

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

HACKER

Cliff Stoll ve své knize Kukaččí vejce popisuje, jakým způsobem se jeden s prvních soudně stíhaných hackerů dostal k heslům uživatelů PC ve Spojených státech.

Heslo, které si zvolí uživatel, je v počítači zakódováno a jeho kódovaná verze je uložena v počítači. Heslo je zakódováno algoritmem, který funguje jen jednosměrně. Ze zakódovaného tvaru nelze získat původní heslo.

Aby hacker získal původní heslo, přeložil pomocí počítače všechna slova ve slovníku do kódovaného tvaru. Pokud bylo heslo ze slovníku, našel shodnou zakódovanou verzi a tedy i původní heslo. Proto není vhodné používat jako hesla běžná slova, ale raději náhodné skupiny písmen a čísel.



Pokus se zopakovat hackerův postup na jednoduchém algoritmu. K nahrazení znaků hesla použijeme následující tabulku.

A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	R	S	T	U
20	21	22	23	24	25	26	27	28	29
V	W	X	Y	Z		π	@	&	_
30	31	32	33	34	35	36	37	38	39
0	1	2	3	4	5	6	7	8	9
40	41	42	43	44	45	46	47	48	49

Kódovací algoritmus si ukážeme na zakódování slova Adelka:

- Znaky slova zapíšeme pomocí čísel z tabulky tak, že každý znak z horního řádku tabulky nahradíme dvojčiferným číslem z dolního řádku tabulky.
V případě slova Adelka, dostaneme: 10 13 14 21 20 10
- Vynásobíme získaná dvojčiferná čísla:
 $10 \cdot 13 \cdot 14 \cdot 21 \cdot 20 \cdot 10 = 7\,644\,000$
- Zapíšeme dvojčiferná čísla z kroku 1 za sebe a získáme jedno dvanáctičiferné číslo 101314212010. Rozdělíme toto číslo na dvě poloviny a tato dvě šestičiferná čísla vynásobíme:
 $101314 \cdot 212010 = 21479581140$
- Vynásobíme obě výsledná čísla z kroku 2 a 3 a dostaneme:
 $7644000 \cdot 21479581140 = 164189918234160000$
- Výsledné číslo rozdělíme zleva po dvojicích cifer na dvojčiferná čísla:



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

16 41 89 91 82 34 16 00 00

V případě lichého počtu cifer, k samostatné poslední číslici připíšeme 9.

6. Dvojciferná čísla nahradíme symboly pomocí tabulky.
Pokud máme číslo, které není v tabulce, opíšeme ho.
Pokud vychází číslo od 0 do 9 z tabulky, napíšeme za ně symbol α .
Dostaneme:
G1 α 899182ZG0000

Urči, které heslo ze seznamu přísluší kódu: MT7270SS0074 α 00

- a) Pavel
- b) Honza
- c) Pepa5
- d) Jan221
- e) Mira s
- f) Adam 7
- g) Marta
- h) Jarda
- i) 2hadi