

# СЕТИ. БЕЗОПАСНОСТЬ

Урок 21 (F)

Прямые и функциональные методы  
кодирования



АНОНС

# Цели

- Знать принципы работы современных систем безопасности данных и их слабые места
- Уметь использовать на прикладном уровне современные инструменты криптографии и математические модели
- Уметь самостоятельно реализовывать криптоалгоритмы
- Получить алгоритмическую подготовку в вопросах анализа криптосистем

# Три кита

## **Кодирование**

Как записать, чтобы потом можно было прочитать

## **Шифрование**

Как записать, чтобы другие не могли прочитать

## **Стеганография**

Как записать, чтобы другие не нашли, ЧТО читать

# Содержание части

## Кодирование:

- Методы записи информации
- Методы изменения параметров информации, размеров, стойкости к повреждениям

## Шифрование:

- Алгоритмические особенности шифрования, наличие и анализ уязвимостей
- Реализация алгоритмов симметричного шифрования на основе алгоритма AES
- Математика ассиметричного шифрования, ЭЦП, сертификатов, на основе алгоритма RSA
- Устройство системы безопасности операционных систем

## Стеганография:

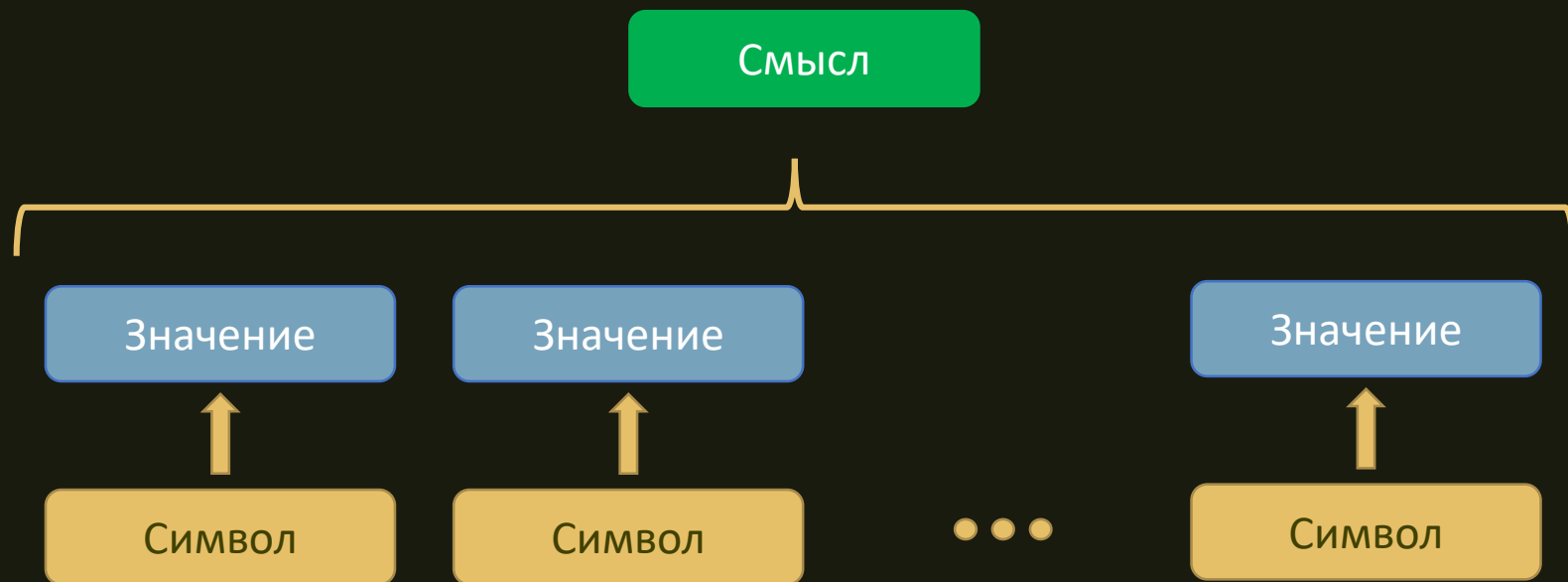
- Методы скрытого кодирования информации производными характеристиками
- Методы технического скрытия информации через коллизии функционала





Кодирование

# Лингвистика



# Кодирование







Привет, мир!

207 240 232 226 229 242 44 32 236 232 240 33



11001111 11110000 11101000 11100010 11100101 11110010 00101100 00100000 11101100 11101000 11110000 00100001

# ASCII 1251

Стандартная часть

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0				©	Е	§	Є	.		°						
1		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3		32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
4		48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
5		64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
6		80	81	82	83	84	85	86	87	88	89	90	91	92	93	94
7		96	97	98	99	100	101	102	103	104	105	106	107	108	109	110
8		112	113	114	115	116	117	118	119	120	121	122	123	124	125	126
9		128	129	130	131	132	133	134	135	136	137	138	139	140	141	142
A		144	145	146	147	148	149	150	151	152	153	154	155	156	157	158
B		160	161	162	163	164	165	166	167	168	169	170	171	172	173	174
C		176	177	178	179	180	181	182	183	184	185	186	187	188	189	190
D		192	193	194	195	196	197	198	199	200	201	202	203	204	205	206
E		208	209	210	211	212	213	214	215	216	217	218	219	220	221	222
F		224	225	226	227	228	229	230	231	232	233	234	235	236	237	238
		240	241	242	243	244	245	246	247	248	249	250	251	252	253	254

Национальная часть  
"Кодировка"

8	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
9	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
A	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
B	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
C	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
D	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
E	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц
F	Ѓ	Г	Г	Г	„	...	†	‡	‰	Љ	«	Њ	К	Ћ	Ц

# Асимметрия значений

Привет, мир!

207 240 232 226 229 242 44 32 236 232 240 33

ï ð è â å ò , ì è ð !

# Краткий список распространенных кодировок

- [ISO 646](#)
  - [ASCII](#)
- [BCDIC](#)
- [EBCDIC](#)
- [ISO 8859](#):
  - [ISO 8859-1](#), [ISO 8859-2](#), [ISO 8859-3](#), [ISO 8859-4](#), [ISO 8859-5](#), [ISO 8859-6](#), [ISO 8859-7](#), [ISO 8859-8](#), [ISO 8859-9](#), [ISO 8859-10](#), [ISO 8859-11](#), [ISO 8859-13](#), [ISO 8859-14](#), [ISO 8859-15](#)
  - [CP437](#), [CP737](#), [CP850](#), [CP852](#), [CP855](#), [CP857](#), [CP858](#), [CP860](#), [CP861](#), [CP863](#), [CP865](#), [CP866](#), [CP869](#)
- Кодировки [Microsoft Windows](#):
  - [Windows-1250](#) для языков Центральной Европы, которые используют латинское написание букв (польский, чешский, словацкий, венгерский, словенский, хорватский, румынский и албанский)
  - [Windows-1251](#) для кириллических алфавитов
  - [Windows-1252](#) для западных языков
  - [Windows-1253](#) для греческого языка
  - [Windows-1254](#) для турецкого языка
  - [Windows-1255](#) для иврита
  - [Windows-1256](#) для арабского языка
  - [Windows-1257](#) для балтийских языков
  - [Windows-1258](#) для вьетнамского языка
- [MacRoman](#), [MacCyrillic](#)
- [KOI8](#) (KOI8-R, KOI8-U...), [KOI-7](#)
- [Болгарская кодировка](#)
- [ISCII](#)
- [VISCII](#)
- [Big5](#) (наиболее знаменитый вариант Microsoft [CP950](#))
  - [HKSCS](#)
- [Guobiao](#)
  - [GB2312](#)
  - [GBK](#) (Microsoft [CP936](#))
  - [GB18030](#)
- [Shift JIS](#) для японского языка (Microsoft [CP932](#))
- [EUC-KR](#) для корейского языка (Microsoft [CP949](#))
- [ISO-2022](#) и [EUC](#) для [китайской письменности](#)
- Кодировки [UTF-8](#), [UTF-16](#) и [UTF-32](#) набора символов [Юникод](#)

# Unicode

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2500	—	—			…	…			…	…			⸀	⸁	⸂	⸃
2510	⸄	⸅	⸆	⸇	⸈	⸉	⸊	⸋	⸌	⸍	⸎	⸏	⸐	⸑	⸒	⸓
2520	⸔	⸕	⸖	⸗	⸘	⸙	⸚	⸛	⸜	⸝	⸞	⸟	⸠	⸡	⸢	⸣
2530	⸤	⸥	⸦	⸧	⸩	⸪	⸫	⸬	⸭	⸮	ⸯ	⸰	⸱	⸲	⸳	⸴
2540	⸵	⸶	⸷	⸸	⸹	⸺	⸻	⸼	⸽	⸾	⸿	⹀	⹁	⹂	⹃	⹄
2550	=		ƒ	π	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ	ƒ
2560	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2570	⸴	/	\	X	-	-	-	-	-	-	-	-	-	-	-	-

[unicode-table.com](https://unicode-table.com)

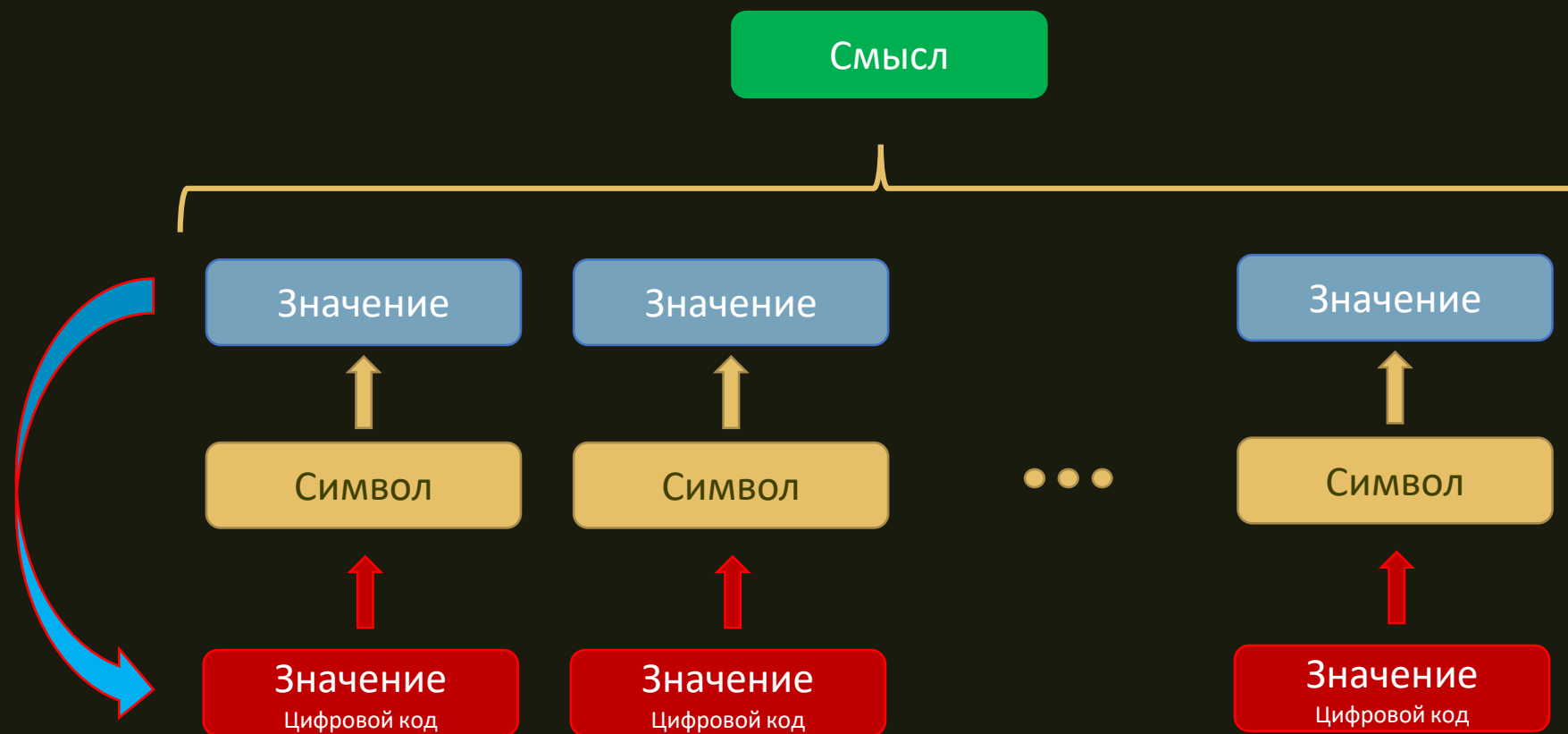
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2500	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2510	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2520	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2530	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2540	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2550	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2560	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴
2570	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴	⸴

LangBox ISO-8859-6-16 Fontset (221 Arabic glyphs)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0				٠	@	ذ	-			ء	آ	ط	ظ	خ	ك	ي
1			ا	١	ء	ر	ف	ء		ء	آ	س	ط	س	ك	ا
2			"	٢	آ	ز	ق	ء		ء	آ	س	ط	س	ك	ا
3			#	٣	أ	ك	س	ء		ء	آ	س	ط	س	ك	ا
4			\$	٤	ؤ	ل	ش	ء		ء	آ	س	ط	س	ك	ا
5			%	٥	إ	ص	م	ء		ء	آ	س	ط	س	ك	ا
6			&	٦	ئ	ن	ض	ء		ء	آ	س	ط	س	ك	ا
7			'	٧	ا	ط	ه	ء		ء	آ	س	ط	س	ك	ا
8			)	٨	ظ	ب	ل	ء		ء	آ	س	ط	س	ك	ا
9			(	٩	ة	ع	ي	ء		ء	آ	س	ط	س	ك	ا
A			*	:	:	غ	ت	ء		ء	آ	س	ط	س	ك	ا
B			+	:	:	ث	ء	ء		ء	آ	س	ط	س	ك	ا
C			,	>	ج	\	ء			ء	آ	س	ط	س	ك	ا
D			-	=	ح	[	ء	{		ء	آ	س	ط	س	ك	ا
E			.	<	خ	^	ء	~		ء	آ	س	ط	س	ك	ا
F			/	؛	د	—	ء			ء	آ	س	ط	س	ك	ا

(C) LangBox International

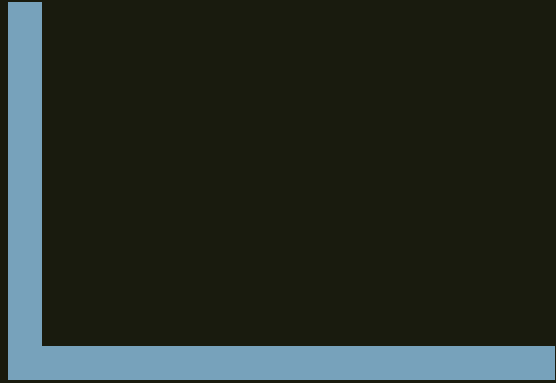

# Многоуровневость



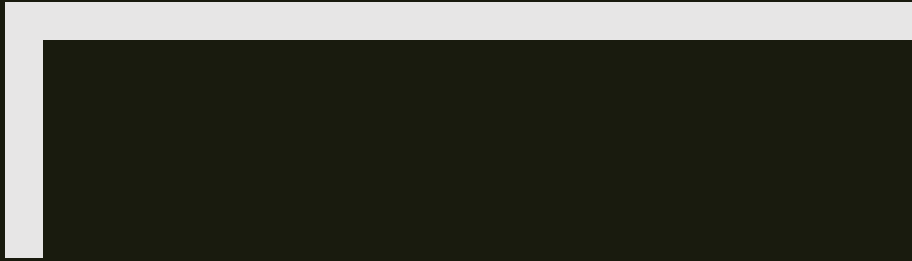
# Дзен

34 38 34 38 34 39 34 39 34 38 34 38 34 38 34 38 34 38 34 39 34 39 34 38 34 38 34  
38 34 38 34 38 34 38 34 39 34 39 34 38 34 38 34 38 34 39 34 38 34 39 34 39 34  
38 34 38 34 38 34 39 34 38 34 38 34 39 34 39 34 38 34 38 34 38 34 38 34 38 34  
39 34 39 34 38 34 38 34 38 34 38 34 38 34 38 34 39 34 39 34 38 34 38 34 38 34  
38 34 38 34 39 34 39 34 38 34 38 34 38 34 38 ...





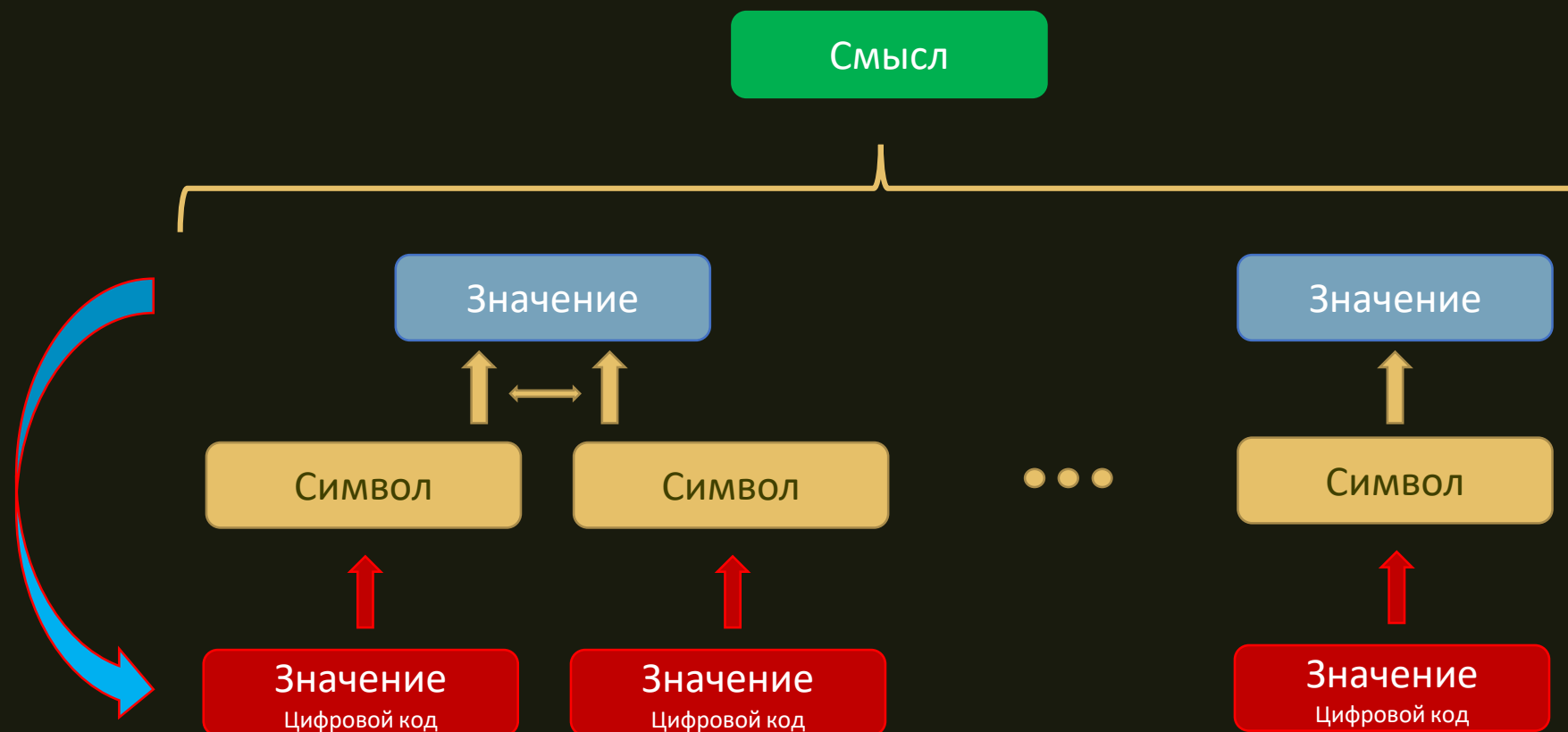
0	1	2	3	4	5
○	㉑	㉒	㉓	㉔	㉕
.	।	२	३	४	५
○	㊸	㊹	3	㊼	㊽
○	一	二	三	四	五

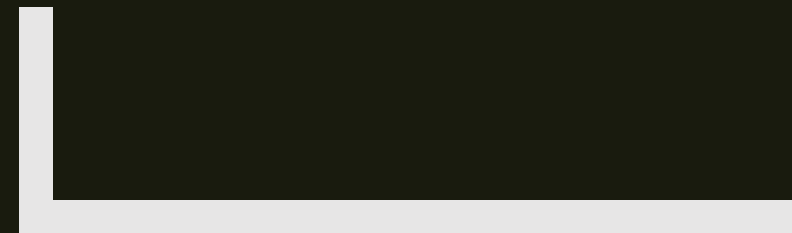


0	1	2	3	4	5
○	㉑	㉒	㉓	㉔	㉕
.	一	二	三	四	五
○	㉖	㉗	㉘	㉙	㉚
○	一	二	三	四	五



# Взаимосвязь

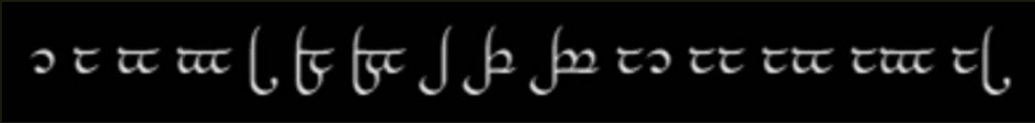




零一 二 三 四 五 六 七 八 九 十

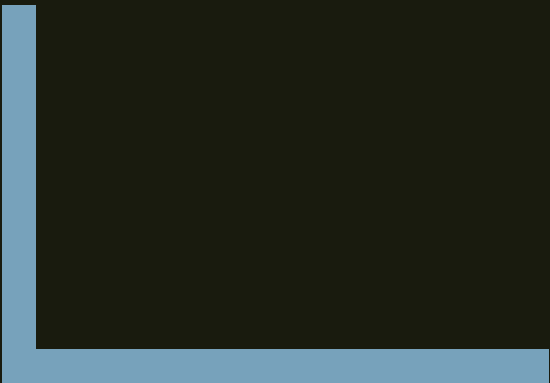
二十      十二      二十二

China

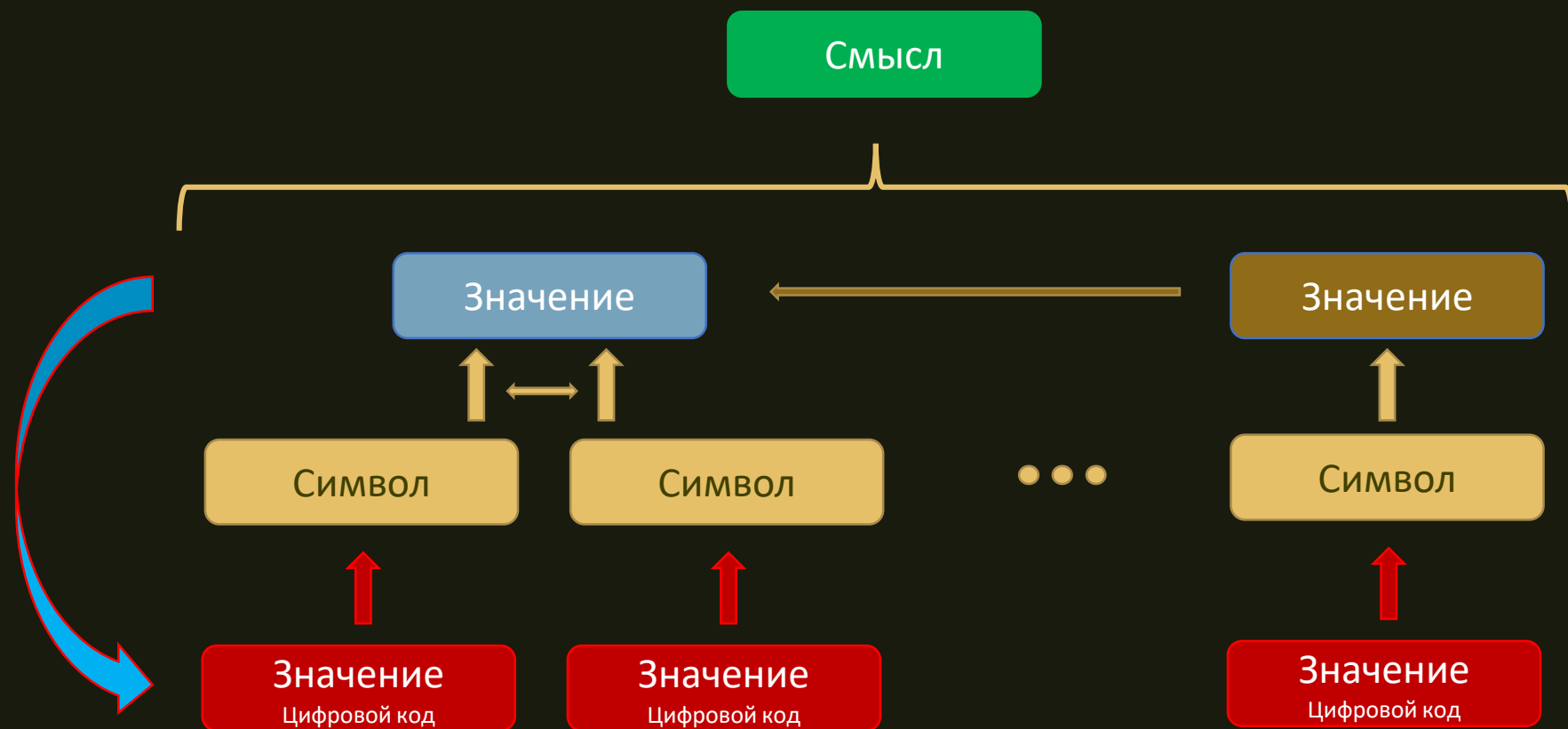


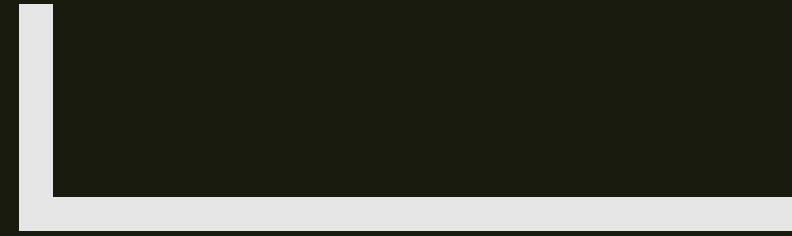
ττ τς ττ

# Elfian Sindarin



# Коррекция





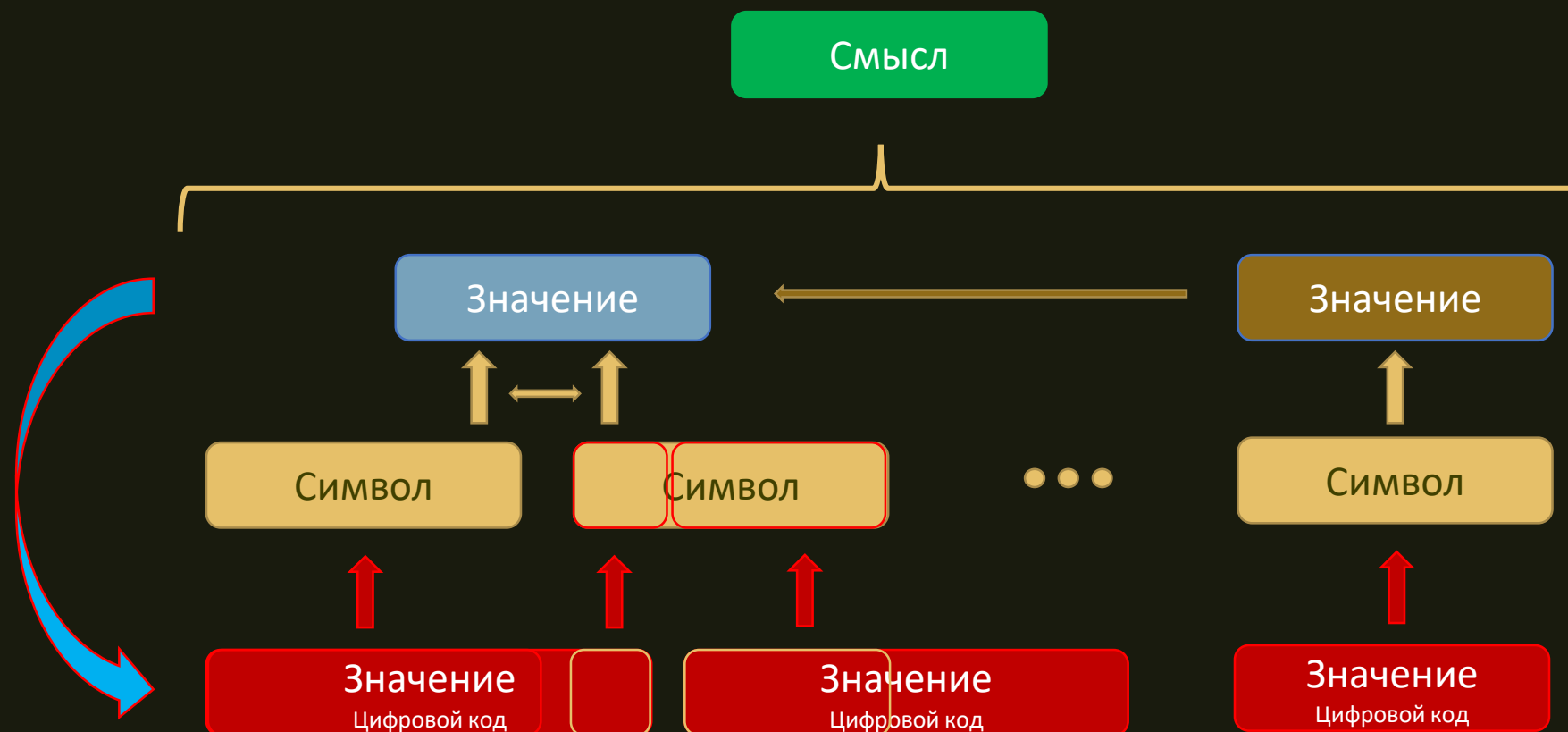
# Braille



----- \*----- \*\*----- \*\*\*-- \*\*\*\*\*\_ \*\*\*\*\*  
\_\*\*\*\* \_\*\*\*\* \_\*\* \_-\* \*\_-----

Morze

# Нарушение кратности





# Блочное кодирование



Base 64

АБВГД



# Base 64

АБВГД

11000000 11000001 11000010 11000011 11000100 (00000000)

Base 64

АБВГД

**110000**00 11000001 11000010 11000011 11000100 (00000000)

# Base 64

АБВГД

**110000**00 11000001 11000010 11000011 11000100 (00000000)

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/  
0.... ...**[48]** ....

**w**.....



# Base 64

АБВГД

11000000011000001 11000010 11000011 11000100 (00000000)

ABCDEFGHIJKL**M**NOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/  
0.... ...**[12]** ....

w**M**.....

# Base 64

АБВГД

11000000 11000001 11000010 11000011 11000100 (00000000)

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

wMHCw8Q

# Base 64

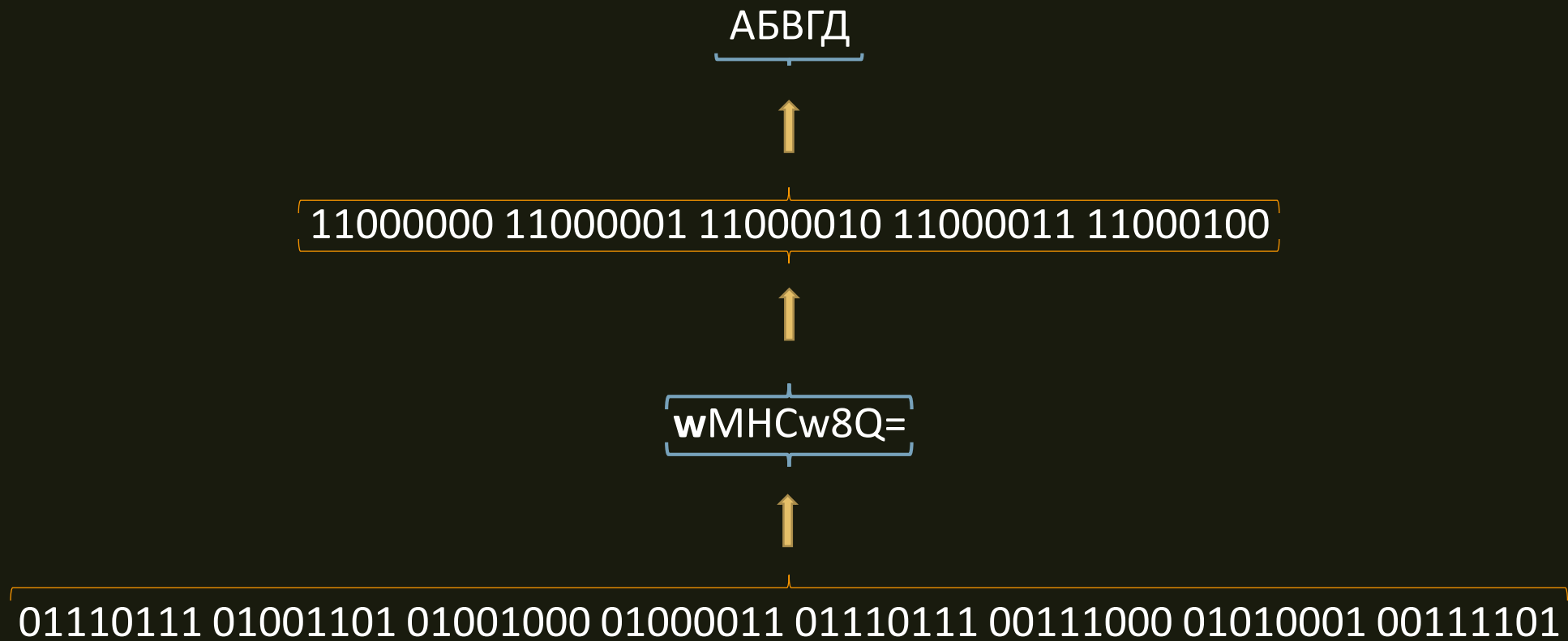
АБВГД

11000000 11000001 11000010 11000011 11000100 (00000000)

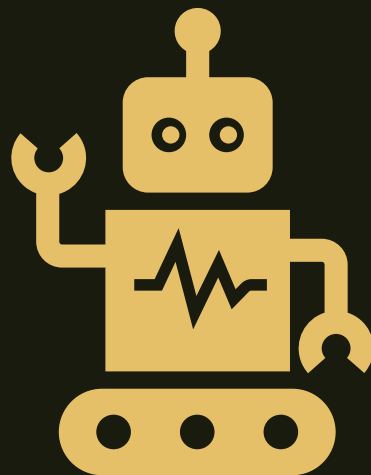
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-

wMHCw8Q=

# Два уровня кодирования



# Практика





Функциональное кодирование

# Функциональное кодирование

## Задачи:

- Сужение/расширение алфавита
  - Гарантия доставки
  - Гарантия декодирования
  - Изменение количества используемых кодов/символов
- Сжатие кода
  - Уменьшение и оптимизация длины записи
- Защита кода от помех
  - Обнаружение и восстановление кода в случаях возникновения повреждений





Кодирование длин серий (RLE)



RLE

11000111 11111011 00100001

11 000 11111111 0 11 00 1 0000 1




RLE

11000111 11111011 00100001

11 000 11111111 0 11 00 1 0000 1

2:1 3:0 8:1 1:0 2:1 2:0 1:1 4:0 1:1



# RLE

11000111 11111011 00100001

11 000 11111111 0 11 00 1 0000 1

2:1 3:0 8:1 1:0 2:1 2:0 1:1 4:0 1:1

2:1 3:0 8:1 1:0 2:1 2:0 1:1 4:0 1:1


2:1 3:0 8:1 1:0 2:1 2:0 1:1 4:0 1:1

RLE

2:1 3:0 8:1 1:0 2:1 2:0 1:1 4:0 1:1

1: 2 3 8 1 2 2 1 4 1

# RLE



2:1 3:0 8:1 1:0 2:1 2:0 1:1 4:0 1:1

1: 2 3 8 1 2 2 1 4 1

1: 10 11 1000 1 10 10 1 100 1





Гамма-коды Эллиоса

# Гамма-код

Число	Кодирование
1	1
2	0 10
3	0 11
4	00 100
5	00 101
6	00 110
7	00 111
8	000 1000
9	000 1001



# Гамма-код Эллиоса

1: 10 11 1000 1 10 10 1 100 1

1: 010 011 0001000 1 010 010 1 00100 1

# Гамма-код Эллиоса

1: 10 11 1000 1 10 10 1 100 1

1: 010 011 0001000 1 010 010 1 00100 1

1010011000100010100101001001



# Декодирование

1010 0110 0010 0010 1001 0100 1001



# Выделение первого бита

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

# Выделение ведущих нулей

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

1: 010 011 0001000 1 010 010 1 00100 1

# Удаление ведущих нулей

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

1: 010 011 0001000 1 010 010 1 00100 1

1: 10 11 1000 1 10 10 1 100 1

# Перевод в актуальную систему счисления

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

1: 010 011 0001000 1 010 010 1 00100 1

1: 10 11 1000 1 10 10 1 100 1

1: 2 3 8 1 2 2 1 4 1

# Декодирование RLE

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

1: 010 011 0001000 1 010 010 1 00100 1

1: 10 11 1000 1 10 10 1 100 1

1: 2 3 8 1 2 2 1 4 1

11 000 11111111 0 11 00 1 0000 1



# Группировка по 4 бита и перевод в A16

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

1: 010 011 0001000 1 010 010 1 00100 1

1: 10 11 1000 1 10 10 1 100 1

1: 2 3 8 1 2 2 1 4 1

11 000 11111111 0 11 00 1 0000 1

1100 0111 1111 1011 0010 0001

C7 FB 21

# Перевод по ASCII1251

1010 0110 0010 0010 1001 0100 1001

1: 010 0110 0010 0010 1001 0100 1001

1: 010 011 0001000 1 010 010 1 00100 1

1: 10 11 1000 1 10 10 1 100 1

1: 2 3 8 1 2 2 1 4 1

11 000 11111111 0 11 00 1 0000 1

1100 0111 1111 1011 0010 0001

C7 FB 21

Зы!



# Декодирование

1010 0100 1110 1111 0101 0101 1101 01

...

Ой)



# Практика

