Тема 3 Криптография

1. Что такое криптография и криптоанализ?

**Криптография** — это наука, которая занимается разработкой методов шифрования информации для обеспечения её конфиденциальности, целостности, аутентификации и неотказуемости. Основные цели криптографии — сделать информацию доступной только для тех, кому она предназначена, и защитить её от несанкционированного доступа. Она включает в себя шифрование (превращение открытого текста в зашифрованный) и дешифрование (обратный процесс).

Основные разделы криптографии:

* **Симметричное шифрование**: когда для шифрования и дешифрования используется один и тот же ключ.
* **Асимметричное шифрование**: когда используются разные ключи — открытый для шифрования и закрытый для дешифрования.
* **Хеш-функции**: алгоритмы, которые преобразуют данные любой длины в фиксированный размер строки (хеш), часто используемые для проверки целостности данных.

**Криптоанализ** — это наука о взломе криптографических систем, то есть анализе и поиске слабых мест в системах шифрования. Цель криптоанализа — найти способы расшифровать сообщение без знания ключа, который был использован для его шифрования.

Криптоанализ может использовать различные методы:

* **Анализ на основе полного перебора ключей** (brute force) — метод, при котором проверяются все возможные варианты ключей.
* **Анализ частотности** — метод, который использует статистические свойства языка для нахождения ключа в классических шифрах.
* **Дифференциальный и линейный криптоанализ** — методы, которые используются для анализа симметричных шифров.

Криптография и криптоанализ тесно связаны, так как развитие одного стимулирует развитие другого.

1. Какие древние шифры вы знаете?

### 1. ****Шифр Цезаря****

Один из самых известных и простых шифров. Использовался Юлием Цезарем для шифрования военной корреспонденции. Суть шифра в том, что каждая буква открытого текста заменяется на другую букву, отстоящую на фиксированное количество позиций в алфавите. Например, сдвиг на три позиции:

* Открытый текст: **A** -> Зашифрованный текст: **D**

### 2. ****Шифр Скитала****

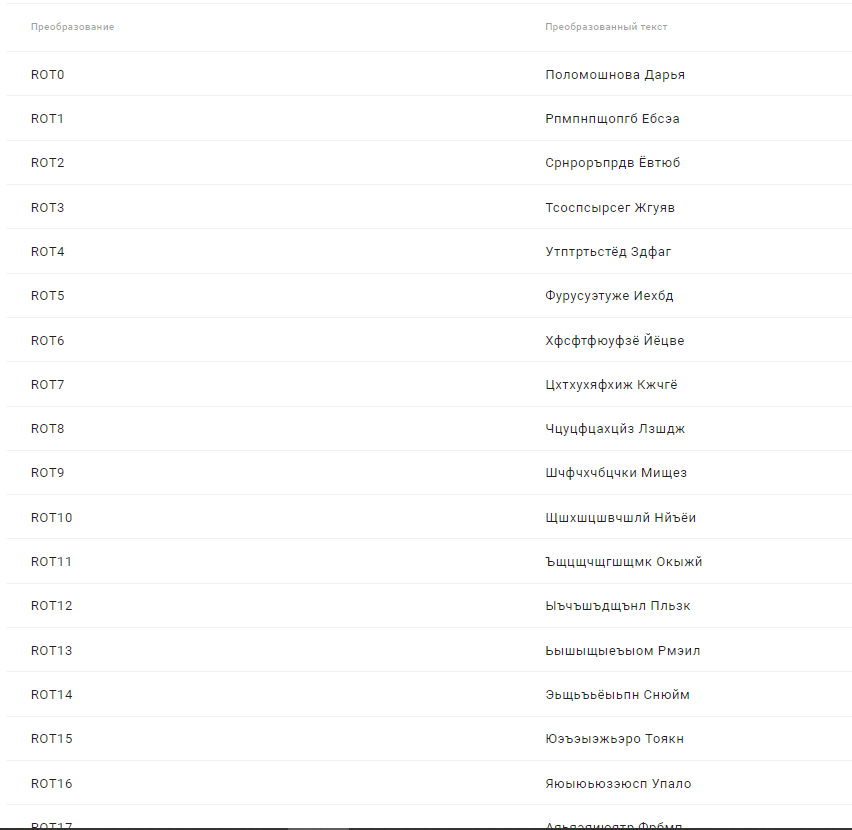
Использовался в Спарте. Это один из первых известных методов шифрования, основанных на физических устройствах. Шифр представлял собой цилиндр (скиталу), вокруг которого наматывали ленту с написанным текстом. После наматывания шифрованное сообщение представляло собой последовательность бессмысленных символов. Чтобы расшифровать сообщение, нужно было намотать ленту на цилиндр того же диаметра.

### 3. ****Шифр Полибия****

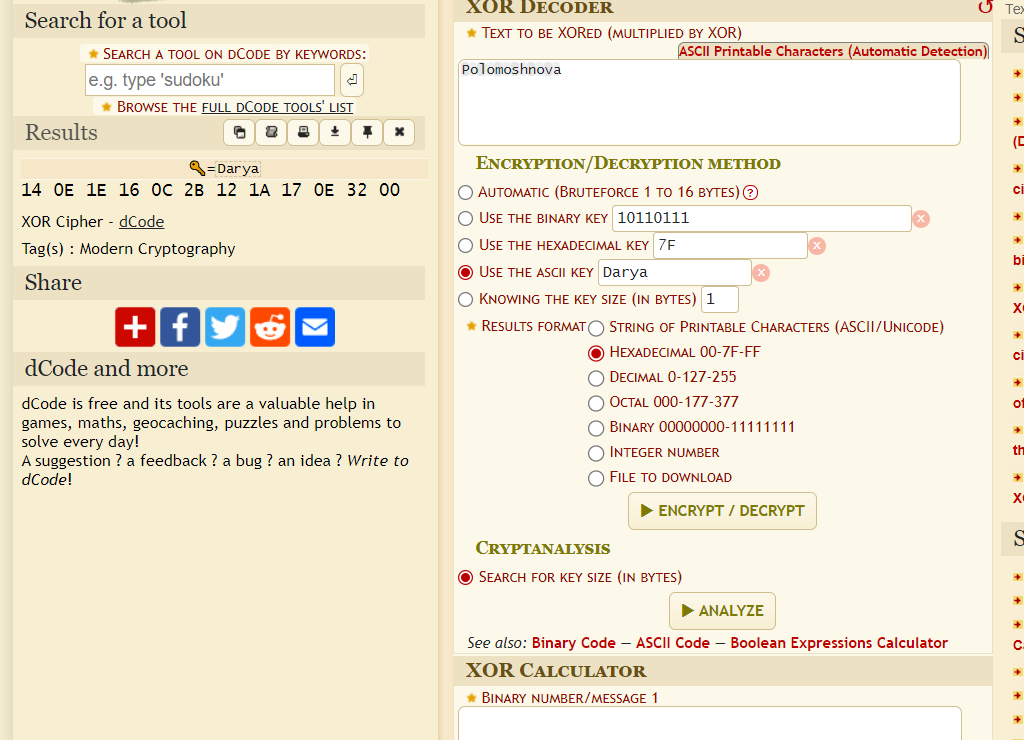
Древнегреческий шифр, созданный Полибием, представлял собой таблицу 5x5, в которой каждая буква алфавита кодировалась парой чисел. Сообщение передавалось в виде числовых пар, каждая из которых соответствовала координатам буквы в таблице.

1. Шифр Цезаря.

Зайдите на сайт <https://planetcalc.ru/1434/>, зашифруйте шифром цезаря свои имя и фамилию. Результаты вставьте в отчет.



1. Шифр xor. Найдите в интернете сайт, осуществляющий шифрование xor, например, <https://www.dcode.fr/xor-cipher> и зашифруйте сою фамилию, используя имя в качестве ключа. Результаты вставите в отчет.



1. Найдите в интернете сайт, который осуществляет шифрование симметричными шифрами (например <https://www.dcode.fr>, <https://cryptii.com/>) зашифруйте свое имя и фамилию. Попробуйте расшифровать. Сколько времени понадобилось? Результаты вставьте в отчет.

Вводные данные: Polomoshnova Darya  
Шифр цезаря: Wvsvtvzouvch Khyfh  
Обратная расшифровка: Polomoshnova Darya

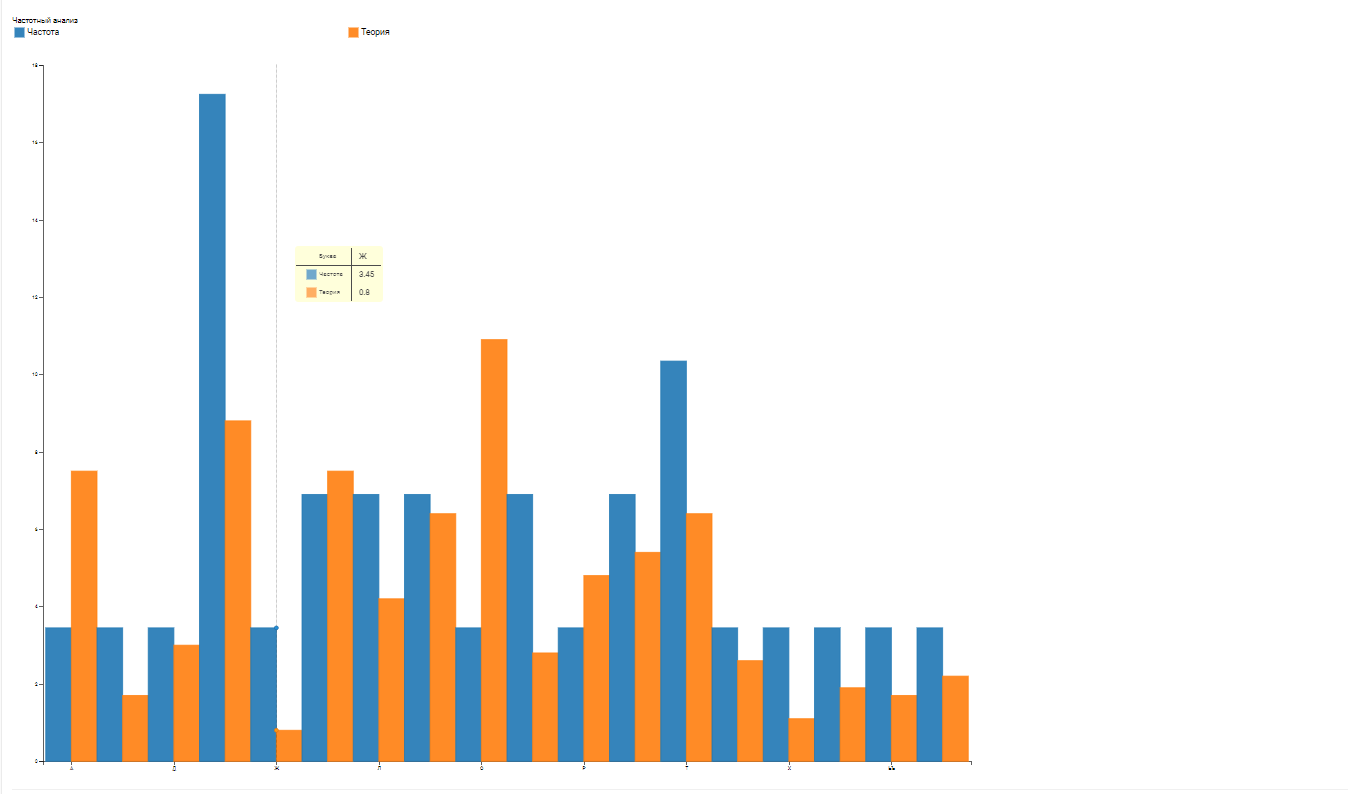
1. Что такое частотный анализ? Зайдите на сайт <https://planetcalc.ru/733/>, придумайте СВЮ фразу и проведите частотный анализ. Результаты вставьте в отчет.

**Частотный анализ** — это метод криптоанализа, который основан на изучении частоты появления символов в зашифрованном тексте. Частотный анализ использует статистические закономерности естественных языков. Например, в русском языке буквы «О», «Е», «А» встречаются чаще, чем «Ф» или «Щ». Криптоаналитики могут использовать эти особенности для расшифровки шифров замены, таких как шифр Цезаря или простой шифр подстановки.

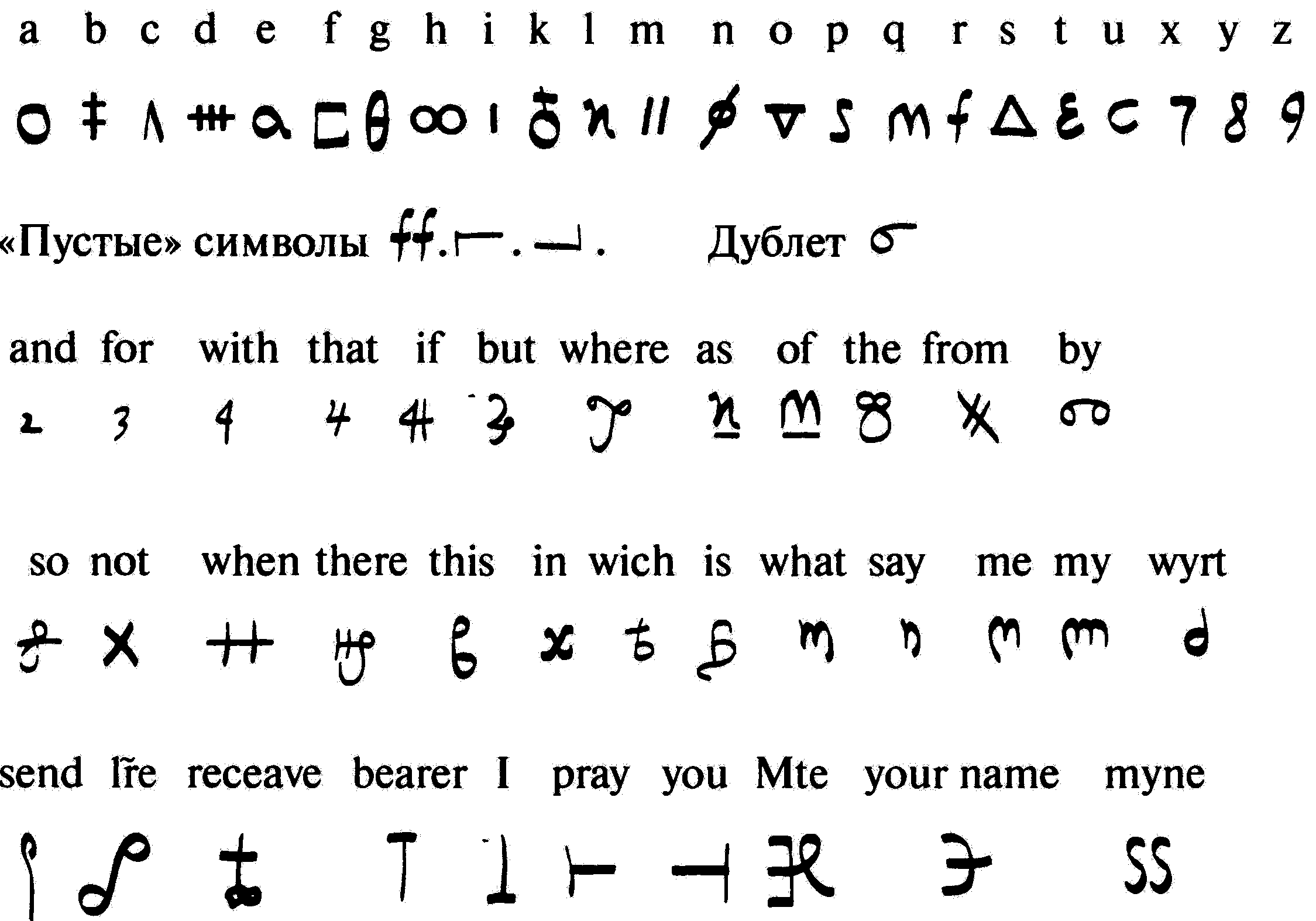
Фраза для анализа:

**Если нет хлеба, пусть едят пирожные**

Результаты анализа:



1. На 22-м слайде представлен шифр



Что это за шифр и какие исторические события м ним связаны?

На изображении представлен шифр **Марии Стюарт**, использовавшийся для тайной переписки. Этот шифр был применён Марией, королевой Шотландии, во время её заключения, чтобы тайно общаться с союзниками. Один из самых известных эпизодов связан с заговором Бабингтона, когда переписка Марии была расшифрована агентами Фрэнсиса Уолсингема. Это стало ключевым доказательством её участия в заговоре против королевы Елизаветы I, что привело к суду и казни Марии в 1587 году.

1. Что делала эта машина?



Кто взломал шифр? Когда это было?

На изображении показана **машина "Энигма"**, использовавшаяся для шифрования сообщений во время Второй мировой войны. Она генерировала сложные шифры, которые менялись каждый день. Немецкие вооружённые силы широко использовали её для секретной связи. Шифр "Энигмы" был взломан в 1940 году группой криптоаналитиков во главе с польским математиком **Марианом Реевским**, а позднее их работу продолжили в Великобритании. Английский математик **Алан Тьюринг** и его команда в Блетчли-Парке сыграли ключевую роль в окончательном взломе системы.

1. Симметричные шифры. Достоинства и недостатки.

**Симметричные шифры** — это методы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ. Примеры таких шифров: AES, DES, Triple DES.

**Достоинства:**

1. **Высокая скорость**: Они быстрее, чем асимметричные шифры, благодаря простоте математических операций.
2. **Меньшая вычислительная нагрузка**: Менее требовательны к ресурсам.

**Недостатки:**

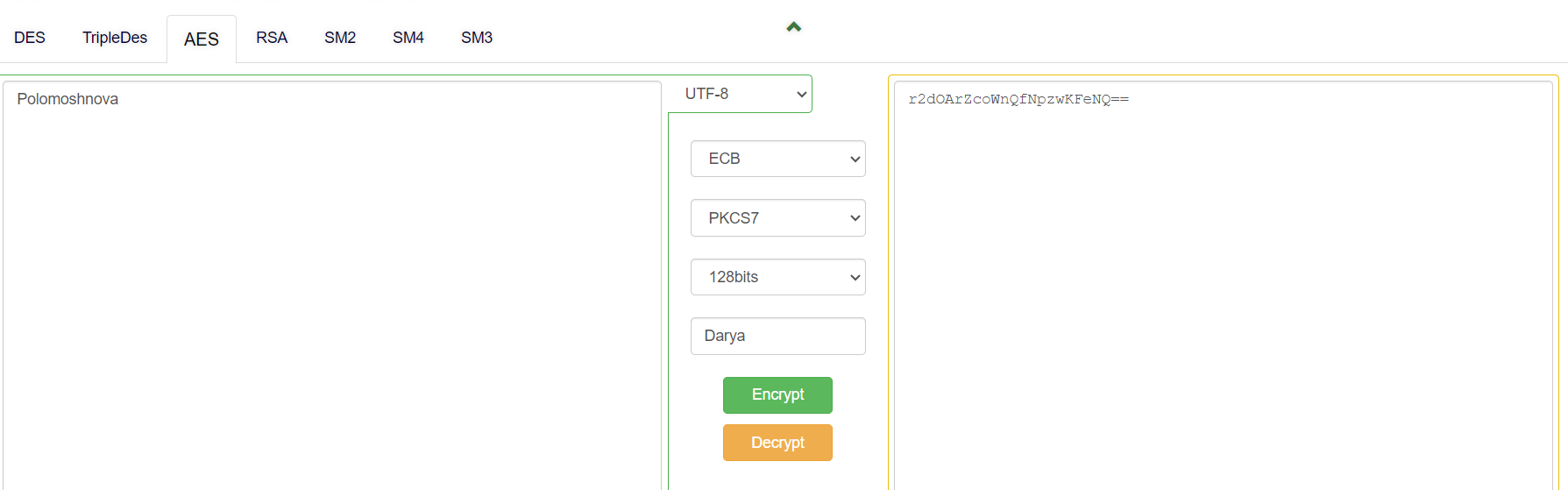
1. **Проблемы с управлением ключами**: Требуется безопасный канал для передачи ключа.
2. **Масштабируемость**: С ростом числа пользователей количество ключей увеличивается экспоненциально.
3. Какие современные симметричные системы вы знаете?

Современные симметричные шифры широко используются для обеспечения безопасности данных. Вот несколько популярных систем:

1. **AES (Advanced Encryption Standard)** — самый популярный симметричный алгоритм, использующийся во многих стандартах и протоколах, например, SSL/TLS.
2. **DES (Data Encryption Standard)** — устаревший, но всё ещё используется для совместимости с некоторыми системами.
3. **Triple DES (3DES)** — улучшенная версия DES, которая шифрует данные трижды для повышения безопасности.
4. **RC4** — потоковый шифр, хотя в настоящее время считается небезопасным.
5. **Blowfish** и его улучшенная версия **Twofish** — алгоритмы для общего использования, известные своей скоростью и надёжностью.

Эти алгоритмы применяются для защиты данных в различных системах, от электронной коммерции до облачных технологий.

1. Зайдите на один из сайтов, осуществляющих шифрование AES, например <https://the-x.cn/en-US/cryptography/Aes.aspx> Зашифруйте свою фамилию, используя в качестве ключа имя. Результат приложите к отчету.



1. Чем современные симметричные криптосистемы отличаются от применяемых до 1990-стых?

Современные симметричные криптосистемы отличаются от тех, что использовались до 1990-х годов, несколькими ключевыми аспектами:

1. **Безопасность**: Современные алгоритмы, такие как AES, обладают большей криптостойкостью благодаря увеличенным размерам ключей (128, 192, 256 бит), что делает их значительно сложнее для взлома по сравнению с DES (56-битные ключи).
2. **Оптимизация для аппаратуры**: Новые шифры лучше оптимизированы для работы на современных процессорах и устройствах.
3. **Проблемы устаревших алгоритмов**: Многие ранние шифры (например, DES) были взломаны или больше не считаются безопасными из-за роста вычислительных мощностей.