***Контрольные вопросы***

1. ***В чем заключается метод одноразового ключа?***

Этот метод криптографии дает 100% гарантию безопасности при условии, что необходимые условия удовлетворяются. Сам метод является классической техникой, однако квантовая физика дает возможность реализации условий, при которых он срабатывает.

Основная идея метода заключается в следующем: каждый символ открытого текста (сообщения, которое нужно зашифровать) и каждый символ ключа (одноразового ключа) представляют собой битовые последовательности. Шифрование происходит путем побитового сложения символов открытого текста с символами ключа по модулю 2 (XOR-операция). Расшифрование осуществляется путем выполнения такой же операции с зашифрованным текстом и ключом.

1. ***Каковы правила данного метода шифрования?***

Правила данного метода шифрования, следующие:

• Длинна ключа должна быть не меньше длины исходного сообщения

• Ключ может быть использован только единожды

• Ключ должен быть полностью случайным

• Ключ должен быть известен только получателю и адресату

1. ***Чем однобазисная система отличается от двух базисной?***

Описанный выше однобазисный метод достаточен для передачи данных между Алисой и Бобом, однако, недостаточно защищен от перехвата. Для выполения этой задачи вводится двух–базисная схема

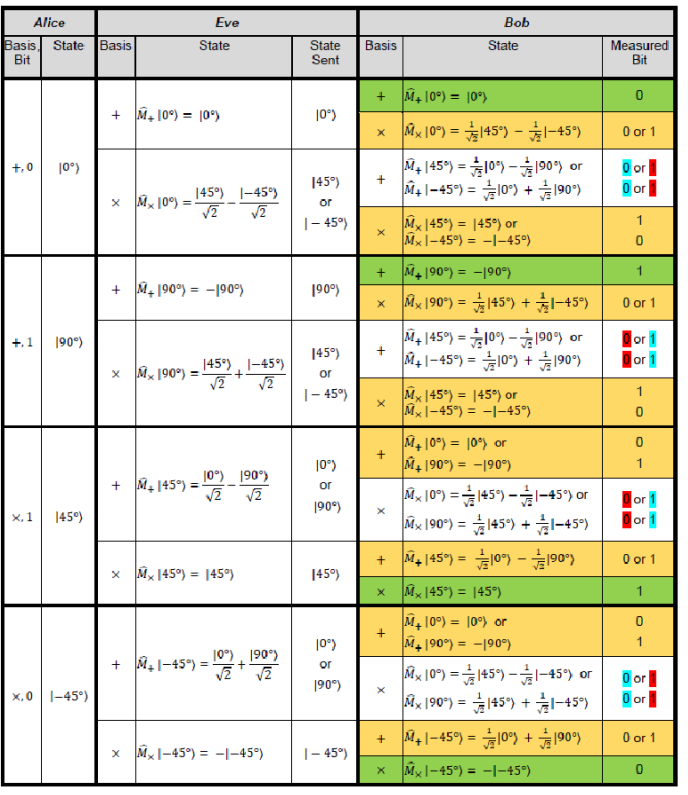
1. ***Для чего в установке используется полуволновая пластинка?***

поворачивает вектор поляризации на удвоенный угол относительно угла между оптической осью пластинки и исходным вектором поляризации падающего света

1. ***Как производится выполнение протокола шифрования?***
2. Алиса случайным образом выбирает базисы и биты, Боб случайным образом выбирает базисы.

Изображение выглядит как текст, снимок экрана, число, линия

Автоматически созданное описание

1. Алиса посылает сигналы, Боб записывает результаты своих измерений  Изображение выглядит как текст, линия, число, Шрифт

   Автоматически созданное описание
2. Алиса и Боб сравнивают свои базисы (я выбрала +, я выбрал -) Изображение выглядит как текст, Шрифт, линия, типография

   Автоматически созданное описание
3. Смотрят на итоговый ключ :
4. Алиса шифрует две буквы с помощью сгенерированного кода. Использованы буквы 𝑄 и 𝑀 английского алфавита: Изображение выглядит как текст, число, снимок экрана, Шрифт

   Автоматически созданное описание
5. Далее, Алиса отправляет зашифрованные буквы в + базисе. 0 ∘ обозначает бит 0, 90∘ обозначает бит 1. Боб принимает сигналы в + базисе, таким образом, что отраженный свет – бит 1, прошедший – 0 Изображение выглядит как текст, Шрифт, линия, число

   Автоматически созданное описание
6. Теперь, используя полученный ранее код, Боб может расшифровать сообщение: Изображение выглядит как текст, число, Шрифт, снимок экрана

   Автоматически созданное описание
7. ***Как можно обнаружить перехватчика сообщения (Еву)?***

Алиса и Боб открыто сравнивают биты, сохраненные после п.2. В случае наличия ошибок, возможно присутствие шпиона (Ева) и ключ удаляется. Если же шпион не обнаружен и ошибок нет, протестированные биты удаляются и оставшиеся становятся финальным ключом шифрования.

1. ***Как выбираются Алисой базис и бит при создании ключа шифрования?***

Случайным образом. Алиса случайным образом выбирает базис(+/x) и бит (1 и 0) в этом базисе.

1. ***Каковы правила бинарного сложения?***

***Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание***