Я. И. Фролов, М. В. Лемеза

ГЕНЕРАЦИЯ ПАРОЛЕЙ В БАНКОВСКОМ ДЕЛЕ

Рассматриваются методы генерации случайных чисел в компьютерных технологиях, а также в банковском деле в частности. Анализ наиболее популярных сервисов для генерации паролей.

Введение

Случайные числа и случайность имеют множество применений в криптографии, науке, играх, искусстве, а также во многих других областях. Для разных задач, требуется генерация разного качества, именно по этой причине существует потребность в разнообразных методах генерации случайных чисел. Генераторы случайных чисел (ГСЧ) делятся на два основных типа: Генераторы псевдосучайных чисел (ГПСЧ) и Генераторы случайных чисел (ГСЧ). С развитием информационных технологий и интернета, возросла потребность в качественной генерации случайных чисел, не только у специалистов, но и у обычных людей. В данной публикации мы рассмотрим основные методы генерации случайных чисел их преимущества и недостатки , а также их практическое применение.

I. Генераторы псевдослучайных чисел (ГПСЧ)

Из-за простоты и дешевизны для выработки случайных чисел чаще всего используются генераторы, созданные как соответствующие программы на ЭЦВМ. С помощью этих программ по некоторому алгоритму получают последовательности чисел. Алгоритм построен так, что знаки 0 и 1 появляются в среднем одинаковое число раз и отсутствует зависимость между появлениями этих знаков и сформированными из них многозначными числами. Числа получаемые с помощью таких генераторов называются псевдослучайными или квазислучайными. Простейшим примером может служить разложение в десятичную дробь иррациональных чисел. Качественные требования, предъявляемые к ГПСЧ:

- Достаточно длинный период, гарантирующий отсутствие зацикливания последовательности в пределах решаемой задачи. Длина периода должна быть математически доказана
- Эффективность – быстрота работы алгоритма и малые затраты памяти
- Воспроизводимость – возможность заново воспроизвести ранее сгенерированную последовательность чисел любое количество раз
- Портируемость – одинаковое функционирование на различном оборудовании и операционных системах
- Быстрота получения

Никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые их свойства.

II. Генераторы случайных чисел (ГСЧ)

Генераторы истинно случайных чисел генерируют последовательности случайных чисел на основе измеряемых, хаотически изменяющихся параметров физического процесса. Работа таких устройств часто основана на использовании надёжных источников энтропии таких, как тепловой шум, дробовой шум, фотоэлектрический эффект, квантовые явления, погодные явления и другие физические процессы. Простейшим примером генератора может служить подбрасывание монетки или игральной кости. Основная проблема аппаратных генераторов случайных чисел – это их относительная медленная по сравнению с ГПСЧ работа.

Алгоритмы проверки PIN

На данный момент, в основном, используются следующие 2 алгоритма проверки PIN: Visa PVV и IBM 3624 PIN offset.

Visa PVV

Данный алгоритм первоначально был разработан платежной системой Visa, но, в настоящее время является рекомендованным алгоритмом проверки PIN как для карт Visa, так и для MasterCard. В основе данного алгоритма лежит значение PVV (PIN verification value), которое является криптограммой, получаемой на основе следующих величин:

- Номер карты (далее PAN)
- Индекс ключа проверки PIN (PIN verification key index, далее, PVKI)
- Ключ проверки PIN (PIN verification key, далее, PVK)
- Сам PIN-код карты

Для получения PVV формируется блок из PAN (последние 11 цифр, кроме контрольного числа карты), PVKI, PIN (строго, первые 4 цифры), который зашифровывается с помощью PVK, после чего из него, с помощью специальной

функции, извлекаются 4-х значное число, которое и является значением PVV. Данное значение PVV является эталонным для проверки PIN кода. Т.е. при получении операции с введенным PIN для его проверки на основании PAN, PVKI, PVK формируется новое значение PVV и сравнивается с эталонным PVV для карты. Если значения совпадают, то PIN считается верным, если не совпадают – неверным.

К особенностям данного алгоритма можно отнести следующие «ограничения»:

- Принципиальная невозможность восстановления PIN из значения PVV
- Использование PIN-кода размером строго 4 цифры

IBM 3624 PIN offset

Данный алгоритм первоначально был разработан компанией IBM для использования в банкоматах IBM 3624. Как именно планировалось его использовать, история умалчивает, а авторы статьи не знают, но, в данном случае, это не принципиально. В настоящее время данный алгоритм считается устаревшим, но достаточно успешно используется по нескольким причинам:

- карточные системы «старых» регионов (Западная Европа, Северная Америка) достаточно консервативны и, во многом, работают на «достаточно» старых системах, что их вполне устраивает
- данный алгоритм позволяет восстановить значение PIN кода из проверочного значения (см. далее), что м.б. весьма полезно при определнных условиях

В основе данного алгоритма лежит значение PIN offset (PIN verification value), которое является криптограммой, получаемой на основе следующих величин:

- Контрольное значение (Validation data, далее VD) – некоторое значение (обычно – часть номера карты, но это не обязательно)
- Децимализационная таблица (Decimalization table, далее DT)
- Ключ проверки PIN (PIN verification key, далее, PVK)
- Сам PIN-код карты

Для простоты дальнейшего описания под ключом проверки PIN в случае метода IBM 3624 PIN offset будем совокупность ключа PVK и значения таблицы децимализации DT.

Для получения PIN offset контрольное значение VD зашифровывается с помощью ключа PVK, после чего из полученного значения с помощью таблицы децимализации DT получается блок из 16 десятичных цифр.

Из полученного блока берутся первые N цифр, где N – длина PIN (метод IBM 3624 позволяет проверять PIN с длиной до 16 цифр), далее из каждой цифры PIN по модулю 10 вычитается соответствующая цифра полученного блока. Полученное значение и будет значением PIN offset.

Проверка PIN

Терминология

Для упрощения дальнейшего описания введём некоторые термины:

- PIN блок – значение PIN кода карты, некоторым специальным образом упакованной в блок из 8 байт. Стоит пояснить, что никакого шифрования в данном процессе не используется. Способы упаковки, в данном случае, бывают разные, но это не принципиально.
- Зашифрованный PIN блок – значение PIN блока, зашифрованное по алгоритму DES/3DES с помощью ключа (ключа терминала, банка, платежной сети, пр.), специально выделенного для целей шифрования PIN блока.
- Проверочное значение PIN – PVV или PIN offset в зависимости от того, какой метод проверки PIN используется.
- Дополнительные данные проверки PIN – данные, кроме PIN и проверочного значения PIN, необходимые для проверки PIN в соответствии с алгоритмами Visa PVV/IBM 3624 PIN offset в соответствии со списком, приведенным в описании алгоритмов (см. выше).

Требования платежных систем

В части проверки PIN можно указать следующее:

- Открытые значения PIN и PIN блока не должны никаким образом передаваться, храниться или обрабатываться вне специально отведенных программно аппаратных комплексов (HSM на стороне процессинговых систем или EPP и некоторых других страшных абревиатур на стороне терминальных устройств(банкоматы, POS-терминалы и пр.)).
- Зашифрованный PIN блок не должен храниться после завершения операции в системах, отвечающих за онлайн/оффлайн обработку транзакций (есть ещё системы, от-

вечающие за выпуск самих карт, их это требование не касается).

Просмотр PIN

Как мы уже определились ранее, для проверки PIN нам необходимы следующие данные:

- Сам PIN, который мы будем проверять
- Проверочное значение PIN
- Дополнительные данные проверки PIN

С PIN все достаточно просто. Как уже указано выше, открытое значние PIN мы получить не можем ни при каких условиях. Таким образом, нам остается только зашифрованный PIN блок. В дополнение к нему нам нужен ключ для его расшифровки. Назавем этот ключ PPK (PIN protection key, термин взят из документации на HSM фирмы SafeNet).

Далее необходимо определиться с проверочным значением PIN и дополнительными данными.

Первый вариант – это хранение проверочного значения на магнитной полосе карты после поля Service Code. Модифицированную версию ISO 7813 с указанием того, где хранится PVV, можно посмотреть здесь. По приведенному описанию формата треков стоит добавить, что под 5-и символьным значением PVV подразумевается следующая последовательность 1 символ PVKI и 4 символа самого PVV, а для PIN offset – значение PIN offset для PIN из 5 цифр. Если PIN имеет отличную от 5 цифр длину, то размер PIN offset, соответственно, изменится. Какие плюсы у этого метода. Безусловно – возможность проверять PIN для любого, кто будет иметь необходимые для проверки ключи. Здесь стоит заметить, что при запуске нового карточного подукта в платежную сеть, обычно, передаются ключи, на которых выпущена карта. Таким образом, при использовании данного метода возможность проверки PIN появляется как у самого эмитента карты, так и у платежной сети. К недостаткам такого метода можно отнести то, что данный вариант делает PIN карты статическим до тех пор, пока карта не будет перевыпущена.

Второй вариант – это хранение проверочного значения в некотором хранилище, обычно, БД системы, отвечающей за выполнение проверок при авторизации карты. В этом случае при проверке PIN необхоидмо извлечь проверочное значение из этого хранилища, а уже потом, выполнять проверку, используя это значение. Как следствие, при использовании данного метода, невозможно вполнять проверку PIN во внешней системе (в той же платежной системе) и она м.б. выполнена только в той системе, которая имеет доступ к хранилищу проверочных значений. Однако, такая система позволяет изменять PIN код карты без каких либо затрат на смену пластика (для чего это нужно, что при этом необходимо сделать и какие после этого м.б. проблемы, описывать не буду, т.к. это находится за рамками данной статьи).

Независимо от того, каким образом и кем (эмитент карты или платежная сеть) была получена вся необходимая информация, сама проверка PIN выполняется на HSM, который для выполнения проверки получает ключ PPK в защищенном виде, ключ проверки PIN в защищенном виде, зашифрованный PIN блок, проверочное значение PIN и дополнительные данные проверки, в ответ на что возвращается только результат проверки: верный PIN, неверный PIN, прочая ошибка. Т.е. в процессе проверки система, отвечающая за авторизацию, с самим открытым значением PIN кода никак не соприкасается.

III. Банковское мошенничество

Реквизиты банковской карты – это секретная информация. Если она попадёт в руки не тех людей, вы можете потерять деньги. Реквизиты – это всё, что написано на карте: номер из 16 цифр, имя и фамилия владельца, срок действия и трехзначный код безопасности на обратной стороне. Для удобства мы отнесём к реквизитам и смс-код, который присылает вам банк, когда вы платите в интернете или переводите деньги.

По правилам платёжных систем реквизиты нельзя сообщать посторонним. Если банк узнает, что ваши реквизиты попали в чужие руки, то сразу заблокирует карту. Однако кое-что сообщать всё-таки можно. Разберёмся на примере, какую информацию содержит Ваша пластиковая карта.

1. Наименование и/или логотип банка-эмитента – наименование и/или логотип банка, выпустившего платёжную карточку.

2. Чип – микросхема, вшитая в пластик и выполняющая ту же роль, что и магнитная полоса, т.е. обеспечивающая проведение расчётов с помощью платёжной карточкой.

3. Номер карточки – 16 цифр, идущих в ряд.

4. Имя и фамилия держателя платёжной карточки.

5. Срок действия – указывается на карточке в формате ММ/ГГ и показывает до какого момента времени (включительно) действительна карта.

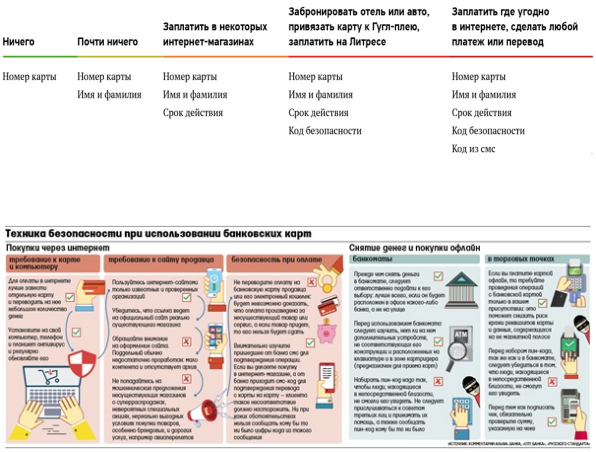
6. Бренд платёжной системы.

7. Магнитная полоса – полоса, содержащая необходимые данные для проведения расчётов с использованием платёжной карточки.

8. CVV2 (CVC2) – трехзначный код на оборотной стороне карточки, обеспечивающий дополнительную безопасность, предназначенный специально для проведения расчётов в сети.

9. Полоса для подписи – место, где держатель ставит свою подпись.

Что может сделать мошенник, который завладел вашими реквизитами?



IV. Вывод

Таким образом, на нынешний момент ваши деньги хорошо защищены. Но в каждом деле есть исключения. Поэтому огромная просьба: не передавайте реквизиты своих карт посторонним людям и соблюдайте технику безопасности.

Список использованных источников

1. Иванова, В. М. Случайные числа и их применение, 1984
2. https://www.belinvestbank.by/individual/page/moshennichestvo-v-seti-internet
3. Visa Payment Technology Standards Manual

Фролов Ярослав Ильич, студент кафедры информационных технологий автоматизированных систем БГУИР, iaroslav_frolov@mail.ru.

Лемеза Марк Викторович, студент кафедры информационных технологий автоматизированных систем БГУИР, suslik2034@gmail.com.

Научный руководитель: Гуринович Алевтина Борисовна, заместитель декана по научно-методической работе БГУИР, кандидат физ.-мат. наук, доцент кафедры ВМиП, gurinovich@bsuir.by.