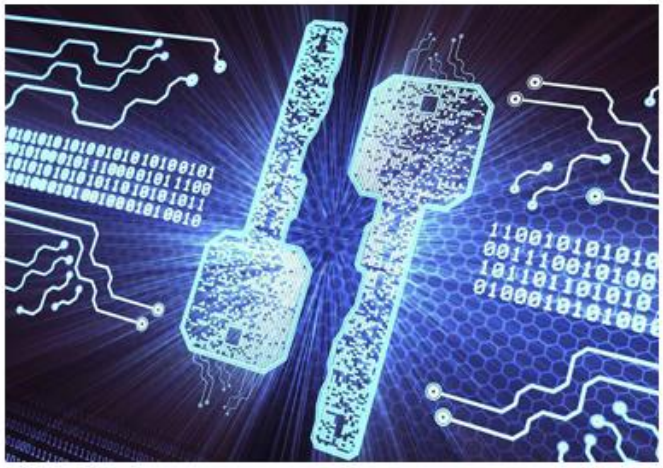
УЧЕНЫЕ МИФИ ПРЕДЛОЖИЛИ НОВЫЙ СПОСОБ ЗАЩИТЫ ЧАТОВ В МЕССЕНДЖЕРАХ



Защита информации в мессенджерах – одна из серьезных задач, которую решают современные программисты. Считается, что корпорации хотят читать переписку людей, чтобы точнее отправлять целенаправленную рекламу или «сдавать» персональные данные тем, кто больше заплатит. Хакеры хотели бы использовать эту информацию для кражи персональных данных и денег. Не исключено, что силовые структуры во всем мире через мессенджеры следят за тем, что люди думают или делают. И это, в частности, помогает выявить террористов. Поэтому, если человек не пользуется защищенными мессенджерами, кто-то легко может перехватить его данные.

Ученые кафедры «Криптология и кибербезопасность» ядерного университета МИФИ разработали постквантовый алгоритм для защиты группового обмена данных в мессенджерах.

Как рассказал профессор Института интеллектуальных кибернетических систем НИЯУ МИФИ Сергей Запечников, во всем мире идет активная работа над созданием квантовых компьютеров. Эти машины смогут за короткое время решать задачи разложения целых чисел на простые множители и дискретного логарифмирования, на которых во многом основана стойкость современной криптографии.

По словам ученого, принцип действия новых методов станет базироваться на том, что нарушитель при попытке взломать криптографический алгоритм столкнется не с одной вычислительно сложной задачей, как сейчас, а с необходимостью перебора колоссального количества однотипных вычислительных задач.

— Если решить каждую из них в отдельности нарушителю с квантовым компьютером будет легко, число задач будет настолько большим, что даже квантовый компьютер окажется бесполезен, — уточнил Сергей Запечников. — Мессенджеры – персональные средства мгновенного обмена сообщениями и файлами – сегодня очень популярны. Практически каждый современный человек пользуется ими. Предполагается, что в будущем их роль в информационных технологиях только возрастет. Поэтому очень важно уже сейчас предусмотреть криптографические протоколы для их защиты.

Мона ПЛАТОНОВА.

УЧЕНЫЕ МИФИ ПРЕДЛОЖИЛИ НОВЫЙ СПОСОБ ЗАЩИТЫ ЧАТОВ В МЕССЕНДЖЕРАХ

Автор: Мона ПЛАТОНОВА

Защита информации в мессенджерах - одна из серьезных задач, которую решают современные программисты. Считается, что корпорации хотят читать переписку людей, чтобы точнее отправлять целенаправленную рекламу или "сдавать" персональные данные тем, кто больше заплатит. Хакеры хотели бы использовать эту информацию для кражи персональных данных и денег. Не исключено, что силовые структуры во всем мире через мессенджеры следят за тем, что люди думают или делают. И это, в частности, помогает выявить террористов. Поэтому, если человек не пользуется защищенными мессенджерами, кто-то легко может перехватить его данные.

Ученые кафедры "Криптология и кибербезопасность" ядерного университета МИФИ разработали постквантовый алгоритм для защиты группового обмена данных в мессенджерах.

Как рассказал профессор Института интеллектуальных кибернетических систем НИЯУ МИФИ Сергей Запечников, во всем мире идет активная работа над созданием квантовых компьютеров. Эти машины смогут за короткое время решать задачи разложения целых чисел на простые множители и дискретного логарифмирования, на которых во многом основана стойкость современной криптографии.

По словам ученого, принцип действия новых методов станет базироваться на том, что нарушитель при попытке взломать криптографический алгоритм столкнется не с одной

вычислительно сложной задачей, как сейчас, а с необходимостью перебора колоссального количества однотипных вычислительных задач.

- Если решить каждую из них в отдельности нарушителю с квантовым компьютером будет легко, число задач будет настолько большим, что даже квантовый компьютер окажется бесполезен, - уточнил Сергей Запечников. - Мессенджеры - персональные средства мгновенного обмена сообщениями и файлами - сегодня очень популярны. Практически каждый современный человек пользуется ими. Предполагается, что в будущем их роль в информационных технологиях только возрастет. Поэтому очень важно уже сейчас предусмотреть криптографические протоколы для их защиты.

стр. 2

Источник *Московская правда*, № 3, 11 января 2023 стр. 2