

Ülesanded

I töö:

Ülesanne 1 (30 punkti) Sõnest $S = \text{asfdfsadfgfdasdsfdfsfga}$ valitakse ühtlase jaotusega üks täht. Kui suur on tõenäosus, et kaks sõltumatult valitud tähte osutuvad võrdseteks?

Ülesanne 2 (30 punkti) Olgu X juhuslik suurus väärtustega $\{a, s, d, f, g\}$, mis on seotud eelmises ülesandes toodud katsega – valida ühtlaselt täht sõnest S . Leia suuruse X kombinatoorne entroopia H_{comb} .

Ülesanne 3 (40 punkti) Krüpteeritavad sõnumeid esitatakse arvudena $\{0, \dots, 25\}$, võti $K = (k_1, k_2)$ valitakse ühtlase jaotusega hulgast $\{1, \dots, 25\} \times \{1, \dots, 25\}$, kusjuures krüpteerimine toimub kahe-arvuliste komplektide $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ kaupa järgmiselt:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} k_1 & 0 \\ k_2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \pmod{26} .$$

Kas see siffer of täielikult salastav? Põhjenda!

II töö:

Ülesanne 1 (30 punkti). Arvuta (võimalikult lihtsalt): (A) $3^{1110} \pmod{1189}$ ja (B) $3^{1000} \pmod{1019}$.

Ülesanne 2 (70 punkti). Leida võrrandi: (A) $x^2 \equiv 1 \pmod{37481}$ kõik lahendid vahemikus $[0 \dots 37480]$, ja (B) $x^2 \equiv 1 \pmod{41779}$ kõik lahendid vahemikus $[0 \dots 41778]$. Põhjenda vastust!

Lahendused

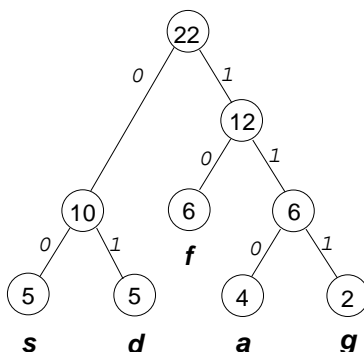
Ülesanne I-1. Tähtede loendamise teel sõnes $S = \text{asfdfsadfgfdasdsfdfsfga}$ arvutame tähtede väljatuleku tõenäosused:

$$p(a) = \frac{4}{22}, p(s) = \frac{5}{22}, p(d) = \frac{5}{22}, p(f) = \frac{6}{22}, p(g) = \frac{2}{22} .$$

Otsitav tõenäosus tuleb siis:

$$p^2(\mathbf{a}) + p^2(\mathbf{s}) + p^2(\mathbf{d}) + p^2(\mathbf{f}) + p^2(\mathbf{g}) = \frac{16 + 25 + 25 + 36 + 4}{484} = \frac{106}{484} \approx 0.219$$

Ülesanne I-2. Kombinatorse entroopia leidmiseks ehitame Huffmani puu:



ja seejärel arvutame koodi keskmise pikkuse. Saame, et

$$H_{\text{comb}} = \frac{1}{22} \cdot (5 \cdot 2 + 5 \cdot 2 + 6 \cdot 2 + 4 \cdot 3 + 2 \cdot 3) = \frac{50}{22} \approx 2.27 .$$

Ülesanne I-3. Toodud šiffer ei ole täielikult salastav, sest krüptogrammi teadmine annab infot avateksti kohta (isegi juhul, kui võtme kohta info puudub). Tõepoolest, erinevate avatekstide arv on 26^2 kuid erinevate võtmete arv ainult 25^2 ja seetõttu saab piiramatu vastane krüptogrammi $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ abil välistada osa avatekstidest – ta proovib läbi kõik võtmed ja arvutab igale võtmele vastava avateksti (mida on täpselt üks, sest krüpteerimisteisendus on pööratav). Kuna võtmeid on vähem kui avatekste, siis osad avatekstid "jäävad üle" ja ründaja saab teada, et need avatekstid antud krüptogrammile $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ ei vasta, kuid see on juba informatsioon avateksti kohta.

Ülesanne II-1. (A) $3^{1110} \pmod{1189}$ arvutamiseks lahutame mooduli teguriteks ja saame, et $1189 = 29 \cdot 41$. Seega $\phi(1189) = 28 \cdot 40 = 1120$ ja Euleri teoreemist tulenevalt $3^{1120} \pmod{1189} = 1$. Seega $3^{1110} \equiv 3^{1110-1120} \equiv 3^{-10} \equiv (3^5)^{-2} \equiv 243^{-2} \equiv (243^2)^{-1} \equiv 59049^{-1} \equiv 788^{-1} \pmod{1189}$. Eukleidese algoritmi kasutades saame, et $(-255) \cdot 788 + 169 \cdot 1189 = 1$, millest järelduvalt $788^{-1} \equiv -255 \equiv 934$.

(B) $3^{1000} \pmod{1019}$ arvutamiseks üritame lahutada mooduli teguriteks, püüdes seda jagada väiksemate algarvudega kui $\sqrt{1019}$. Saame, et 1019 ei jagu arvudega 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, millest järeldub, et 1019 on algarv. Fermat' teoreemi järgi $3^{1018} \pmod{1019} = 1$. Seega $3^{1000} \equiv 3^{1000-1018} \equiv 3^{-18} \equiv (3^9)^{-2} \equiv 19683^{-2} \equiv 322^{-2} \equiv (322^2)^{-1} \equiv 103684^{-1} \equiv 765^{-1} \pmod{1019}$. Eukleidese algoritmi kasutades saame, et $341 \cdot 765 + (-256) \cdot 1019 = 1$, millest järelduvalt $765^{-1} \equiv 341$.

Ülesanne II-2. (A) Võrrandi $x^2 \equiv 1 \pmod{37481}$ kõigi lahendite leidmiseks hulgas $\mathbb{Z}_{37481} = \{0, \dots, 37480\}$ lahutame esmalt mooduli teguriteks (proovides jagamist väikeste algarvudega) ja saame: $37480 = 37 \cdot 1013$. Seega on \mathbb{Z}_{31481} Hiina jäägiteoreemi järeldusena kahe korpuse otsekorrutis $\mathbb{Z}_{37} \times \mathbb{Z}_{1013}$, kusjuures mõlemas korpuses on antud võrrandil parajasti kaks lahendit: $\pm 1 \pmod{37}$ ja $\pm 1 \pmod{1013}$. Neid lahendeid kombineerides saame neli erinevat lahendit ringis \mathbb{Z}_{37481} . Kaks lahendit on arvutamatagi teada: need on 1 ja $-1 \equiv 37480 \pmod{37481}$.

Eukleidese algoritmi kasutades saame, et $(-219) \cdot 37 + 8 \cdot 1013 = 1$. Seega saame ühe mittetriviaalse lahendi kui võtame korpuses \mathbb{Z}_{37} lahendi $x_1 \equiv -1 \equiv 36$ ja korpuses \mathbb{Z}_{1013} lahendi $x_2 \equiv 1$. Saame, et sellele lahendite paarile vastab ringis \mathbb{Z}_{37481} lahend:

$$x = (-219) \cdot 37 \cdot 1 + 8 \cdot 1013 \cdot 36 \pmod{37481} = 21274 .$$

Seega on otsitavad lahendid 1, 16207 (st -21274), 21274 ja 37480.

(B) Võrrand $x^2 \equiv 1 \pmod{41779}$ lahendatakse analoogiliselt. Kõigepealt leiame, et $41779 = 41 \cdot 1019$ ja Eukleidese algoritmi kasutades saame, et $174 \cdot 41 + (-7) \cdot 1019 = 1$. Seega saame ühe mittetriviaalse lahendi järgmiselt:

$$x = 174 \cdot 41 \cdot 1018 + (-7) \cdot 1019 \cdot 1 \pmod{41779} = 27512 .$$

Seega on otsitavad lahendid 1, 14627 (st -27512), 27512 ja 41778.