Uvod v računalništvo
vaje

21. – 23. december 2015

Primer zgoščevalne funkcije

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

1. Posamezne črke gesla nadomestimo z zaporednimi številkami teh črk v abecedi (a → 1, b → 2, …, ž → 25). V pomoč nam je spodnja tabela.

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

   Morebitne številke v geslu pustimo nespremenjene. Geslo "vohun1" se tako pretvori v naslednje zaporedje: 23 16 9 22 15 1.
2. Seštejemo števila iz 1. koraka, rezultat je eno samo število (vsota). V našem primeru: 23 + 16 + 9 + 22 + 15 + 1 = 86.
3. Delimo število iz 2. koraka s 7 in poiščemo ostanek. V našem primeru dá deljenje števila 86 s številom 7 ostanek 2 (86 = 12 · 7 + 2).
4. Ostanku iz 3. koraka prištejemo 1, rezultat pa nato množimo z 9. V našem primeru: (2 + 1) · 9 = 27.
5. Obrnemo številke števila iz 4. koraka in nato nadomestimo vsako številko z ustrezno črko abecede. V našem primeru dobimo 72, kar ustreza nizu "fb". S pomočjo zgornje zgoščevalne funkcije smo torej geslo "vohun1" zašifrirali v niz "fb".

Naloga 1

Z uporabo opisane zgoščevalne funkcije poiščite šifrirano obliko naslednjih gesel:

a) sonce
b) morje
c) pla11ža

Naloga 2

Z uporabo Cezarjeve šifre (glejte tudi 2. vaje, naloga 9) in ključa $k = 5$ dešifrirajte naslednje prejeto sporočilo: tiuvn tpšt še zajdeo.

Naloga 3

Prestregli ste naslednje sporočilo, šifrirano s pomočjo Cezarjeve šifre:
gitunzs fbidi sz miš tušeln ažm abnmabihzst. Najdite vrednost ključa *k* in dešifrirajte sporočilo.

Naloga 4

Ena izmed enostavnih operacij (sicer sorazmerno zapletenega) algoritma DES je tudi *ekskluzivni ALI* (XOR). Izračunajte 6-bitni niz, ki je rezultat naslednje operacije: 100111 XOR 110101.

Naloga 5

Za algoritem RSA izberite $p = 3$ in $q = 5$.

a) Izračunajte n in m.
b) Naj bo $e = 11$. Kolikšen je d?
c) Navedite javni in zasebni ključ.
d) Kakšna je šifrirana oblika sporočila "3"?
e) Ponovno dešifrirajte sporočilo, ki ste ga dobili v podnalogi c) in preverite, ali dobite izvorno sporočilo "3".

Naloga 6

Za algoritem RSA izberite $p = 3$ in $q = 11$.

a) Izračunajte n in m.
b) Izberite e in d.
c) Navedite javni in zasebni ključ.
d) Kakšna je šifrirana oblika sporočila "2"?

Naloga 7

Za algoritem RSA izberite $p = 11$ in $q = 7$. Najdite števili e in d, ki jih potrebujemo za šifriranje oziroma dešifriranje.