Дополнительная (справочная) литература по дисциплине

1. І.Д. Горбенко. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч. 1. Криптографічний захист інформації. —Харків: ХНУРЕ, 2004 р. — 368.

2. Вербицький О.В. Вступ до криптології. — Львів: Науково - технічна література. — 1998. — 247 с.

Примеры элементарных симметричных шифров:

1) двоичное поточное шифрование (двоичное гаммирование);
2) *m*-ичное поточное шифрование (*m*-ичное гаммирование);
3) моноподстановка;
4) полиподстановка.

1. Двоичное поточное шифрование

$$C_i = M_i \oplus K_s ,$$
$$M_i = C_i \oplus K_s .$$

Пример 1.

M = “plain text” ; $l_M = 10$;

K = “password” ; $l_K = 8$;

	p	l	a	i	n	‘ ’	t	e	x	t
	70	6C	61	69	6E	20	74	65	78	74
⊕	p	a	s	s	w	o	r	d	p	a
	70	61	73	73	77	6F	72	64	70	61
	00	0D	12	1A	19	4F	06	01	08	15
	–	–	–	–	–	O(л)	–	–	–	M(р)

2. *m*-ичное поточное шифрование

$$C_i = (M_i + K_s) \bmod m ,$$

$$M_i = (C_i - K_s) \bmod m .$$

Пример 2.

$m = 27$;

M = “plain text” ; $l_M = 10$;

K = “password” ; $l_K = 8$;

0	1	2	3	4	5	6	7	8	9	10	11	12	
a	b	c	d	e	f	g	h	i	j	k	l	m	
13	14	15	16	17	18	19	20	21	22	23	24	25	26
n	o	p	q	r	s	t	u	v	w	x	y	z	‘ ’

C = “dls injhlt” ; $l_C = 10$.

	p	l	a	i	n	‘ ’	t	e	x	t
	15	11	0	8	13	26	19	4	23	19
+	p	a	s	s	w	o	r	d	p	a
	15	0	18	18	22	14	17	3	15	0
	30	11	18	26	35	40	36	7	38	19
mod *m*	3	11	18	26	8	13	9	7	11	19
	d	l	s	‘ ’	i	n	j	h	l	t

M = “plain text” ; $l_M = 10$;

K = “password” ; $l_K = 8$;

C = “dls injhlt” ; $l_C = 10$.

	d	l	s	‘ ’	i	n	j	h	l	t
	3	11	18	26	8	13	9	7	11	19
-	p	a	s	s	w	o	r	d	p	a
	15	0	18	18	22	14	17	3	15	0
	-12	11	0	8	-14	-1	-8	4	-4	19
	15	11	0	8	13	26	19	4	23	19
mod *m*	p	l	a	i	n	‘ ’	t	e	x	t

C = “dls injhlt” ; $l_C = 10$;

K = “password” ; $l_K = 8$;

M_1 = “plain text” ; $l_M = 10$.

3. Моноподстановка

Пример 3. m=27;

	0	1	2	3	4	5	6	7	8	9	10	11	12
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Вых.	n	p	g	m	r	h	w	b	u	c	f	t	a

	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Вх.	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**‘ ’**
Вых.	‘ ’	q	i	x	j	d	v	k	e	y	l	z	s	o

“plain **t**ex**t**” → “itnu o**v**r**l**v” ;

“itnu o**v**r**l**v” → “plain text” .

Прямая таблица:

	0	1	2	3	4	5	6	7	8	9	10	11	12
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Вых.	n	p	g	m	r	h	w	b	u	c	f	t	a

	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Вх.	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**‘ ’**
Вых.	‘ ’	q	i	x	j	d	v	k	e	y	l	z	s	o

Обратная таблица:

	0	1	2	3	4	5	6	7	8	9	10	11	12
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Вых.	m	h	j	s	v	k	c	f	p	r	u	x	d

	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Вх.	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**‘ ’**
Вых.	a	‘ ’	b	o	e	z	l	i	t	g	q	w	y	n

	0	1	2	3	4	5	6	7	8	9	10	11	12
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Вых.	m	h	j	s	v	k	c	f	p	r	u	x	d

	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Вх.	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**‘ ’**
Вых.	a	‘ ’	b	o	e	z	l	i	t	g	q	w	y	n

“itnu o**v**r**l**v” → “plain text” .

4. Полиподстановка

Пример 4. m=27, n=3;

	0	1	2	3	4	5	6	7	8	9	10	11	12
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Вых.1	n	p	g	m	r	h	w	b	u	c	f	t	a
Вых.2	r	t	c	u	a	z	‘ ’	w	b	y	x	v	s
Вых.3	s	a	t	v	u	b	w	y	c	‘ ’	x	d	z

	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Вх.	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**‘ ’**
Вых.1	‘ ’	q	i	x	j	d	v	k	e	y	l	z	s	o
Вых.2	l	o	q	i	p	n	h	d	j	m	e	k	g	f
Вых.3	r	m	l	k	e	p	f	n	q	g	o	h	i	j

plain **t**ex**t** → ivsuljv**a**o**v** ,

“ivsuljv**a**o**v**” → “plain text” .

Прямая таблица (отрывок)

	0	1	2	3	4	5	6	7	8	9	10	11	12	…
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	…
Вых.1	n	p	g	m	r	h	w	b	u	c	f	t	a	…
Вых.2	r	t	c	u	a	z	‘ ’	w	b	y	x	v	s	…
Вых.3	s	a	t	v	u	b	w	y	c	‘ ’	x	d	z	…

Обратная таблица (отрывок)

	0	1	2	3	4	5	6	7	8	9	10	11	12	…
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	…
Вых.1	m	h	j	s	v	k	c	f	p	r	u	x	d	…
Вых.2	e	i	c	u	x	‘ ’	z	t	q	v	y	n	w	…
Вых.3	b	f	i	l	r	t	w	y	z	‘ ’	q	p	o	…

	0	1	2	3	4	5	6	7	8	9	10	11	12
Вх.	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Вых.1	m	h	j	s	v	k	c	f	p	r	u	x	d
Вых.2	e	i	c	u	x	‘ ’	z	t	q	v	y	n	w
Вых.3	b	f	i	l	r	t	w	y	z	‘ ’	q	p	o

	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Вх.	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**‘ ’**
Вых.1	a	‘ ’	b	o	e	z	l	i	t	g	q	w	y	n
Вых.2	s	o	r	p	a	m	b	d	l	h	k	j	f	g
Вых.3	u	x	s	v	n	a	c	e	d	g	k	h	m	j

“ivsuljvaov” → “plain text” .

Домашнее задание (выполнить **до** п.з.№1)

1) Используя шифр ***двоичного гаммирования***, выполнить *расшифрование* заданной криптограммы ***C*** с использованием указанного ключа ***K***. И криптограмма и ключ заданы в виде последовательности байт в *шестнадцатеричной* системе счисления. Восстановленное исходное сообщение ***M*** необходимо представить *в таком же виде*.

C =12, 34, 56, 78, 9A, BC, DE, F0 ;

K = AC, EF, BD.

2) Используя шифр ***m-ичного гаммирования*** (с основанием алфавита m=27) с алфавитом, приведенным ранее в лекции, выполнить *расшифрование* заданной криптограммы ***C*** с использованием указанного ключа ***K*** (восстановить исходное сообщение M).

C =<ht ls**e**impkq> (l_C=11);

K =<vpemg**a**r” (l_K=7).

3) Используя шифр ***моно****подстановки* с ключом, приведенным ранее в лекции (со степенью подстановки m=27), выполнить *расшифрование* заданной криптограммы ***C*** (восстановить исходное сообщение *M*).

C = <**u** gqa**u** wo**v**rl**v**> (I_C=13).

4) Используя шифр ***поли**подстановки* с ключом, приведенным ранее в лекции (со степенью подстановки m=27, количеством выходных алфавитов n=3), выполнить *расшифрование* заданной криптограммы ***C*** (восстановить исходное сообщение *M*).

C =<u**l**b**q**pz<u>nhc</u>**q****l**> (I_C=11).