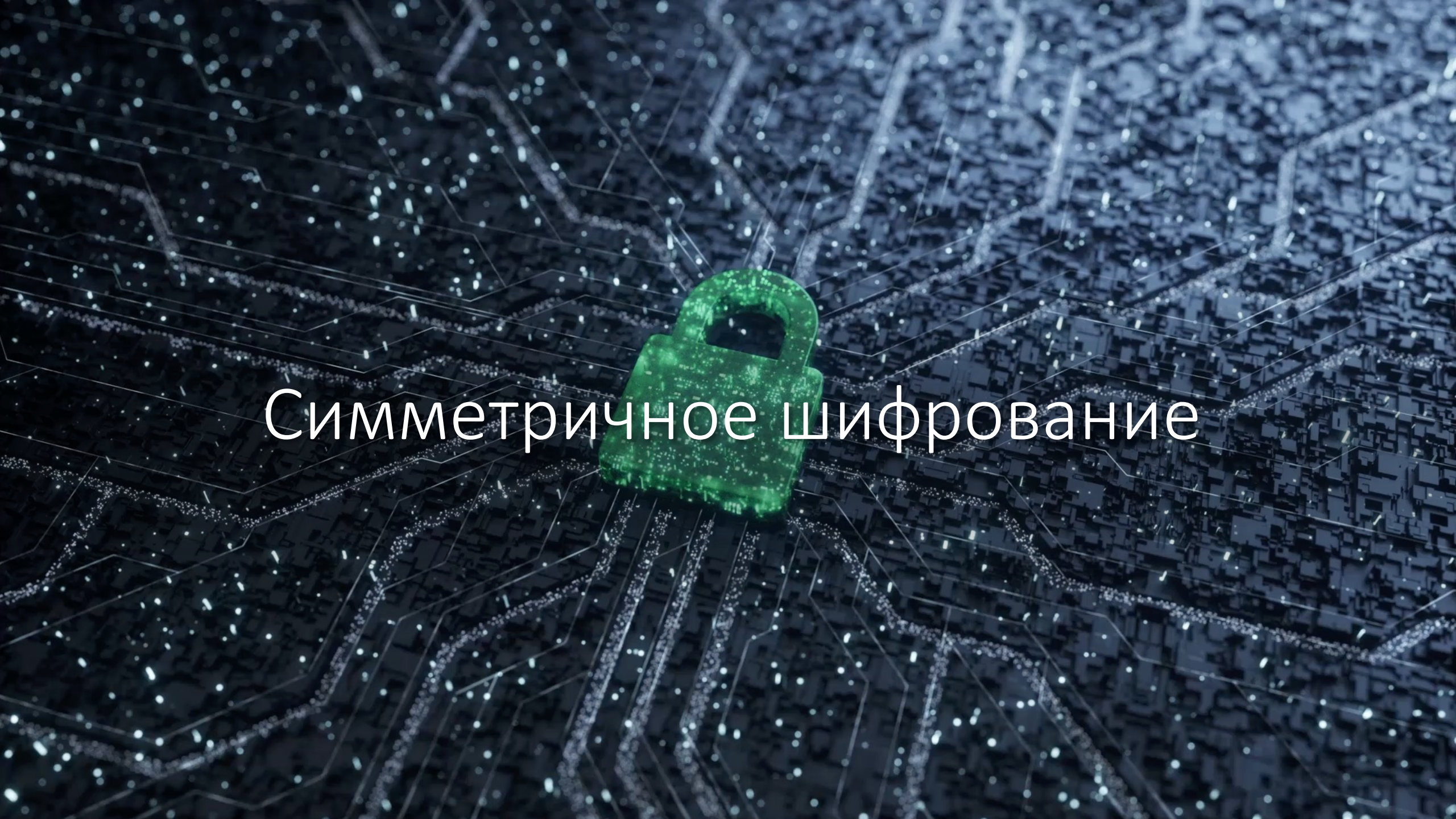
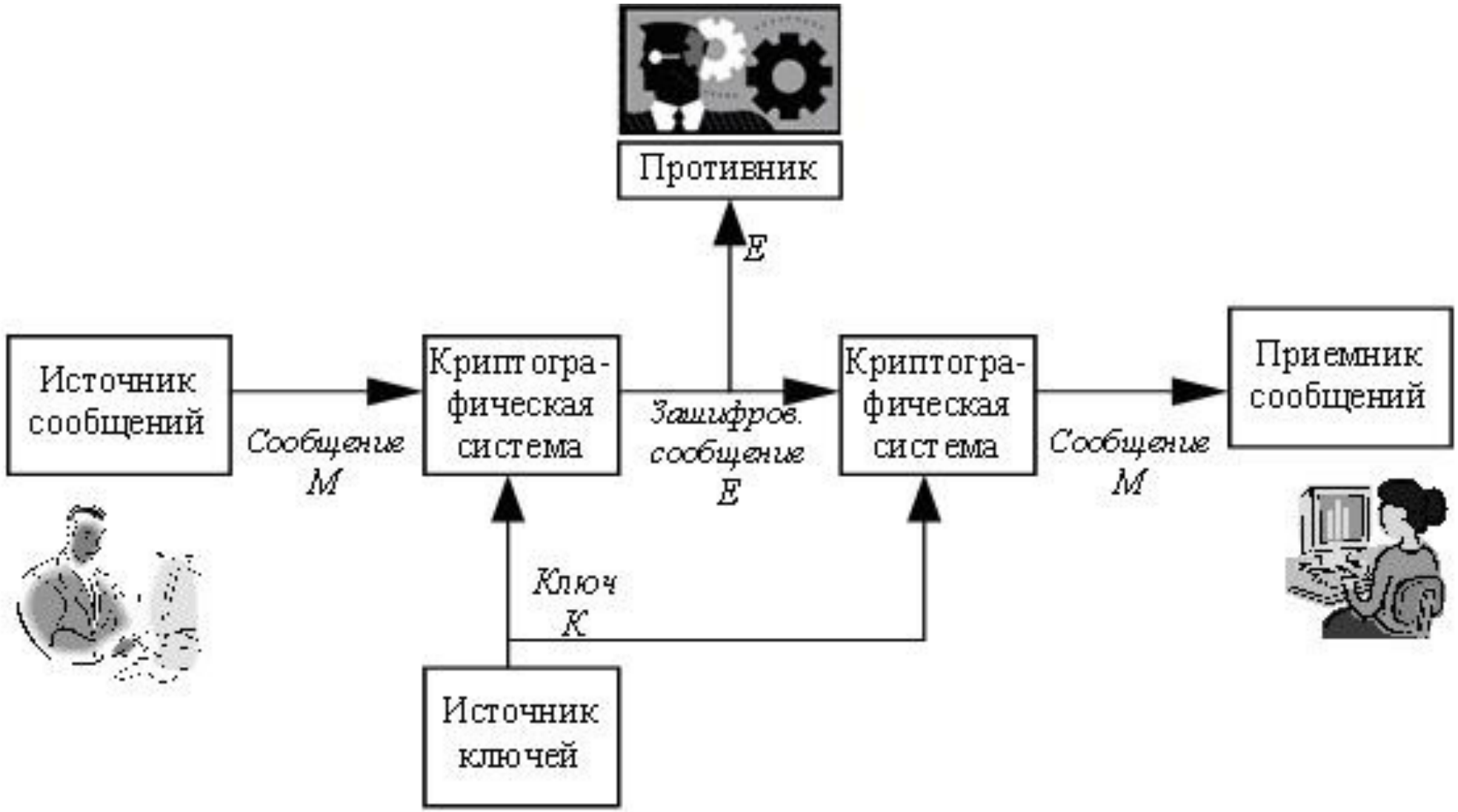
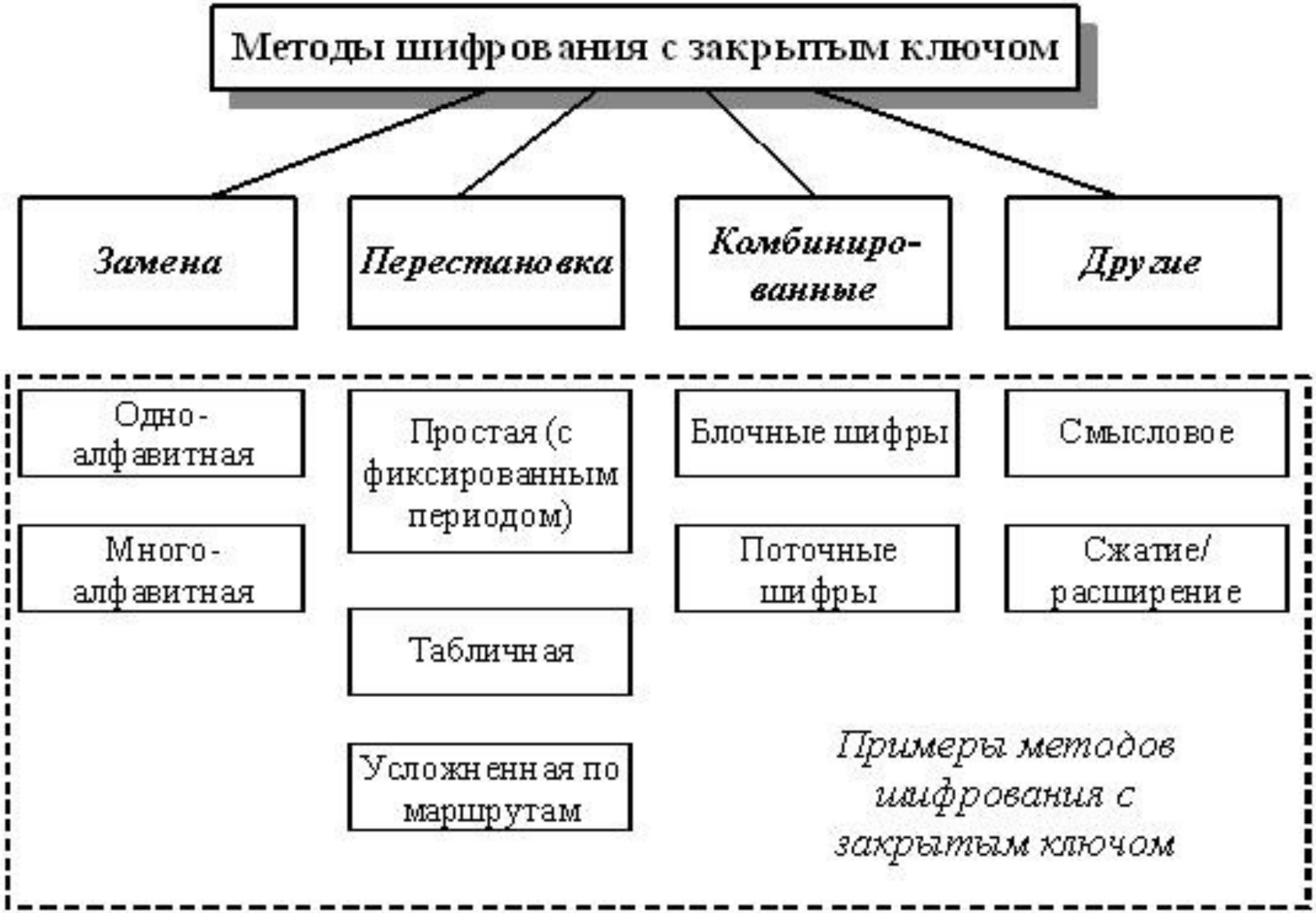


Симметричное шифрование

Общая схема симметричного шифрования



Методы замены


Методы шифрования с закрытым ключом
Замена
Перестановка
Комбиниро-ванные
Другие
Одно-алфавитная
Много-алфавитная
Простая (с фиксированным периодом)
Табличная
Усложненная по маршрутам
Блочные шифры
Поточные шифры
Смысловое
Сжатие/ расширение
Примеры методов шифрования с закрытым ключом

Методы замены

Методы шифрования заменой (подстановкой) основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

Одноалфавитная замена

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	Σ
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Открытое сообщение																			
В	Ы	Ш	Л	И	Т	Е		П	О	Д	К	Р	Е	П	Л	Е	Н	И	Е
Зашифрованное сообщение с использованием шифра 1																			
О	Н	У	Р	Ъ	Х	П	Ф	Ж	.	Щ		Г	П	Ж	Р	П	Ц	Ъ	П
Зашифрованное сообщение с использованием шифра 2																			
)	⊕	▽	♠	*	%	>	∞	=	-	<	♥	(	>	=	♠	>	#	*	>

ТНФЖ.ИПЩЪРЪ

Зашифрованное сообщение										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ
После замены Ъ на О										
								О		О
После замены Ъ на А										
								А		А
После замены Ъ на И										
								И		И
После замены Ъ на Е										
								Е		Е

ТНФЖ.ИПЩЪРЪ

Зашифрованное сообщение										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ
Варианты подобранных дешифрованных сообщений										
Ж	Д	И		С	У	М	Р	А	К	А
Д	Ж	О	Н	А		У	Б	И	Л	И
В	С	Е	Х		П	О	Б	И	Л	И
М	Ы		П	О	Б	Е	Д	И	Л	И

Пример таблицы замен для двухбуквенных сочетаний

Откр. текст	Зашифр. текст	Откр. текст	Зашифр. текст
аа	кх	бб	пш
аб	пу	бв	вь
ав	жа	...	...
...	...	яэ	сы
ая	ис	яю	ек

Пропорциональные шифры

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035…

В этом случае сообщение

БОЛЬШОЙ СЕКРЕТ

может быть зашифровано следующим образом:

10175713256210321376275180076175413413075 9

Многоалфавитные подстановки

В целях маскирования естественной частотной статистики исходного языка применяется многоалфавитная подстановка, которая также бывает нескольких видов. В **многоалфавитных подстановках** для замены символов исходного текста используется не один, а несколько алфавитов. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке.
Примером многоалфавитной подстановки может служить схема, основанная на использовании таблицы Вижинера. Этот метод, известный уже в XVI веке, был описан французом Блезом Вижинером в "Трактате о шифрах", вышедшем в 1585 году.

Таблица Виженера

Исходное сообщение:

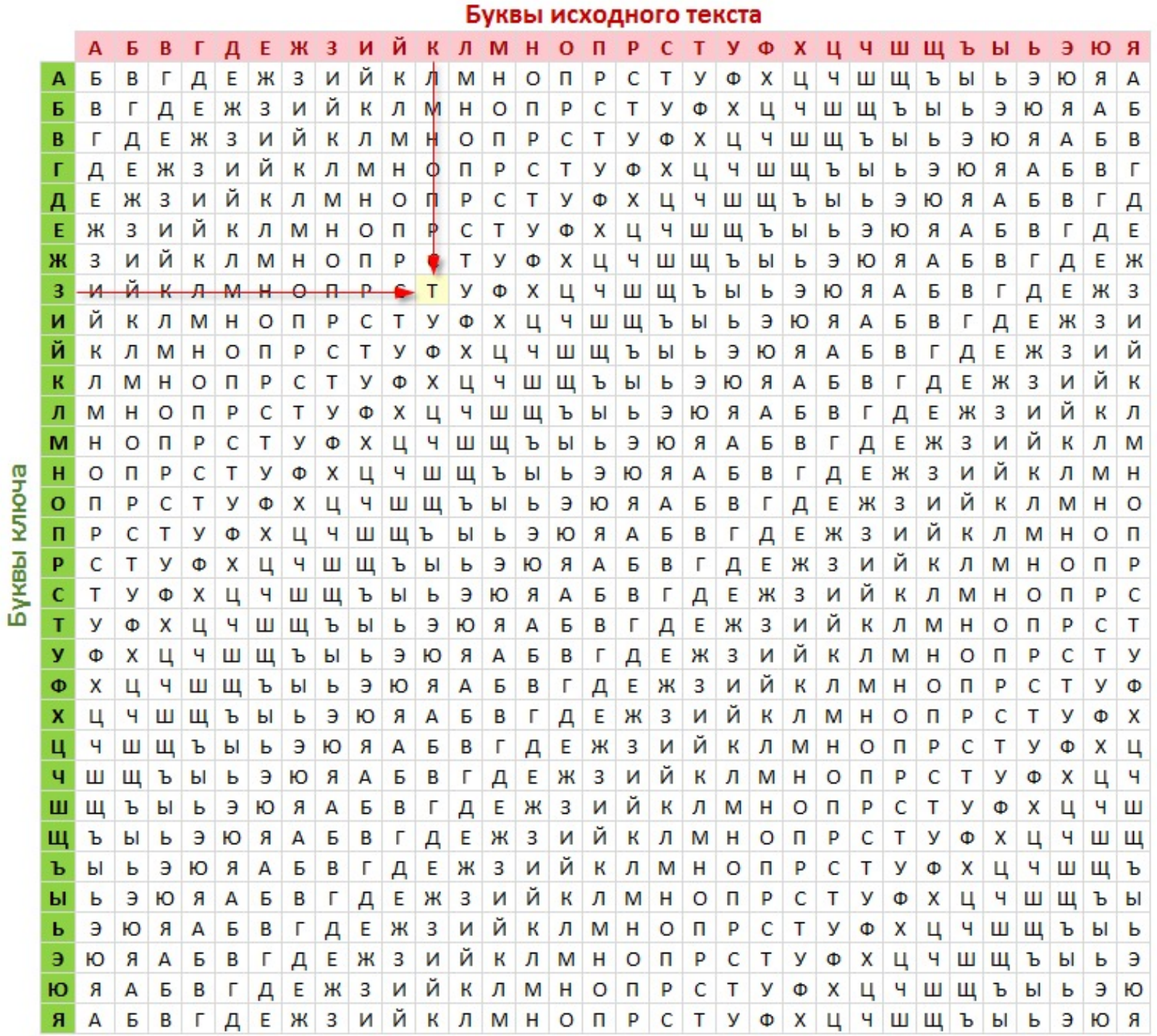
Школа

Ключ:

Класс

Шифртекст:

Гцпэт



Методы гаммирования

Еще одним частным случаем многоалфавитной подстановки является **гаммирование**. В этом способе шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Если в исходном алфавите, например, 33 символа, то сложение производится по модулю 33. Такой процесс сложения исходного текста и ключа называется в криптографии *наложением гаммы*.

0 (А) до 32 (Я)

исходный символ - x
Ключ – k

$$z = x + k \pmod{N},$$

z – закодированный символ
N - количество символов в алфавите

Г (3) и Ю (31) :

$$3 + 31 \pmod{33} = 1,$$

Б (1)

Двоичное гаммирование

$$z = x + k(mod2) = x \oplus k.$$

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

X – м (10)
К – к (12)

$14_{(10)}=1110_{(2)}$, $12_{(10)}=1100_{(2)}$

Сложим по модулю два двоичные числа 1110 и 1100 :

Исходное число 1 1 1 0

Гамма 1 1 0 0

Результат 0 0 1 0

Зашифрованное число 0 0 1 0

Гамма 1 1 0 0

Результат 1 1 1 0