Uvod v Računalništvo

Vaje 11

Luka Šveigl

1. DOMAČA NALOGA

Z uporabo zgoščevalne funkcije iz Naloge 11.1 poiščite šifrirano obliko naslednjih gesel:

a) Sonce
b) Morje
c) Pla11ža

Zgoščevalna funkcija:

Recimo, da imamo podano naslednjo zgoščevalno funkcijo (angl. hash function). Oglejmo si, kako lahko s to funkcijo šifriramo geslo "vohun1".

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

1. Posamezne črke gesla nadomestimo z zaporednimi številkami teh črk v abecedi (a -> 1, b -> 2, ..., ž -> 25). V pomoč nam je tabela. Morebitne števke v geslu pustimo nespremenjene.
2. Seštejemo števila iz 1. koraka, rezultat je eno samo število (vsota).
3. Delimo število iz 2. koraka s 7 in poiščemo ostanek.
4. Ostanku iz 3. koraka prištejemo 1, rezultat pa nato množimo z 9.
5. Obrnemo števke števila iz 4. koraka in nato nadomestimo vsako števko z ustrezno črko abecede.

a) Geslo: sonce
    1. Novo geslo: 19 16 15 3 6
    2. Vsota: 19 + 16 + 15 + 3 + 6 = 59
    3. Ostanek deljenja s 7: 59 / 7 = 8 + 3, ker je 8 * 7 = 56 in 59 – 56 = 3
       Ostanek je 3
    4. Prištejemo 1: 3 + 1 = 4
       Množimo z 9: 4 * 9 = 36
    5. Obrnemo števke: 36 -> 63
       Nadomestimo števke: **ec**

b) Geslo: morje
    1. Novo geslo: 14 16 18 11 6
    2. Vsota: 14 + 16 + 18 + 11 + 6 = 65
    3. Ostanek deljenja s 7: 65 / 7 = 9 + 2, ker je 9 * 7 = 63 in 65 – 63 = 2
       Ostanke je 3
    4. Prištejemo 1: 2 + 1 = 3
       Množimo z 9: 3 * 9 = 27
    5. Obrnemo števke: 27 -> 72
       Nadomestimo števke: **fb**

c) Geslo: pla1lža
    1. Novo geslo:17 13 1 1 1 25 1
    2. Vsota: 17 + 13 + 1 + 1 + 1 + 25 + 1 = 59
    3. Ostanek deljenja s 7: 59 / 7 = 8 + 3, ker je 8 * 7 = 56 in 59 – 56 = 3
       Ostanek je 3
    4. Prištejemo 1: 3 + 1 = 4
       Množimo z 9: 4 * 9 = 36
    5. Obrnemo števke: 36 -> 63
       Nadomestimo števke: **ec**

Ugotovimo, da z uporabo te zgoščevalne funkcije dobimo nova gesla sonce -> ec, morje -> fb in pla1lža -> ec. Rezultat prvega in drugega gesla je enak, čeprav sta gesli različni.

2. DOMAČA NALOGA

Aknpkl ak ejckmiuzef juf eiufk nuik uspkmešemujb knbvb

Da dešifriramo to navodilo, moramo najprej ugotoviti ključ, ki je bil uporabljen za šifriranje. Najprej sem poizkusil z ključem k = 5 iz naloge 11.2 ampak se to ni izšlo.

Reševanje sem začel tako, da sem začel s ključem k = 1, kar pomeni, da so vse črke v abecedi zamaknjene samo za 1 mesto, tako a zamenja b, itd. Rezultat s tem ključem nima smisla:

blorlm bl fkčlnjvžfg kvg fjvgl ovjl všrlnftfnvkc loczc

Nato sem reševanje nadaljeval s ključem k = 2, katerega rezultat prav tako nima smisla:

cmpsmn cm gldmokzagh lzh gkzhm pzkm ztsmogugozlč mpčžč

Ker tudi s ključem k = 2 nisem bil uspešen sem poizkusil ključ k = 3, kar spet ni podalo nobenega logičnega stavka:

čnršno čn hmenplžbhi mži hlžin ržln žušnphvhpžmd nrdad

Nato sem poskusil še s ključem k = 4, ki pa mi je končno podal logično rešitev:

dostop do informacij naj imajo samo avtorizirane osebe

To nalogo sem torej reševal z načinom “Brute force”, kjer sem začel z ključem k = 1 in poskusil vse možne rešitve. Imel sem srečo, saj sem hitro prišel do prave rešitve, če pa nebi bi najverjetneje napisal program za reševanje cezarjeve šifre. Lahko bi poskusil tudi analizirati stavek in previdno izbirati ključe, ampak sem raje začel z brute force metodo.

3. DOMAČA NALOGA

Izvedeli smo, da sta javni in privatni ključ različna in da je e * d = 81, pri čemer za zapis d-ja zadoščata dva bita, ter velja: 1 < e < m in 0 < m < n. Kakšno je originalno sporočilo M, če je šifrirano sporočilo C = 5.

Znani podatki:

Javni ključ ni enak privatnemu ključu

e * d = 81

Za zapis d zadoščata 2 bita

1 < e < m

0 < m < n

C = 5

Izračun ostalih podatkov:

e * d mod m = 1, 81 mod m = 1, **m = 80**, ker če 81 delimo z 80 dobimo ostanek 1

Če za zapis d zadoščata 2 bita, potem je to število lahko 00, 01, 10 ali 11, torej je njegov razpon vrednosti od 0 do 3

00 ni mogoče, saj e * 0 ne more biti 81

01 = 1, 81 / 1 = e -> e = 81, ne zadosti pogoju e < m

10 = 2, 81 / 2 = e -> e = 40,5, ni celo število

11 = 3, 81 / 3 = e -> **e = 27**, ker mora biti e < m, in sta m in e tuji: pravilna rešitev

m = (p - 1)(q - 1) -> 80 = (p - 1)(q – 1), možna p in q sta:

p = 17, q = 6, ker 16 * 5 = 80, ni pravilno, q ni praštevilo

p = 41, q = 3, ker je 40 * 2 = 80, pravilno, 41 in 3 sta praštevili

p = 21, q = 5, ker je 20 * 4 = 80, ni pravilno, p ni praštevilo

p = 81, q = 2, ker je 80 * 1 = 80, ni pravilno, p ni praštevilo

n = p * q -> n = 41 * 3 -> **n = 123**

Izračunani podatki: e = 27, d = 3, m = 80, n = 123, p = 41, q = 3

Dešifriranje:

C^d mod n = M -> 5^3 mod 123 = M -> 125 mod 123 = 2, ker če 125 delimo z 123 dobimo rezultat 1 in ostanek 2, torej je originalno sporočilo **M = 2.**

Originalno sporočilo M = 2