1.2.3 *Olgu $K := 6$, $x :=$ `MÄEKÜLAPIIMAMEES`. Šifreerides saame (μ(`M`)$+ 6 = \mu$(`S`) jne) krüptogrammiks stringi* `SBKQDRGŽOOSGSKKV` *(eesti keele liiasuse tõttu on küllalt raske leida pikemaid sõnu, mis nihkešifriga šifreeritult tähendust omaks). Antud küllalt huvitava krüptogrammi saamise järel rakendab Bob vastandprotseduuri: μ(`S`)$- 6 = \mu$(`M`), μ(`B`)$- 6 = \mu$(`Ä`) jne.*

Muidugi võib siin eesti tähestiku asemel võtta suvalise teise märgihulga, nii näiteks võime meie tähestikku lisada tühiku ning mõned punktuatsioonimärgid või kasutada hoopis originaalset vanade roomlaste tähestikku (kodeerides lisandunud tähed mingil kergesti arusaadaval viisil). Erijuhul $K = 3$ nimetatakse seda krüptosüsteemi ka **Caesari šifriks** (Julius Caesar nimelt kasutas seda šifrit).

Pangem tähele, et nihkešiffer ei ole turvaline, kuna teda saab täieliku läbivaatusmeetodit kasutades krüptoanalüüsida. Kuna antud juhul $|\mathcal{K}|$=32, siis ei ole see eriti raske (arvestades ka eesti keele ülalmainitud omapärasid).

Harjutus 1.2.4 . *Leida täieliku läbivaatusmeetodiga krüptogrammile* `VOAATVSUOVOVFVS` *vastav avatekst.*

Krüptosüsteem 1.2.5 (afiinne šiffer) . *Olgu $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32}$ ning*

$$\mathcal{K} = \{(a, b) : \gcd(a, 32) = 1\}.$$

Iga $K = (a, b) \in \mathcal{K}$ jaoks defineerime

$$E_K(x) = ax + b \pmod{32} \text{ ning}$$
$$D_K(y) = a^{-1}(y - b) \pmod{32}.$$

Tingimus $\gcd(a, 32) = 1$ on vajalik, kuna vastasel juhul poleks E_K bijektsioon. Antud krüptosüsteemi korral $|\mathcal{K}| = 32 \cdot \phi(32) = 32 \cdot 16 = 512$. Kontrollimine annab, et $D_K(E_K(x)) = a^{-1}((ax + b) - b) \equiv x \pmod{32}$ (kõik tehted toimuvad modulo 32, kaasa arvatud pöördelemendi leidmine).

Kuidas leida elementi $a^{-1} \mod 32$? Vastus lihtne, tuleb kasutada järgmist Eukleidese algoritmi modifikatsiooni (kuna edaspidi läheb meil seda algoritmi korduvalt vaja, siis peatume sellel siin pikemalt).

Algoritm 1.2.6 (Eukleidese algoritm) *Olgu* $\gcd(a, n) = 1$, *vaja leida* $a^{-1} \mod n$.

funct *inv*$(a, n) \equiv$
  $r_0 = n$; $r_1 := a$; $i := 0$; $t_0 := 0$; $t_1 := 1$;
  while *true* **do**
    $q_{i+1} := \lfloor r_i / r_{i+1} \rfloor$;
    $r_{i+2} := r_1 - r_{i+1} q_{i+1}$;
    $t_{i+2} := t_i - q_{i+1} t_{i+1} \mod n$;
    if $r_{i+2} = 0$ **then** *inv* $:= t_{i+1} \mod n$; **exit**; **fi**
    $i := i + 1$;
  od.

Harjutus 1.2.7 . *Tõestada, et* $a^{-1} = t_{i+1} \mod n$.

Näide 1.2.8 *Olgu* $n = 6534$, $a = 31$.

1. $r_0 = 6534$, $r_1 = 31$.

2. $i = 0$: $6534 = 210 \cdot 31 + 24$, *siit* $q_1 = 210$, $r_2 = 24$.

$$t_2 = 0 - 210 \cdot 1 = 6324 \mod 6534.$$

3. $i = 1$: $31 = 1 \cdot 24 + 7$,

$$t_3 = 1 - 1 \cdot 6324 = 211 \mod 6534.$$

4. $i = 2$: $24 = 3 \cdot 7 + 3$,

$$t_4 = 6324 - 3 \cdot 211 = 5691 \mod 6534.$$

5. $i = 3$: $7 = 2 \cdot 3 + 1$,

$$t_5 = 211 - 2 \cdot 5691 = 1897 \mod 6534.$$

6. $i = 4$: $3 = 3 \cdot 1 + 0$,

$$t_6 = 5691 - 3 \cdot 1897 = 0 \mod 6534.$$

7. *Kuna* $r_6 = 0$, *siis* $a^{-1} = t_5 = 1897$.

Kontroll: $1897 \cdot 31 \equiv 1 \pmod{6534}$.

Harjutus 1.2.9 . *Võttes* $K = (3, 1)$, *šifreerida nimi* `OTTOKATZ`. *Sama võtme korral dešifreerida krüptogramm* `QNCKYGZBBD`.

Eelpool toodud krüptosüsteeme nimetatakse **monoalfabeetilisteks**, kuna iga valitud võtme korral kujutub suvaline avateksti sümbol konstantseks sümboliks. **Polüalfabeetiliste** šifrite, kus iga üksiku sümboli šifreering sõltub ka selle sümboli asukohast avatekstis, näitena toome Vigenère'i šifri.

Krüptosüsteem 1.2.10 (Vigenère'i šiffer) *Olgu* $m > 0$ *mingi fikseeritud naturaalarv. Olgu* $\mathcal{P} := \mathcal{C} := \mathcal{K} := (\mathbb{Z}_{32})^m$. *Võtme* $K = (k_1, \ldots, k_m)$ *korral*

$$E_K(x_1, \ldots, x_m) := (x_1 + k_1, \ldots, x_m + k_m)$$

ja

$$D_K(y_1, \ldots, y_m) := (y_1 - k_1, \ldots, y_m - k_m),$$

kus kõik tehted toimuvad ringis $\mathbb{Z}_{32}$.

Näide 1.2.11 *Olgu* $x =$ *KESEIOSANDLUGEDASEESAI* *ning* $K =$ *KASSILT*. *Siis saame komponenthaaval liites*

KESEIOSANDLUGEDASEESAI+
KASSILTKASSILTKASSILTK=
ZEETQWIKNŽÜYRÕNAETMÜTS

Harjutus 1.2.12 *Olgu* $y =$ *KESEIOSANDLUGEDASEESAI* *ning* $K =$ *KASSILT*. *Leida vastav avatekst.*

Viimase substitutsioonišifrina defineerime *eriti* lihtsa lihtšifri.

Krüptosüsteem 1.2.13 (Kordumatu numbrijada (*one-time pad*)) .
Olgu

$$\mathcal{P} = \mathcal{K} = \mathcal{C} = \mathbb{Z}^m,$$

$m > 0$. *Defineerime*

$$E_K(x) := x \oplus K$$
$$D_K(y) := y \oplus K.$$

Kordumatu numbrijada on tingimusteta turvaline:

$$(\forall y \in \mathcal{C})(\forall x \in \mathcal{P})(\exists K \in \mathcal{K}) y = x \oplus K.$$

Halvaks omaduseks on see, et võti on sama pikk kui avatekst ning *iga* uue avateksti šifreerimiseks tuleks turvalisuse saamiseks valida uus võti.

Siiamaani toodud šifrid olid kõik substitutsioonišifri erijuhud: erinevad avateksti sümbolid asenduvad erinevateks krüptogrammi sümboliteks. Permutatsioonišifri korral jäetakse avateksti sümbolid muutmata, selle asemel muudetakse nende järjekorda.

Krüptosüsteem 1.2.14 (permutatsioonišiffer) *Olgu* m *mingi fikseeritud positiivne täisarv. Olgu* $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{32})^m$ *ning olgu* $\mathcal{K} = \mathcal{S}_m$. *Suvalise võtme (permutatsiooni)* $\pi \in \mathcal{K}$ *jaoks defineerime*

$$E_\pi(x_1, \ldots, x_m) := (x_{\pi(1)}, \ldots, x_{\pi(m)})$$

ja

$$E_\pi(y_1, \ldots, y_m) := (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(m)})$$

Põhjalikuks ülevaateks lihtšifritest võib soovitada eesti keeles ilmunud raamatut [Liv94].