Sieci komputerowe, ćwiczenie: Szyfrowanie algorytmem RC4

RC4 to znany strumieniowy algorytm szyfrujący. Cechuje się szybkością i prostotą, przez co znalazł szerokie zastosowanie, między innymi jako jedna z metod szyfrowania w protokole SSL, w szyfrowaniu dokumentów Word i Excel, oraz w protokole WEP w sieciach bezprzewodowych WiFi.

Szyfrowanie wiadomości **w** (składającej się z ciągu bajtów) do szyfrogramu **x** następuje w dwóch etapach. W pierwszym, generujemy tablicę pomocniczą **S** o rozmiarze 256 bajtów:

1. Najpierw tworzona jest tablica identycznościowa **S** = *{0, 1, 2, ... 255}*.
2. Korzystając z klucza tworzymy permutacje **S**:

j = 0
od i=0 do i=255 :
j = (j + $\mathbf{S}_i$ *+* $klucz_{[i \text{ modulo długość klucza}]}$ *) modulo 256*
zamień $\mathbf{S}_i$ *z* $\mathbf{S}_j$

Następnie generujemy ciąg liczb pseudolosowych i szyfrujemy wiadomość:

i = 0
j = 0
od k = 1 do długości wiadomości :
i = (i + 1) modulo 256
j = (j + $\mathbf{S}_i$*) modulo 256*
zamień $\mathbf{S}_i$ *z* $\mathbf{S}_j$
$\mathbf{x}_k = \mathbf{S}_{[(\mathbf{S}i \ + \ \mathbf{S}j) \text{ modulo } 256]}$ XOR $\mathbf{w}_k$

Zadania:

1. Wymyśl klucz i wypisz odpowiadającą jemu tablicę **S**.

2. Wymyśl krótką wiadomość i zaszyfruj ją korzystając z tablicy **S** oraz wartości liter w tablicy ASCII (poniżej). Podaj klucz, wiadomość i wynik.

   Ponieważ szyfrogram może zawierać liczby od 0 do 255, które nie odpowiadają literom alfabetu, podaj wynik jako ciąg wartości liczbowych w systemie szesnastkowym.

Fragment tablicy ASCII:

	32		46		48	49	50	51	52	53	54	55	56	57		65	66	67	
	20		2E		30	31	32	33	34	35	36	37	38	39		41	42	43	
spacja			.		0	1	2	3	4	5	6	7	8	9		A	B	C	
68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	
44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
87	88	89	90	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	
57	58	59	5A	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	
W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
112	113	114	115	116	117	118	119	120	121	122									
70	71	72	73	74	75	76	77	78	79	7A									
p	q	r	s	t	u	v	w	x	y	z									

XOR:

W systemie dwójkowym:

	0	**1**
0	0	1
1	1	0

W systemie szesnastkowym:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0