**29.05.2020**

**Выполнил конспект: Бобнев Алексей П1-17.**

**6.1. Классические шифры**

Наука, занимающиеся вопросами безопасной связи, называется криптологией. Она в свою очередь разделяется на два направления криптографию и криптоанализ.

Криптография – наука о создании безопасных методов связи, о создании стойких шифров. Она занимается поиском математических методов преобразования информации.

Криптоанализ – раздел, посвященный исследованию возможности чтения сообщений без знания ключей. Он связан непосредственно со взломом шифров. Специалисты, занимающиеся криптоанализом и исследованием шифров, называются криптоаналитиками.

Шифр – совокупность обратимых преобразований множества открытых текстов на множества зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

**Основные требования, которые предъявляются к методам шифрования:**

1. Сложность и трудоемкость процедур шифрования и расшифрования должны определяться в зависимости от степени секретности защищаемых данных.
2. Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику известен способ закрытия.
3. Способ закрытия и набор используемых служебных данных не должны быть слишком сложными. Затраты на защитные преобразования должны быть приемлемые при заданном уровне сохранности информации.
4. Выполнение процедур прямого и обратного преобразования должно быть формальным и как можно проще.
5. Процедуры прямого и обратного преобразования не должны зависеть от длины сообщения.
6. Ошибки, возникающие в процессе преобразования, не должны распространяться по системе и вызывать потерю информации.
7. Избыточность сообщений, вносимая закрытием, должна быть как можно меньшей.
8. Объем ключа не должен затруднять его запоминание и пересылку.

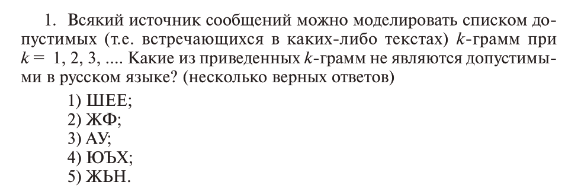
**6.4. Асимметричные криптосистемы**

Криптосистема называется асимметричной, поскольку для зашифрования и расшифрования в ней используется разные преобразования.

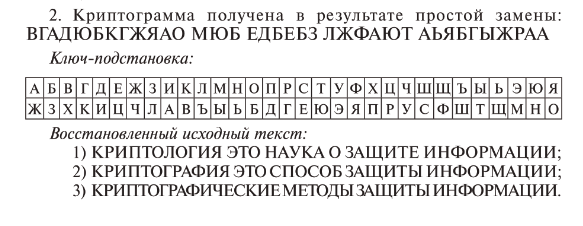
Криптографическая система с открытым ключом – система шифрования и/или электронной подписи, при которой открытый ключ передается по открытому каналу и используется для проверки ЭП и/или для шифрования сообщения.

Первое практическое воплощение принцип открытого шифрования получил в системе RSA, разработанной в 1977 г. в Массачусетском Технологическом Институте (США) и получившей свое название RSA от первых букв фамилий авторов: Рональд Ривест, Эди Шамир, Леонард Адлеман.

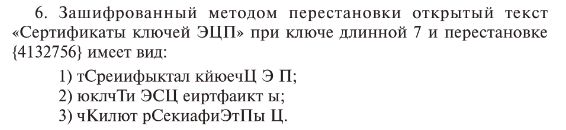
**Контрольные вопросы:**



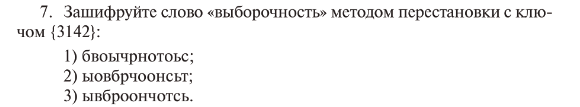
Ответ: 2, 4 и 5. Потому что “шее” и “ау” можно использовать – это допустимые k-граммы. Из этих кусков можно получить слова, которые имеют смысл.



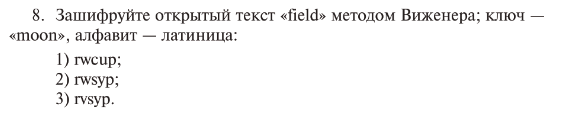
Ответ: 2, чтобы проверить правильность решения задачи, можно посчитать буквы.



Ответ: 1. Определил ответ по первой букве.



Ответ: 1. Определил ответ по первой букве.



Ответ: 2. Используя таблицу Виженера, получаем правильный ответ.