Всероссийская научно-образовательная школа
"Квантовый скачок"

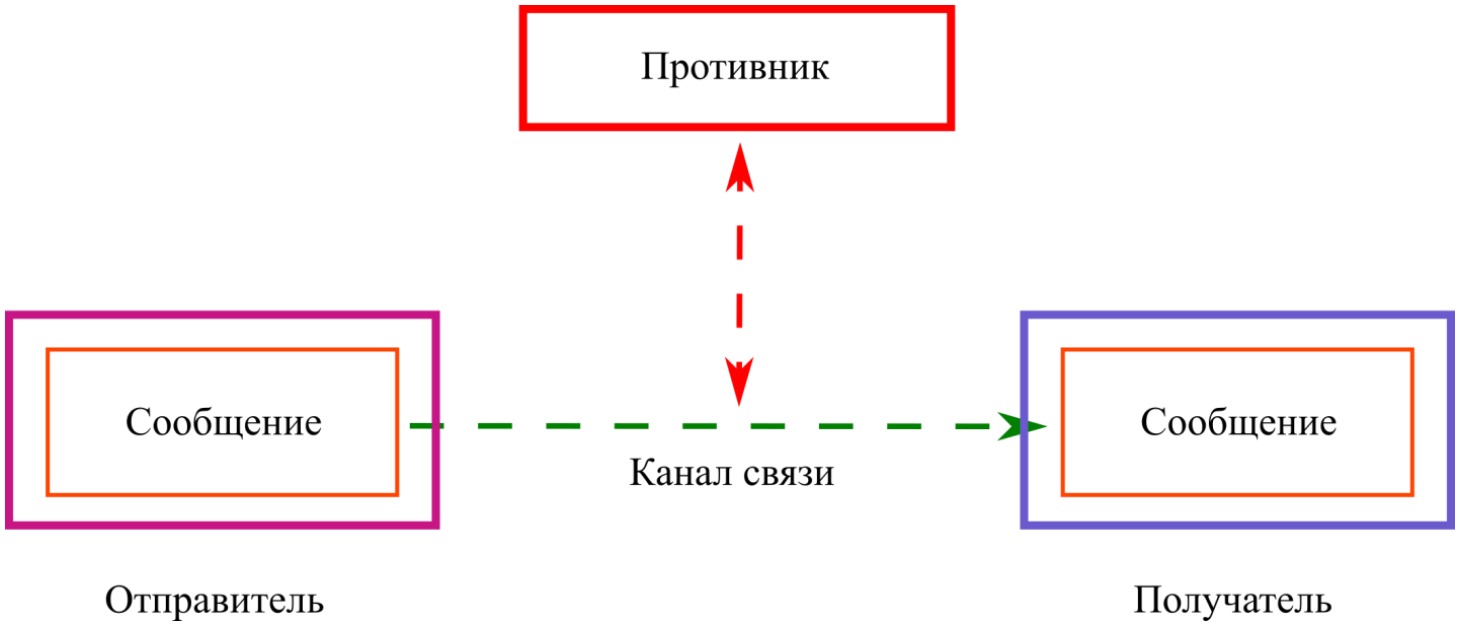
Информационная безопасность: переход к квантовой криптографии

Каширский Данила Евгеньевич
канд. физ.-мат. наук
доцент каф. квантовой электроники и фотоники
ст. научн. сотр. лаб. квантовых информационных технологий
e-mail: kde@mail.tsu.ru

Содержание

Задача секретной передачи информации

- Предположим, что **отправитель** хочет послать сообщение **получателю**, причем, сделать это безопасно: он хочет быть уверен, что перехвативший это сообщение не сможет его прочесть. По сложившейся традиции первого участника данного процесса (отправителя) принято называть Алисой, а второго участника (получателя) – Бобом. Третьего участника (противника) – Евой.



Какими способами можно передать информацию секретно?

Задача секретной передачи информации

Задача передачи важной информации определенному адресату в тайне от всех остальных может быть решена, в общем случае, тремя способами:

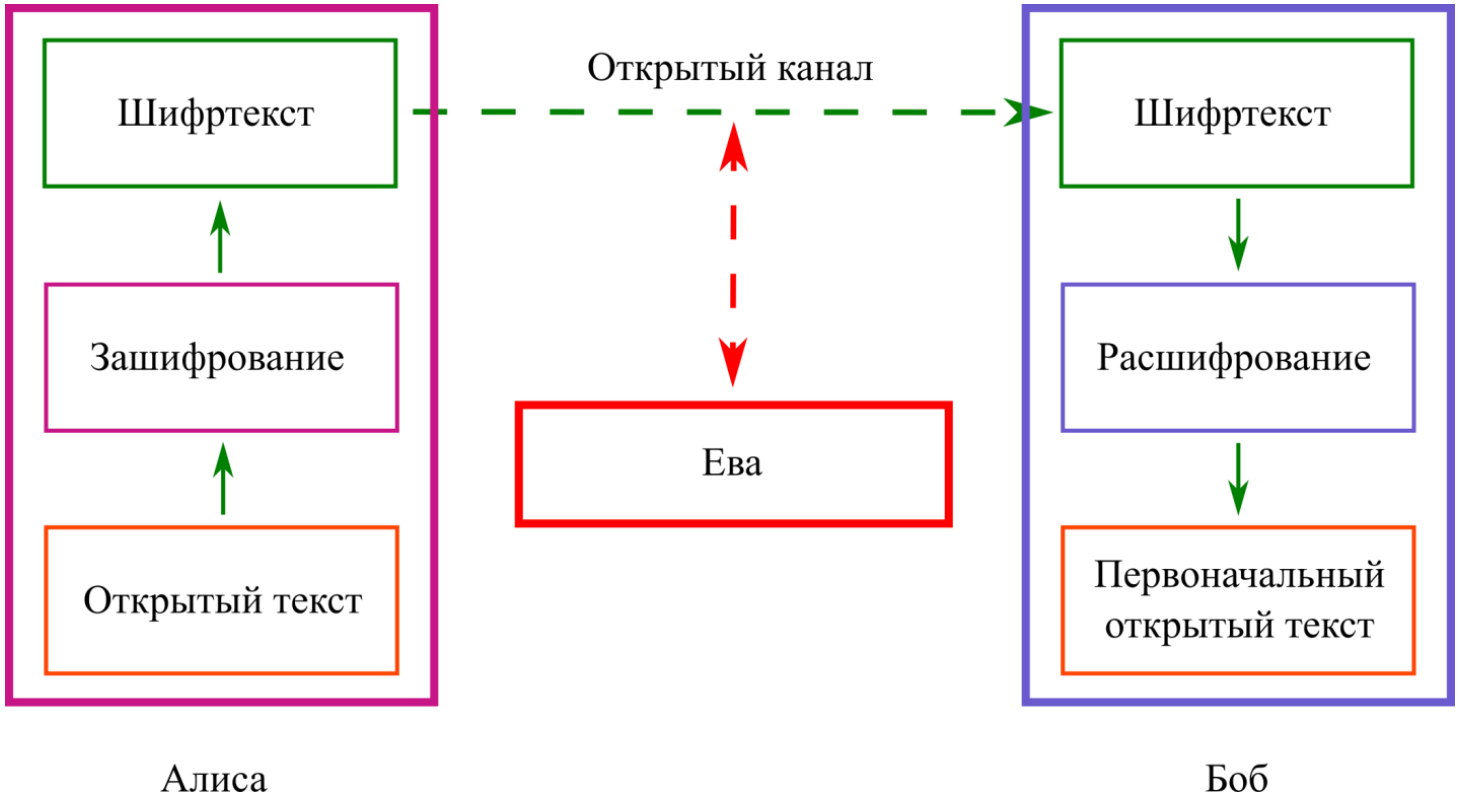
1. За счет создания абсолютно надежного канала передачи информации между адресатами.

2. За счет сокрытия самого факта передачи информации. Такой подход получил достаточно широкое распространение и является предметом изучения *стеганографии* (от греч. στεγανός «скрытый» + γράφω «пишу»; букв. «тайнопись»).

3. За счет преобразования информации таким образом, чтобы восстановить ее мог только законный получатель.

Задача секретной передачи информации

- **Криптография** (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») - искусство и наука сокрытия сообщений для обеспечения секретности передаваемой информации.
- Тех, кто воплощает в жизнь криптографию, называют **криптографами**



Шифры

Корни криптографии находятся в римской и египетской цивилизациях.

Около 4000 лет назад египтяне общались посредством сообщений, написанных иероглифами. Этот код был секретом, известным только писцам, которые передавали сообщения от имени королей.

Шифры

- Позже перешли к использованию простых моно-буквенных шифров замещения. Это включало замену алфавитов сообщения другими алфавитами с каким-то секретным правилом. Зная этот секрет, можно извлечь исходное сообщение из искаженного сообщения.

A ●−
B −●●●
C −●−●
D −●●
E ●
F ●●−●
G −−●
H ●●●●
I ●●

J ●−−−
K −●−
L ●−●●
M −−
N −●
O −−−
P ●−−●
Q −−●−
R ●−●

S ●●●
T −
U ●●−
V ●●●−
W ●−−
X −●●−
Y −●−−
Z −−●●

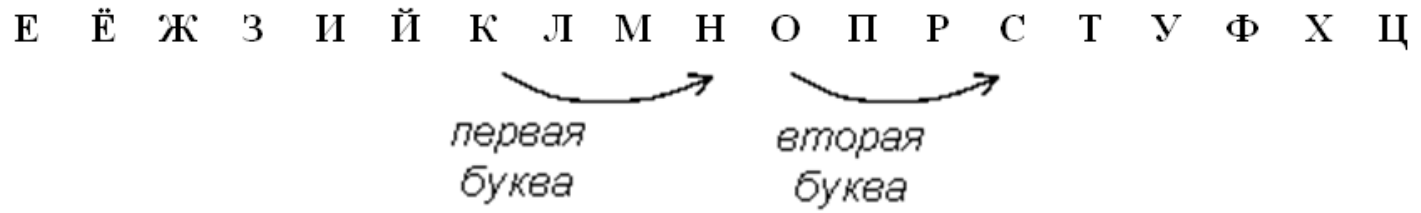
Исходный текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Исходный текст	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Зашифрованный текст	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	А

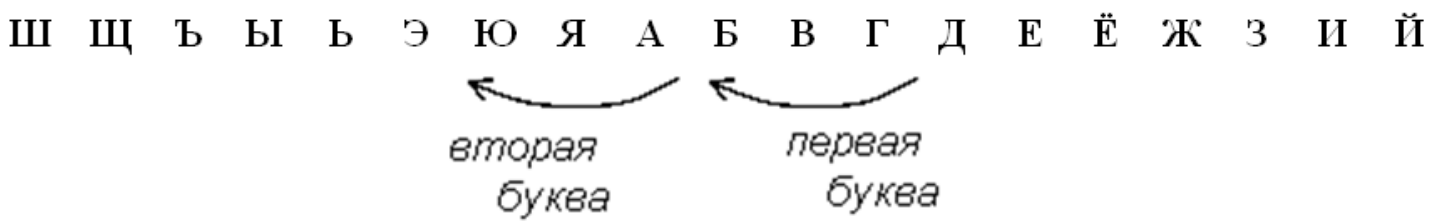
Исходный текст	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Зашифрованный текст	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Шифр Цезаря

а



б



Шифр Цезаря

Алфавит «Русские буквы» (33 символа)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х

24	25	26	27	28	29	30	31	32	33
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

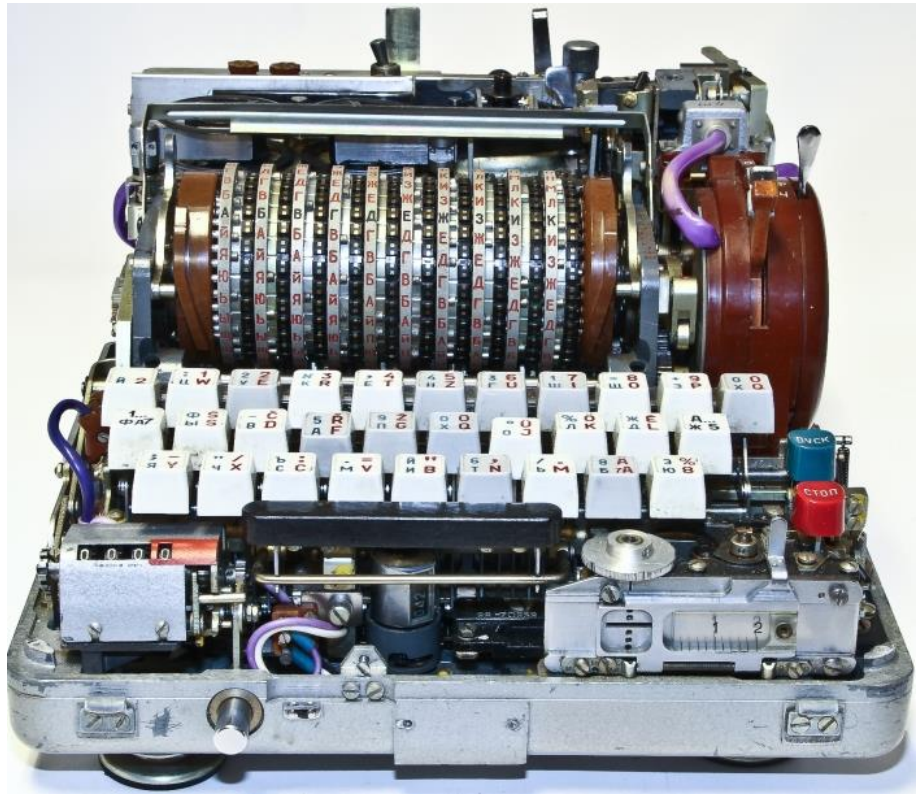
Задание 1. Используя русский алфавит из 33 букв , зашифруйте слово **КЛЮЧ** классическим шифром Цезаря со сдвигом на три.

Задание 2. Используя русский алфавит из 33 букв, дешифрируйте сообщение **СДУГХРГВФЕВКЯ**, зашифрованное классическим шифром Цезаря со сдвигом на три.

Шифртехника

- В криптографии **скитала** (или *сцитала* от греческого *σκυτάλη*, жезл), известный также как *шифр Древней Спарты*, представляет собой прибор, используемый для осуществления перестановочного шифрования, состоит из цилиндра и узкой полоски пергамента, обматывавшейся вокруг него по спирали, на которой писалось сообщение. Античные греки и спартанцы в частности, использовали этот шифр для связи во время военных кампаний.

Шифртехника



Шифровальная машина Энигма

Немецкая шифровальная машина Лоренца

Алгоритмы ограниченного использования

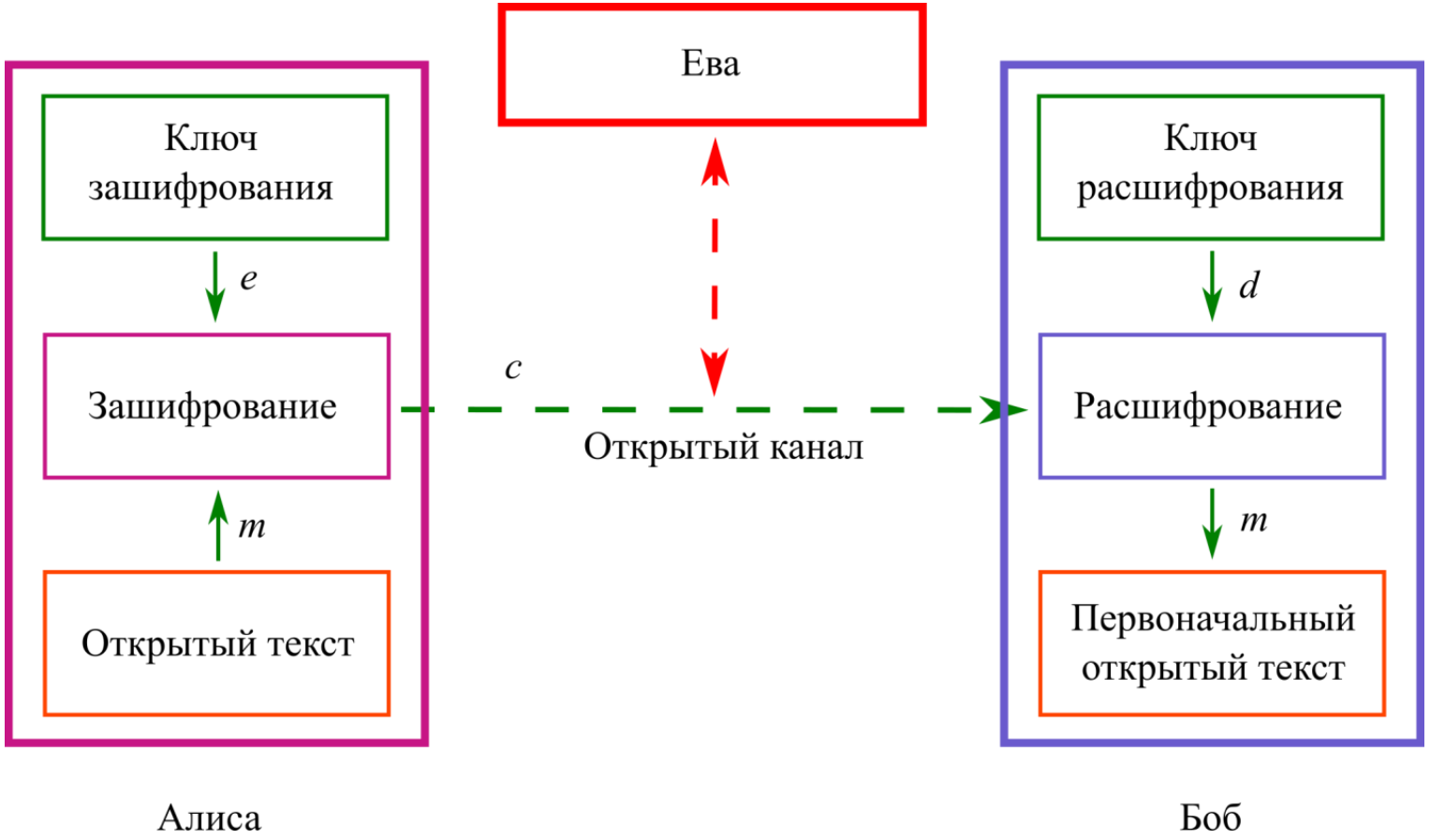
- **Алгоритмом ограниченного использования** называется алгоритм, безопасность которого основана на сохранении самого алгоритма в тайне. Такие алгоритмы совершенно не соответствуют используемым стандартам в настоящее время. Они представляют сугубо исторический интерес.

Почему отказались от использования таких алгоритмов?

Алгоритмы общего использования

- В основе **алгоритмов общего использования** лежит **принцип Керкгоффса**, сформулированный в XIX веке голландским криптографом Огюстом Керкгоффсом, согласно которому в засекреченном виде держится только определенный набор параметров алгоритма, называемый **ключом**, а сам алгоритм шифрования должен быть открытым. Безопасность таких шифров полностью основана на ключах, а не на деталях алгоритмов.

Шифрование с ключами



Одноразовый блокнот - абсолютная секретность информации

Одноразовым блокнотом называют криптосистему, при создании которой соблюдены следующие требования:

1. Используется истинно случайный секретный ключ, известный в простейшем случае двум сторонам.

2. Ключ равен длине сообщения.

3. Ключ используется при зашифровании, для чего объединяется с открытым текстом при помощи легкообратимой функции. Для расшифрования другая сторона использует этот же ключ для проведения над шифртекстом обратного преобразования, приводящего к получению открытого текста.

4. Ключ используется только один раз, после чего должен быть по возможности уничтожен или по крайней мере должны быть предприняты меры, предотвращающие его повторное использование.

Одноразовый блокнот - абсолютная секретность информации

Одноразовым блокнотом называют криптосистему, при создании которой соблюдены следующие требования:

1. Используется истинно случайный секретный ключ, известный в простейшем случае двум сторонам.

2. Ключ равен длине сообщения.

3. Ключ используется при зашифровании, для чего объединяется с открытым текстом при помощи легкообратимой функции. Для расшифрования другая сторона использует этот же ключ для проведения над шифртекстом обратного преобразования, приводящего к получению открытого текста.

4. Ключ используется только один раз, после чего должен быть по возможности уничтожен или по крайней мере должны быть предприняты меры, предотвращающие его повторное использование.

Шифр Вернами

- Рассмотрим пример шифрования с помощью одноразового блокнота. Пусть Алиса хочет передать Бобу сообщение «ТЕСТ». Алиса заменяет символы сообщения их бинарным представлением, которое получается путем перевода номеров символов из десятичной системы счисления в двоичную систему счисления.

Символ	Номер	Бинарное представление					
А	0	0	0	0	0	0	0
Б	1	0	0	0	0	0	1
В	2	0	0	0	0	1	0
Г	3	0	0	0	0	1	1
Д	4	0	0	0	1	0	0
Е	5	0	0	0	1	0	1
Ё	6	0	0	0	1	1	0
Ж	7	0	0	0	1	1	1
З	8	0	0	1	0	0	0
И	9	0	0	1	0	0	1
Й	10	0	0	1	0	1	0
К	11	0	0	1	0	1	1
Л	12	0	0	1	1	0	0
М	13	0	0	1	1	0	1
Н	14	0	0	1	1	1	0
О	15	0	0	1	1	1	1
П	16	0	1	0	0	0	0
Р	17	0	1	0	0	0	1
С	18	0	1	0	0	1	0
Т	19	0	1	0	0	1	1
У	20	0	1	0	1	0	0
Ф	21	0	1	0	1	0	1
Х	22	0	1	0	1	1	0
Ц	23	0	1	0	1	1	1
Ч	24	0	1	1	0	0	0
Ш	25	0	1	1	0	0	1
Щ	26	0	1	1	0	1	0
Ъ	27	0	1	1	0	1	1
Ы	28	0	1	1	1	0	0
Ь	29	0	1	1	1	0	1
Э	30	0	1	1	1	1	0
Ю	31	0	1	1	1	1	1
Я	32	1	0	0	0	0	0

Шифр Вернами

Руководствуясь таблицей, Алиса получает бинарное представление «ТЕСТ». Далее Алисе необходимо объединить сообщение с ключом. Это производится путем применения операции сложения по модулю два (XOR), которая выполняется следующим образом:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Шифр Вернами

- В результате этой операции она получает шифртекст, который отправляет Бобу.

	T						E						C						T					
текст	0	1	0	0	1	1	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0	1	1
ключ	0	1	1	0	1	0	0	0	1	1	0	1	0	1	1	1	1	0	0	0	0	0	1	1
текст XOR ключ	0	0	1	0	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0

Шифр Вернами

- Получив шифртекст, Боб складывает его с ключом с помощью операции XOR. Получившееся бинарное представление расшифрованного сообщения он переводит в буквенный вид

шифртекст	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**
ключ	0	1	1	0	1	0	0	0	1	1	0	1	0	1	1	1	1	0	0	0	0	0	1	1
Шифртекст XOR ключ	0	1	0	0	1	1	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0	1	1
текст	T						E						C						T					

В чем состоит проблема реализации одноразового блокнота?

Одноразовый блокнот

Проблема:

Каждый раз при передаче сообщения нужно передавать новый ключ.

Как передать ключ от Алисы к Бобу, или наоборот?

Квантовая криптография

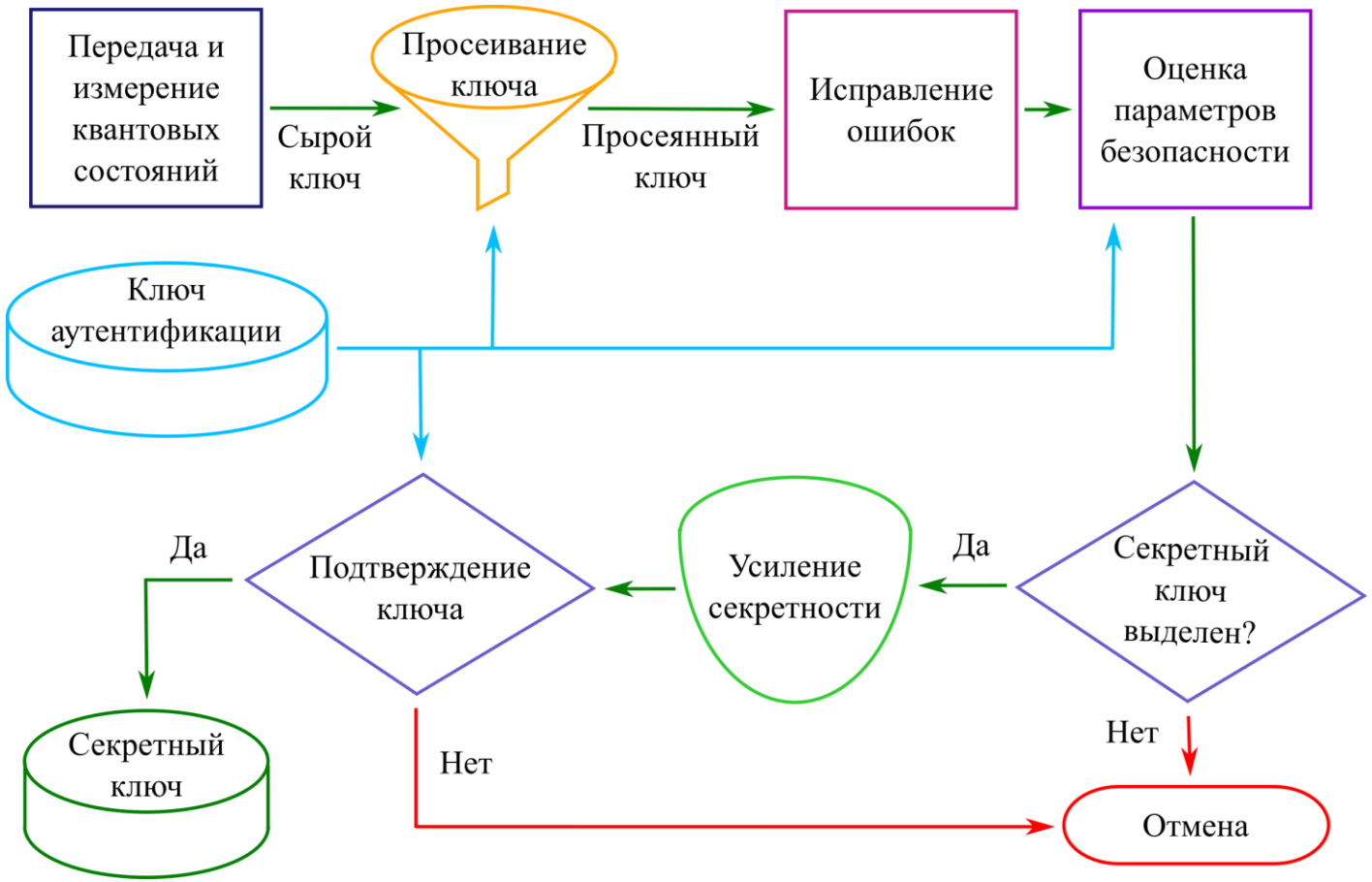
- Квантовая криптография - молодая технология, использующая фундаментальные законы квантовой физики для решения задач защищенной передачи информации.

- Квантовая криптография зародилась на абстрактных идеях, которые в 70-х годах XX века выдвинул Стефан Визнер и которые получили развитие только через 10 лет.

- Еще в 90-е годы идеи квантовой информации воспринимались многими физиками как нечто близкое скорее к физическим аспектам философии.

- В 2000-е задача квантового распределения ключа не только реализована на промышленном уровне, но и пришла в виде учебной дисциплины в ВУЗы.

Общая схема квантового распределения ключей



СПАСИБО ЗА ВНИМАНИЕ!

Квантовый центр ТГУ
qtcenter.tsu.ru