ШИФРОВАНИЕ ИНФОРМАЦИИ МЕТОДОМ ЦЕЗАРЯ

Каримова Наргиза Ибрагимовна
Преподаватель Ташкентского Государственного Технического Университета имени Ислама Каримова
Рахимова Мохира Музаффаровна
Студент Ташкентского Государственного Технического Университета имени Ислама Каримова

Аннотация: *Шифрование — это процесс кодирования информации с целью предотвращения несанкционированного доступа. В случае кражи или утечки зашифрованные данные будут недоступны для прочтения без соответствующего ключа. Большинство пользователей не знают, что много информации уже защищается с помощью технологии шифрования. Например, онлайн-магазины и Интернет-банкинг не работали бы без хорошего шифрования. Шифрование предназначено для защиты средств и личной информации. В корпоративной среде шифрование следует использовать для защиты интеллектуальной собственности и инновационных разработок компании.*

Ключевые слова: *алгоритм, шифрование, шифрование данных, Шифр Цезаря, кодирование, декодирование*

Алгоритм зашифрования (encryption algorithm): Алгоритм, реализующий зашифрование, т. е. преобразующий открытый текст в шифртекст. **Алгоритм расшифрования** (decryption algorithm): Алгоритм, реализующий расшифрование, т. е. преобразующий шифртекст в открытый текст. **Алгоритм расшифрования** (decryption algorithm): Алгоритм, реализующий расшифрование, т. е. преобразующий шифртекст в открытый текст.

ВИДЫ ШИФРОВАНИЯ

Шифрование данных — это преобразование информации, делающее ее нечитаемой для посторонних. При этом доверенные лица могут провести дешифрование и прочитать исходную информацию.

Шифрование данных применяется для защиты информации при ее хранении и передаче, обеспечивает конфиденциальность информации и защиту данных от несанкционированного доступа.

Существует множество способов шифрования/дешифрования, но секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования известен только доверенным лицам.

Также шифрование позволяет предотвращать изменение данных при их передаче и хранении, обеспечивая таким образом целостность информации.

Существует два основных вида шифрования: симметричное и асимметричное.

Симметричное шифрование для шифрования и дешифрования данных использует один и тот же криптографический ключ. Такой метод широко распространён в криптографии, поскольку очень прост в работе и понимании, техническая нагрузка на оборудование невелика и, таким образом, обеспечивается высокая скорость и надежность шифрования.

К недостаткам относят сложность обмена ключами: при успешном перехвате ключа злоумышленник получит неограниченный доступ к зашифрованной информации.

Основу симметричного шифрования заложил алгоритм DES (Data Encryption Standard), использующий 56-битные ключ, из-за чего возникали споры относительно способности данного алгоритма противостоять различным атакам. Этот стандарт применялся до начала 2000-х годов, пока ему на смену не пришел более совершенный AES (Advanced Encryption Standard), где длина ключа составляет 128, 192 или 256 бит.

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и проверки электронной подписи. Закрытый (приватный) ключ применяется для подписания и расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи — это очень большие числа, связанные друг с другом определенной функцией, но так, что зная одно, крайне сложно вычислить второе.

Информация, зашифрованная при помощи открытого ключа, как и сам открытый ключ, может передаваться по незащищенным каналам связи. В такой схеме перехват любых данных не имеет смысла, поскольку восстановить исходную информацию возможно только при помощи закрытого ключа, известного лишь владельцу и не требующего передачи.

Наиболее распространенным алгоритмом с асимметричным шифрованием является алгоритм RSA, в основе которого лежит вычислительная сложность задачи факторизации больших целых чисел. Длина ключа RSA теоретически не ограничивается, но обычно составляет от 1024 до 8192 бит.

У каждого метода есть свои преимущества и недостатки, а лучший эффект достигается при комбинации обоих видов шифрования. Происходит это, например, так:

— посредством асимметричного алгоритма серверу отсылается сессионный ключ для симметричного шифрования;

— сам обмен информацией происходит по симметричному алгоритму.

Вне зависимости от выбранного вида шифрования, ни один из них не является гарантом стопроцентной безопасности. Помните, что любой подход нужно комбинировать с другими средствами информационной защиты.

МЕТОД ЦЕЗАРЯ ШИФРОВАНИЕ

Шифр Цезаря, также известный как шифр сдвига, код Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$Y= (x+k) \mod n$ $X=(y-k) \mod n$

k- ключ, x- символ открытого текста, y- символ шифрованного текста,

n— мощность алфавита

1-таблица: Шифр Цезаря

Буква	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Номер	1	2	3	4	5	6	7	8	9	10	11
Буква	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Номер	12	13	14	15	16	17	18	19	20	21	22
Буква	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
Номер	23	24	25	26	27	28	29	30	31	32	33

2-таблица: Шифр Цезаря

Система Цезаря с ключевым словом

Система Цезаря с ключевым словом. В этой системе шифрования наряду с числовым ключом *K*, *0 ? K ? (M-1),* задающим смещение, используется ключевое слово для изменения порядка символов в заменяющем алфавите.

В качестве ключевого слова необходимо выбирать слово или короткую фразу (не более длины алфавита). Все буквы ключевого слова должны быть различными.

Для создания таблицы замены ключевое слово записываем под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числовым ключом *K*. Оставшиеся буквы алфавита замены записываем в алфавитном порядке (избегая повтора букв) после ключевого слова. При достижении конца таблицы циклически переходим на ее начало и дописываем последние буквы алфавита не встречавшиеся ранее.

Пример:

- Кодирование со сдвигом 2 слова « ШИФР»

Букву «Ш» заменим на «Ъ»

Букву «И» заменим на «К» Получим слово»ЪКЦТ»

Букву «Ф» заменим на «Ц»

Букву «Р» заменим на «Т»

- Декодирование со сдвигом 2 слова « МРЁ»

Букву «М» заменим на «К»

Букву «Р» заменим на «О» Получим слово «КОД»

Букву «Ё» заменим на «Д»

ЗАКЛЮЧЕНИЯ

Шифрование — это процесс кодирования информации с целью предотвращения несанкционированного доступа. В случае кражи или утечки зашифрованные данные будут недоступны для прочтения без соответствующего ключа. Необходимо отличать шифрование от кодирования. Кодирование тоже преобразует информацию, но лишь для удобства хранения и передачи, секретность не является основной задачей. Типичные способы кодирования – азбука Морзе и двоичное кодирование букв для хранения в компьютере. Самое удобное на сегодня решение по шифрованию файлов на компьютере – это создание «контейнера», который виден в системе как отдельный диск. На этот диск можно сохранять или копировать любую информацию, с ним можно работать из любой программы, он ничем, по сути, не отличается от флешки или раздела винчестера, чем и удобен.

РЕКОМЕНДАЦИИ

1. Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Режимы работы блочных шифров ГОСТ 34.13— 2018

2. https://www.kaspersky.ru/blog/encryption-reasons/879

3. https://ru.wikipedia.org/wiki

4. https://www.yaklass.ru/p/informatika/10-klass/informatciia-i-informatcionnye-protcessy-11955/kodirovanie-informatcii-6737203/re-d8441a6e-3958-4fdf-8a6d-b5961baf5714

5. https://ru.stackoverflow.com/questions/