ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ТҰҢҒЫШ ПРЕЗИДЕНТІ - ЕЛБАСЫНЫҢ ҚОРЫ

«ҒЫЛЫМ ЖӘНЕ БІЛІМ – 2017»

студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ – 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«SCIENCE AND EDUCATION - 2017»

14th April 2017, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

«Ғылым және білім - 2017»
студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«Science and education - 2017»

2017 жыл 14 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2017» студенттер мен жас ғалымдардың XII Халықаралық ғылыми конференциясы = The XII International Scientific Conference for students and young scholars «Science and education - 2017» = XII Международная научная конференция студентов и молодых ученых «Наука и образование - 2017». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2017. – 7466 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-827-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-827-6

примере Business Intelligence. Рассмотрены основные положения технологии бизнес интеллекта в Visual Studio, внутренние интерфейсы Microsoft SQL Server. Разработано приложение для многомерного анализа данных в сфере продаж розничной сети бытовой и электронной техники, увеличивающая эффективность работы менеджеров, аналитиков компании.

Список использованных источников

1. Codd E. F., Codd S. B., Salley C. T. Providing OLAP to User-Analysts: An IT Mandate //Arbor Software Corp. Papers. 1996. P.3 - 20.
2. Йохан Потгитер «Масштабируемость OLAP-данных» [Электрон. ресурс] – 17 мая 2010. – Режим доступа: http://www.citforum.ru
3. Миронов В.В., Макарова Е.С. Агрегация показателей в OLAP-кубе при сведении по зависимым измерениям. // Вестник УГАТУ, Т. 16, № 3 (48). 2012. С. 180 – 186.

УДК 004.056.53

СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА С КЛЮЧОМ МНОГОРАЗОВОГО ИСПОЛЬЗОВАНИЯ

Кукенова Ж.А.
Kukenova-95@mail.ru

Студентка 4 курса, факультет информационных технологий, группа ИС-44
Научный руководитель: к.н.ф.н Ла Лира Львовна
Евразийский национальный университет им Л.Н.Гумилева

ВВЕДЕНИЕ

Рассмотрим следующую ситуацию. Вы заведующий лабораторией, в которой находятся очень дорогие и опасные медикаменты, неправильное использование которых может привести к летальному исходу. Вы нанимаете трех лаборантов, которые умеют обращаться с данными веществами, но вы не доверяете им, так как они могут украсть дорогостоющие медикаменты, то есть вы не доверяете ключ-комбинацию от входной двери лаборатории отдельному лабораранту. Предположим, вам нужна такая система, посредством которой два из трех лаборантов могли бы получить доступ к лаборатории, но не один отдельный лаборант войти в лабораторию не мог. Данная проблема может быть решена посредством схемы разделения секрета. Под схемой разделения секрета понимается процедура разделения секрета на доли и процедура восстановления секрета при знании некоторых его долей. В 1979 году А. Шамиром была предложена пороговая, идеальная схема распределения секрета, суть которой заключается в том, что части «секрета», назовем его ключ, распределены между участниками схемы так, что восстановить его могут только достаточно большие подгруппы участников. Приведем формулировку схемы [1]:

Пусть t, w – положительные целые числа такие, что $t \leq w$. Тогда (t,w)-*пороговой схемой разделения секрета* называется метод разделения информации о ключе K среди w участников (множества которых обозначим через П) такой, что любые t участников из П могут вычислить значение K, но никакая группа из (t – 1) участников не сможет его вычислить.

Данная схема имеет ряд полезных свойств [1,2]:

1.Безопасность – обеспечивается положениями теории информационной безопасности.

2.Минимальность – размер каждой части не превышает размер начальных данных.

3.Расширяемость – когда t (количество человек, которое необходимо для раскрытия секрета) фиксировано, остальные части могут быть динамически добавлены или удалены, не затрагивая другие части.

4. Гибкость – в организациях, где важна иерархия, мы можем предоставить каждому участнику, разное количество долей в зависимости от их важности внутри организации.

Слабые стороны:

1.Недоверие среди участников.

2.Можно подобрать ключ недостающего участника посредством перебора комбинаций.

3. Одноразовость ключа. Ключ после первого использования становится известным и не может быть использован вторично.

1. СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА ШАМИРА

Модель Шамира базируется на том факте, что для конкретного возобновления многочлена степени *t-1* требуется не менее *t* его значений в любых *t* попарно различных точках. Приведем формальное представление пороговой схемы Шамира [1].

Допустим K = Z_p, где $p \geq w + 1$ является простым числом. Кроме того, пусть $\Sigma = Z_p$. Ключ будет элементом из Z_p так же, как и каждая доля, данная участнику. В схеме дилер создает случайный полином $a(x)$ степени не больше $(t - 1)$, в котором свободный член является ключом K. Каждый участник P_i , i=1,2,…,w получает некоторую точку (x_i,y_i) на графике этого полинома.

(*t, w*) - пороговая схема Шамира в Z_p.

Стадия инициализации.

1. Дилер D подбирает w различных, ненулевых компонентов из Z_p, обозначенных через x_i, $1 \leq i \leq w$ (вот почему мы требуем $p \geq w+1$). Для каждого $1 \leq i \leq w$ дилер D дает значение x_i участнику P_i. Значения x_i известны всем.

Распределение долей.

2. Предположим, что D хочет разделить секретный ключ $K \in Z_p$. Для этого D тайно выбирает (независимо и случайно) $t - 1$ элементов из Z_p, отличных от нуля; обозначим их через $a_1..., a_{t-1}$.

3. Для $1 \leq i \leq w$ дилер D вычисляет $y_i = a(x_i)$, где

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p .$$

4. Для $1 \leq i \leq w$ дилер D дает долю y_i участнику P_i.

Для восстановление ключа можно использовать интерполяционную формулу Лагранжа, которая дает явное выражение для вычисления (единственного) многочлена степени не выше $(t - 1)$ по следующей формуле:

$$a(x) = \sum_{j=1}^{t} y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \bmod p$$

Просто проверить точность данной формулы: при подстановке $x = x_{i_j}$ все слагаемые в суммировании пропадают, за исключением времени j-го слагаемого, которое равно y_{i_j}. Подобным способом, мы имеем полином степени не выше $(t - 1)$, план - график которого содержит t упорядоченных пар (x_{i_j}, y_{i_j}), $1 \leq j \leq t$.

При возобновлении ключа группа, состоящая более чем из t участников, показывает

свои собственные доли $a(x_k)$, $1 \le k \le l$, $l \ge t$ и, используя, например, интерполяционную теорему Лагранжа, строит единственный полином степени $t-1$, пересекающий t точек $(x_k, a(x_k))$, свободный член которого равен K. При этом исполняются следующие качества:

1. Знания t долей достаточно, чтобы определить ключ K.

2. Знание различных $t-1$ долей не представляет никаких данных о ключе K.

Группа B из t участников способна вычислить $a(x)$ применяя интерполяционную формулу. Однако допустимо упрощение, так как участники из B не обязаны возобновлять полином $a(x)$ целиком. Для это их достаточно определить независимый член $K = a(0)$. Таким образом, все они смогут определить лишь следующее выражение, которое получено с помощью подстановки $x = 0$ в интерполяционную формулу Лагранжа:

$$K = \sum_{j=1}^{t} y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \bmod p$$

То есть ключ это линейная комбинация t долей.

2. ОДНА МОДИФИКАЦИЯ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА А. ШАМИРА

Хотя метод Шамира работает сравнительно отлично, но он, как уже отмечалось, обладает рядом слабых сторон, перечислим некоторые примеры.

1. Одноразовость ключа. После одного применения ключ необходимо заменить, поскольку он уже становится известным не менее чем t участникам схемы-секрета.

2. Отсутствие безопасности от мошенников являющихся участниками схемы.

В [3,4] были рассмотрены подходы к определению схемы разделения секрета с ключом многоразового использования. Рассмотрим вторую проблему. Предположим, что группа из t участников схемы решила восстановить ключ, при этом k участников-злоумышленников хотят ввести в заблуждение остальных $t-k$ участников, предъявив ложные доли и узнать истинные доли честных участников. Схема Шамира не позволяет защититься от злоумышленников такого рода. Для решения этой проблемы, А. Шамиром было предложено выбирать ключи меньше, некоторого заданного S [1]. Но следующий пример показывает, что любые k участников-злоумышленников, могут ввести в заблуждение остальных $t-k$ участников группы, выдав ложные доли D_i', при этом у построенного полинома $a'(x)$ свободный член K' будет меньше S.

Пример [5]. Возьмем следующее, что группа из t участников схемы решила возобновить ключ. Участники-мошенники с номерами $i_1, ..., i_k$ начинают выстраивать полином $\Delta(x)$ такой, что $\Delta(0) = -1$, $\Delta(j_s) = 0$, $s = 1, ..., t-k$, j_s – номера добросовестных участников схемы-секрета и предъявляют для возобновления ключа неверные доли $D'_{i_l} = a(i_l) + \Delta(i_l)$, $1 \le l \le k$.

Добросовестные участники схемы-секрета j_s, $s = 1, ..., t-k$ предъявляют свои доли D_{j_s} и строится полином $a'(x)$ в степени $t-1$, который пересекает t точек (i_l, D'_{i_l}), (j_s, D_{j_s}), $1 \le l \le k$, $1 \le s \le t-k$. Имеем $a'(i) = a(i) + \Delta(i)$, $1 \le i \le t$.

Из неповторимости $a'(x)$ следует, что $a'(x) = a(x) + \Delta(x)$, $\forall x \in Z_p$. Значит, разработанный ключ, являющийся свободным членом $a'(x)$, равен $K' = K - 1 < S$.

В данной р**а**боте предлагается одна схема распределения секрета, являющаяся одной модификацией (t, w)-пороговой схемы А.Шамира, М. Томпа, Х. Уолла с ключом многоразового пользования, которая будет защищена от различных вариантов злоумышленников описанных в примере.

В предложенной схеме Дилер, помимо выдачи уникальных долей, может выдавать

каждому отдельному участнику его порядковый номер, который также будет секретным, тогда как , при использовании секрета Шамира, каждый отдельный участник знал порядковый номер другого.

Фаза инициализации.

1. Дилер *D* выбирает *w* различных, ненулевых, простых элементов из Z_p, обозначенных через x_i, $1 \le i \le w$. Для каждого $1 \le i \le w$ дилер D дает значение x_i участнику P_i. Значения x_i становятся не известными простыми числами.

Распределение долей.

2. Предположим, что *D* хочет разделить секретный ключ $K \in Z_p$. Для этого *D* тайно выбирает (независимо и случайно) $t-1$ элементов из Z_p, отличных от нуля; обозначим их через $a_1 ..., a_{t-1}$.

3. Для $1 \le i \le w$ дилер *D* вычисляет $y_i = a(x_i)$, где

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p .$$

4. Для $1 \le i \le w$ дилер дает долю $y_i = a(x_i)$ участнику P_i.

Ключ схемы это множество пар $\left\{ \left(K, D_\alpha\right) | D_\alpha = x_{i_1}, x_{i_2}, ..., x_{i_t}, \alpha = < i_1, i_2, ..., i_t >, 1 \le i_1, i_2, ..., i_t \le \mathrm{w} \right\}$. Знание любой из пары принадлежащей ключу открывает доступ к нашему секрету.

Процесс возобновления ключа участниками схемы происходит именно так. Пусть множество участников $\beta = \{ j_1, ..., j_t \}$ решило забрать пару $\left(K, D_\beta\right)$ из ключа.

1. Каждый участник выдает секретные доли $(x_j, a(x_j))$, $1 \le s \le t$.

2. Возобновляем полином $a(x)$ со свободным членом K, вычисляем произведение $D_\beta = x_{j_1}, x_{j_2}, ..., x_{j_t}, \beta = < j_1, j_2, ..., j_t >$ участники группы получают $\left(K, D_\beta\right)$ из ключа.

После использования пара $\left(K, D_\beta\right)$ становится нерабочей и должна быть удалена из ключа. Остальная часть ключа пригодна для работы.

Свойства схемы разделения секрета.

1. Ключ схемы можно использовать достаточно много раз. После использования одной подруппой участников, ключ остается рабочим для дальнейшей работы, поскольку знание одной из оставшихся частей ключа (представленной парой $\left(K, D_\alpha\right)$), не дает более никакой информации об оставшихся его частях.

2. Схема защищена от ряда мошенников, когда k участников хотят ввести в обман оставшихся $t-k$ участников, дав им неверные части и узнать истинные доли добросовестных участников.

3. Каждому α соответствует неповторимое D_α , что обеспечивает уникальность ключа для всех из подмножеств с t участников.

Список использованных источников

1. Shamir, Adi *(1979), "How to share a secret", Communications of the ACM, 22 (11): 612–613,* doi:10.1145/359168.359176

2. *Dawson, E.; Donovan, D. (1994), "The breadth of Shamir's secret-sharing scheme", Computers & Security, 13: 69–78,* doi:10.1016/0167-4048(94)90097-3.

3. Е.Р. Байсалов, Ж.М. Тунликбаева Многоразовая схема разделения секрета\\ Труды

межд. конф. «Actual problems of computer sciences», Алматы, КазНУ, 2003, 143-145

4. Л.Л. Ла, М. Нугманов Об одной многоразовой схеме разделения секрета Вестник КазНПУ им.Абая, серия «Физико-математические науки», N (29), Алматы, 2010, 163-166.

5. M. Tompa, H. Woll How to Share a Secret with Cheaters\\ Proceedings on Advances in cryptology – CRYPTO '86, Santa Barbara, California, United States, pp. 261 – 265, 1987.

ҚАЗАҚ ТІЛІНДЕГІ МӘТІНДІ СЫН ЕСІМДЕР НЕГІЗІНДЕ СЕНТИМЕНТ ТАЛДАУ

Қажымұхан Дина Асқарқызы
askarovna0105@mail.ru
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық технологиялар факультеті, Информатика және ақпараттық қауіпсіздік кафедрасы, 5В060200 – Информатика мамандығының 4 курс студенті, Астана, Қазақстан
Ғылыми жетекшісі - Бурибаева А.К.

Жалпы сентимент талдау деп табиғи тілдегі мәтінді өңдеу әдістері, статистика, машиналық оқыту көмегімен пікірдің эмоционалдық реңкін анықтауды айтамыз [1]. Бұл технология жаңа жағдайлар, өнімдер, ұйым, мемлекет және т.б. жағдайларды автоматты түрде бағалау үшін қолданылады [2].

Бүгінгі күні әлеуметтік желі, онда пікір қалдыру әр адамның күнделікті ісіне айналды. Әлеуметтік желі қолданушылары жаңалықтарға байланысты посттарға пікір қалдырып, өз ойларын білдіріп жатады. Әлеуметтік желі кең қолданыста болмаған кезде көптеген жылдар бойы «Адамдар не ойлайды?» деген сұраққа әлеуметтік саулнамалар көмегімен жауап алу бір топ адамдарын ойын зерттеу тәсілі болып келді [4]. Интернетке кең қолданыс және әлеуметтік медиа, әлеуметтік топтардың ойын зерттеудің жаңа тәсілі – сенимент талдауды ұсынады. Алынған ақпаратты және оның қолданылуын талдау маркетингтік, саясат зерттеулерінде, жаңалықтарға әлеуметтік желі қолданушыларының әсерін қадағалау артықшылығын береді. Динамикалық түрде өсіп отыратын Интернеттегі ақпаратты өңдеу, әлбетте, автоматтандырылған ақпараттық технологиялар көмегінсіз іске аспайды.

Сентимент-талдаудың басқа тапсырмасы, пікірлердігі спамдарды, салыстыруларды іздеу үшін, аспектерді анықтау ретінде қолданылуы болып табылады [3].

Мәтіннің реңкін автоматты түрде анықтау үшін келесі тәсілдер бар:

1. Ережелер негізіндегі үлгілерді (rule-based with patterns) қолдану тәсілі. Ол мәтіннің реңкін анықтайтын ережелерді құрудан тұрады. Ол үшін мәтін сөз немесе сөздер тіркесіне (N-grams) бөлінеді.Одан кейін, алынған мәліметтер, жағымды немесе жағымсыз бағалау берілетін үлгілерді белгілеу үшін қолданылады. Белгіленген үлгілер «ЕГЕР шарт, ОНДА қорытынды» түріндегі ережені құру кезінде қолданылады.
2. Оқытушысыз машиналық үйрету (unsupervised learning). Бұл тәсіл мәтіннің көп бөлігін терминдер алатынды деген идеяға сүйенеді. Терминдерді реңкін анықтау арқылы, барлық мәтіннің реңкі туралы қорытынды шығаруға болады.
3. Оқытушымен машиналық үйрету (supervised learning). Бұл тәсілге мәтіннің эмоционалды кеңістік шеңберінде белгіленген, базасында статистикалық немесе ықтималдық жіктеуіші (мысалы, байесовский) құрылатын оқыту жиынтығының болуы талап етіледі.
4. Гибридті тәсіл (hybrid method). Осы тәсіл жоғарыда қарастырылған барлық немесе бірнеше принциптерді үйлестіреді және анықталған тізбек негізіндегі классификаторларды қолданудан тұрады [5];
5. Теориялық-графтық модельдерге негізделген әдіс. Құжаттың мәтіндік корпусындағы барлық сөздер тең мағыналы еместігі жайлы болжам осы әдіс негізінде қолданылады. Кейбір сөздер салмағы үлкен болады және мәтін реңкіне қаттырақ әсер етеді. Бұл әдісті қолдану кезінде реңкті анықтау бірнеше кезеңдерге бөлінеді. 1) зерттелетін