Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье

Дата прошедшей лекции	Номер прошедшей лекции	Название статьи/главы книги/видеолекции	Дата публикации (не старше 2021 года)	Размер статьи (от 400 слов)	Дата сдачи
11.09.2024	1	Этимон цифры и числа	30.08.2023	~2150	25.09.2024
25.09.2024	2	Модификация алгоритма на основе сети Фейстеля с добавлением элемента случайности в ключ шифрования	2021, точная дата не найдена	~2450	09.10.2024
	3				
	4				
	5				
	6				
	7				

Выполнил(а) Снагин С. М., № группы *P3115*, оценка _____
Фамилия И.О. студента — не заполнять

Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т.п.)
https://bit.ly/4dDxNry

Теги, ключевые слова или словосочетания (минимум три слова)
криптография, сеть Фейстеля, коды Хэмминга, блочные шифры

Перечень фактов, упомянутых в статье (минимум четыре пункта)

1. Сеть Фейстеля (далее СФ) — актуальный метод построения блочных шифров, используется в DES, Blowfish, «Магме» и др. криптоалгоритмах.
2. Суть СФ в разбиении данных на несколько частей, одна из которых оборачивается некой функцией (чаще с использованием ⊕ или сложением по 2^n) и накладывается на другие части.
3. В СФ при каждой итерации меняется обрабатываемый блок.
4. СФ прост в реализации при ограниченности ресурсов, шифр использует простые функции (⊕) и алгоритмы шифратора и дешифратора совпадают.
5. СФ уязвим к частотному криптоанализу; неполнота обработанных блоков (=> больше итераций и блоков).
6. Модификация заключается в использовании числа раундов, ⋮ 4, каждый из которых это СФ.
7. Модифицированный алгоритм СФ медленнее обычного в среднем в 1.61 раз
8. Значение энтропии у модиф. алгоритма чуть больше (±0.1), т. к. в нем присутствует элемент случайности.
9. Модиф. алгоритм все равно устойчив к сдвиговым атакам за счет инвертирования случайного бита исходного ключа при формировании раундовых ключей.
10. С.А. Демин «Вероятностное шифрование»: из-за рандома одному исходному тексту может соответствовать несколько шифротекстов, т. е. по сравнению классическим СФ алгоритм более устойчив к криптоанализу.
11. Для модиф. СФ необходимо применять ГПСЧ, что является недостатком.
12. Основа для модиф СФ — внесение в шифруемый блок данных случайной ошибки, которую можно исправить проверочными битами кода Хэмминга.

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)

1. Повышенная стойкость алгоритма шифрования
2. Устойчив к основным видам криптоатак (сдвиговая, грубая сила, диф. анализ,
3. Возможность распараллелить шифрования отдельных блоков, т. е. уменьшить время выполнения.

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)

1. Несмотря на параллельные вычисления, из-за рандомизации, время шифрования отдельного блока увеличено
2. Генерация псевдослучайных чисел повышает сложность реализации алгоритма.
3. Размер зашифрованного блока увеличен (хранение контрольных битов того же кода Хэмминга)

Ваши замечания, пожелания преподавателю *или* анекдот о программистах[1]
Сколько пользователей дискорда нужно, чтобы поменять лампочку? — Ноль, ведь они предпочитают Dark Mode!

[1] Наличие этой графы не влияет на оценку