1. На примере своего варианта реализации практического задания пояснить свойства симметричности и обратимости сети Фейстеля.

Свойство симметричности заключается в том, что для шифрования и дешифровки применяется один и тот же алгоритм, но с разной последовательностью ключей, а именно, в обратном порядке.

Свойство обратимости заключается в том, что исходные данные можно восстановить с использованием той же функции F и ключами в обратной последовательности. Не нужно использовать обратную ей функцию.

1. Каким способом достигаются эффекты рассеивания и перемешивания?

Эффект рассеивания подразумевает, что изменения в одном бите открытого текста приводят к изменениям в нескольких битах зашифрованного текста. Достигается это применением функции f(l, k), скрывающей статистические свойства исходных данных.

Эффект перемешивания достигается обменами половинок блоков.

Векторы инициализации (IV) играют ключевую роль в режимах шифрования CBC (Cipher Block Chaining) и CFB (Cipher Feedback). Они обеспечивают уникальность и безопасность зашифрованных данных. Рассмотрим основные требования к генерации и хранению IV для этих режимов.

Общие требования к вектору инициализации

1. Уникальность:

В режиме CFB вектор инициализации должен быть уникальным для каждого сообщения. Если IV не уникален, это может привести к раскрытию открытого текста криптоаналитиками12.

В режиме CBC уникальность IV не является строгим требованием, но рекомендуется, чтобы избежать потенциальных уязвимостей3.

2. Непредсказуемость:

IV должен быть непредсказуемым. Это достигается путем использования случайных или псевдослучайных чисел, что критично для обеспечения семантической безопасности. Повторное использование одного и того же IV с тем же ключом может привести к компрометации данных36.

3. Размер:

Длина IV должна соответствовать размеру блока шифрования (например, 128 бит для AES). Это обеспечивает корректную работу алгоритма шифрования3.

Специфические требования для режимов CBC и CFB

Режим CBC

Генерация: Для первого блока шифруемого сообщения используется IV, который передается вместе с шифротекстом. Это позволяет расшифровщику восстановить данные, используя тот же IV37.

Хранение: IV не нужно хранить в секрете, но его значение должно быть случайным и непредсказуемым, чтобы избежать атак на шифрование4.

Режим CFB

Генерация: Как и в режиме CBC, вектор инициализации должен генерироваться случайным образом. Он должен изменяться для каждого нового сообщения, что может быть реализовано с помощью счетчиков или других методов генерации случайных чисел12.

Хранение: IV может быть передан вместе с первым блоком шифротекста, так как его секретность не требуется. Однако важно следить за тем, чтобы он оставался уникальным на протяжении всего времени жизни ключа24.

Каждый из режимов блочного шифрования (ECB, CBC, CFB, OFB, CTR) имеет свои особенности и области применения, где они могут быть более или менее целесообразными. Ниже представлены рекомендации по использованию каждого режима.

ECB (Electronic Codebook)

Целесообразно:

Простые приложения, где требуется быстрая обработка небольших объемов данных.

Сценарии, где данные не имеют повторяющихся блоков и не требуют высокой безопасности.

Нецелесообразно:

Хранение конфиденциальной информации, так как одинаковые блоки открытого текста создают одинаковые блоки шифротекста, что может привести к утечкам информации.

Приложения, требующие защиты от криптоанализа.

CBC (Cipher Block Chaining)

Целесообразно:

Шифрование файлов и больших объемов данных, где важна безопасность и целостность.

Приложения, требующие защиты от повторного использования данных (например, в банковских системах).

Нецелесообразно:

Высокоскоростные приложения, требующие параллельной обработки данных, так как каждый блок зависит от предыдущего.

CFB (Cipher Feedback)

Целесообразно:

Потоковое шифрование данных, где необходимо шифрование и расшифровка по частям (например, в сетевых протоколах).

Приложения с ограниченной памятью или ресурсами.

Нецелесообразно:

Сценарии с большими объемами данных, где более эффективны другие режимы (например, CTR).

OFB (Output Feedback)

Целесообразно:

Приложения, требующие высокой скорости обработки и возможности параллельного шифрования.

Системы с высоким уровнем ошибок передачи данных, так как ошибки не влияют на последующие блоки.

Нецелесообразно:

Сценарии, где требуется высокая степень безопасности, так как IV может быть уязвим для атак.

CTR (Counter)

Целесообразно:

Высокопроизводительные приложения, требующие параллельной обработки (например, в облачных сервисах).

Сетевые протоколы и системы с большой пропускной способностью.

Нецелесообразно:

Системы с низким уровнем ресурсов или встраиваемые системы без возможности управления счетчиком и IV.

Каждый режим шифрования имеет свои преимущества и недостатки. Выбор подходящего режима зависит от конкретных требований безопасности и производительности в приложении.