Бабаш А.В, Баранова Е.К.
Национальный исследовательский университет «Высшая школа экономики»

Совершенные шифры. Один новый совершенный шифр

1. J. Katz, Y. Lindell. Introduction to modern cryptography, 2008, p. 553.
2. Bruce Shneier. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C by Wiley Computer Publishing.
3. Bruce Shneier. An Introduction to Cryptography. 2003. 86 p.
4. Encyclopedia of Cryptography and Security. Springer. 2011.
5. Б. Шнайер Секреты и ложь. Безопасность данных в цифровом мире/ СПб.: Питер, 2003. 368 с.
6. Godlewsky P. Key minimal cryptosystems for unconditional secrecy. Cryptology, 1990, № 3.
7. А.Ю. Зубов Совершенные шифры. М. Гелиос АРВ, 2003.
8. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии. М., Гелиос АРВ., 2003.
9. И.Н. Васильева. Криптографические методы защиты информации. М. Юрайт, 2016. стр.64.
10. С. В. Запечников, О.В. Казарин, А.А. Тарасов. Криптографические методы защиты информации. М., Юрайт, 2017.
11. О.Н. Жданов, В.В. Золаторев,. Методы и средства криптографической защиты информации. Учебное пособие. Сиб ГАУ. Красноярск, 2007, 217стр.
12. Фомичев В.М. Методы дискретной математики в криптографии. М.:ДИАЛОГМИФИ, 2010

- **ОПРЕДЕЛЕНИЕ 2.3 [1]** Схема шифрования с пространством открытых сообщений X является совершенно секретной, если для каждого распределения вероятностей на множестве X для каждого сообщения $x \in X$ и каждого зашифрованного текста $y \in Y$ (для которого вероятность $P(y)>0$) выполняется:

  - $P(x/y)=p(x)$.

- (Требование, чтобы $P(y)>0$ является техническим, оно необходимо для предотвращения принадлежности события с нулевой вероятностью.)

- В наших учебниках обычно фиксируют вероятностные распределения на множестве открытых текстах X и множестве ключей K. Российские криптографы называют такие шифры «совершенными шифрами по К. Шеннону» и относят их к теоретически стойким шифрам.

- Авторы приведенных источников [1-11] утверждают, что такие шифры не дешифруемы.
- Bruce Schneier: Даже после того, как инопланетяне из Андромеды приземлятся с их массивными космическими кораблями и немыслимыми вычислительными мощностями, они не смогут прочитать советские шпионские сообщения, зашифрованные одноразовыми колодками.
- J. Katz, Y. Lindell: схемы шифрования, которые являются безопасными даже против противника с неограниченной вычислительной мощностью. Такие схемы называются совершенно секретными.
    - Б. Шнайер: Кодирование одноразового использования это единственный, безопасность которого может быть доказана.
    - С. В. Запечников, О.В. Казарин, А.А. Тарасов: Теоретически существует совершенно секретный шифр (иными словами, абсолютно стойкий шифр), но единственным таким шифром является одна из форм так называемого одноразового шифрблокнота, в которой открытый текст комбинируется с полностью случайным ключимеющийся у нас алгоритмом такой же длины.
    - Заметим, что эти авторы видимо заметили подвох. Они выразили сомнение: ключи, выработанные с помощью некоторого датчика истинно случайных чисел, будут качественными с вероятностью, отличающейся от единицы на ничтожно малую величину.

- Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин:

При рассмотрении вопроса о теоретической стойкости шифров отвлекаются от реальных временных и сложностных затрат по вскрытию шифра (что определяет подход к практической стойкости). Во главу угла ставится принципиальная возможность получения некоторой информации об открытом тексте или использованном ключе. Впервые такой подход исследовал К. Шеннон [Шен63]. Он рассматривал уже знакомую нам модель шифра и единственную криптоатаку на основе шифртекста. Проследим за его рассуждениями.

Как мы указывали, конечной целью работы криптоаналитика является текст сообщения или ключ шифрования. Однако весьма полезной может быть даже некоторая вероятностная информация об открытом тексте. Например, уже предположение о том, что открытый текст написан по-английски, предоставляет криптоаналитику определенную априорную информацию об этом сообщении даже до того, как он увидит шифртекст. Так, например, он заранее знает, что слово “hello”

- Вот как описывает эти шифры Ф.М. Фомичев [12] «История развития шифров поставила перед специалистами ряд неизбежных вопросов: существуют ли нераскрываемые шифры? Если существуют, то как они должны быть устроены? Каковы условия, обеспечивающие нераскрываемость шифра?» Из такого описания нераскрываемого шифра следует вывод, что не имеет смысла тратить силы, средства и время для дешифрования шифрованного сообщения.

- Криптографы делят методы криптоанализа на два класса: бесключевые методы, когда методы дают возможность определить открытый текст, не определяя секретный ключ, и методы с предварительным определением ключа. В последнем случае открытый текст читается путем расшифрования шифрованного текста на найденном ключе.

- В работе [Бабаш А.В., Шанкин Г.П. Криптография. М., Солон-Р, 2002] было дано уточнение определения совершенного шифра. Мы указали, что это определение относится **к нападению на открытый текст** по известному шифрованному тексту.

К нападению на ключ следует отнести Замечание на стр.89 [Бабаш А.В., Шанкин Г.П. Криптография]. **Шифр с множеством открытых текстов X и множеством ключей K является совершенным по нападению на ключ при перехвате шифрованного текста, если для заданных распределений вероятностей на множествах X и K для каждого сообщения m∈M и каждого зашифрованного текста y∈Y выполняется:**

- **p(k/y)=p(k).**

- Теорема 1. При не равновероятном вероятностном распределении на множестве открытых текстов и равновероятном распределении на множестве ключей шифр случайного гаммирования не является совершенным при нападении на ключ при перехвате шифрованного текста.
- Доказательство. Известно, что условие: при любых k, c
  - $p(k/c)=p(k)$
- равносильно условию
  - $p(c/k)=p(c)$
- при любых k, c. Ясно, что $p(c/k)=p(m)$ для открытого текста m зашифрованного ключом k в c. Теперь утверждение теоремы непосредственно следует из условия не равновероятности распределения на множестве открытых текстов.

- Таким образом, шифр случайного гаммирования является практическим шифром. В случае, когда длина ключей достаточно большая одним из методов его дешифрования является нападение на ключ методами дешифрования шифра Виженера. В частности, можно применить метод благоприятного события [Бабаш, Шанкин 2002] в поиске шифрованного текста, зашифрованного локально периодической гаммой [Бабаш, Шанкин 2002].

- Определение 2. Шифр называется не дешифруемым, если он совершенный как при нападении на открытый текст, так и нападении на ключ при перехвате шифрованного сообщения.

- Теорема 2. (сообщение Алиева Ф.К) При равновероятном вероятностном распределении на множестве открытых текстов $M=I^N$ и множестве ключей $K=I^N$, $I=\{1,\ldots,|I|-1,0\}$ шифр случайного гаммирования является не дешифруемым.

- Доказательство очевидно.

- **Шифр Тук тук (название условное)**
- I - алфавит открытого, текста, X_L подмножество открытых текстов множества I^L, $K=I^N$ – множество ключей. Множество шифрованных текстов Y состоит из всех упорядоченных наборов L натуральных чисел $j_1< j_2<\ldots< j_L$, где $1\leq j_1, j_L\leq N$. Частично определенная функция шифрования $F:X_L\times K \rightarrow Y$ – задана алгоритмом: для пары: открытый текст $x=i_1i_2\ldots i_L$ и ключ $k=\alpha(1)\alpha(2)\ldots\alpha(N)$ последовательно определяется шифрованный текст это последовательность упорядоченных номеров $y= j_1< j_2<\ldots< j_L$. Если ключ не содержит буквы i_1, то шифртекст не определен. В противном случае номер j_1 это номер первой буквы i_1 в ключе k: $\alpha(j_1)= i_1$, $\alpha(j)\neq i_1$ для $j<j_1$. Если $i_2\neq\alpha(j)$ для всех j из $\{j_1+1, j_1+2,\ldots N\}$, то шифртекст y не определен. В противном случае число j_2 определено условием: $\alpha(j_2)=i_2$, $\alpha(j)\neq i_2$ для $j_1< j <j_2$. Аналогично шифруются буквы $i_3,\ldots,i_L$.
- Процесс расшифрования очевиден. По шифрованному тексту $y=j_1<j_2<\ldots<j_L$ – номерам ключа определяем буквы ключа - $i_1, i_2,\ldots i_L$ – то есть открытый текст.

Пусть на множестве открытых текстов открытых текстов X_L задано вероятностное распределение $P(X_L)=(p(x(1),\ldots, p(x(W))$ и на множестве ключей K задано вероятностное распределение $P(K) = (p(k) = \frac{1}{|K|}, k \in K)$

Данные распределения индуцируют вероятностное распределение $P(Y) = (p(y), y \in Y)$ и условные вероятностные распределения $P(Y/x)$, $x \in X_L$.

Определение 1.Модель шифра по К. Шеннону совершенна по нападению на открытый текст, если для всех $x \in X_L$ и $y \in Y$

$$p(y/x)=p(y)\neq 0$$

Теорема 1. Шифр «Тук тук» является совершенным по нападению на открытый текст.

Доказательство. Фиксируем $y=j_1< j_2<\ldots< j_L$ из Y и $x=i_1i_2\ldots i_L$ из X_L. Тогда формула

$$P(j(1) < j(2) < \ldots < j(L)/i_1 i_2 \ldots i_L) = (1 - \frac{1}{|I|})^{j(L)-L} (\frac{1}{|I|})^{L}$$

представляет собой сумму вероятностей всех ключей зашифровывающих $x=i_1i_2\ldots i_L$ в $y=j_1< j_2<\ldots< j_L$..

Пусть $X_K(y)$ –открытые тексты, которые могут зашифроваться в $y=j_1<j_2<\ldots< j_L$ при соответствующем выборе ключа. Очевидно, что $X_K(y)= X_L$. Имеем

$$p(y)= \sum_{x \in X_L} p(y/x)\,p(x) = (1 - \frac{1}{|I|})^{j(L)-L} (\frac{1}{|I|})^{L} \sum_{x \in X_L} p(x) = (1 - \frac{1}{|I|})^{j(L)-L} (\frac{1}{|I|})^{L}$$

Определение 2. Модель шифра по К. Шеннону совершенна по нападению на ключ, если для всех $x \in X_L$ и $k \in K$.

$$p(y/k)=p(y)\neq 0$$

Теорема 2. Модель шифра «Тук тук» не является совершенной по нападению на ключ.

Доказательство. Ключу k и шифрованному тексту y соответствует открытый текст x. Вероятность $p(y/k)=p(j_1<j_2<\ldots<j_L/k)$ есть вероятность того, что последовательность $\alpha(j_1)\alpha(j_2)\ldots\alpha(j_L)$ знаков ключа k принадлежит X_L. Следовательно, эта вероятность равна либо нулю, либо единице. Это противоречит значению p(y) согласно (1).

В целях экономии ключевой информации будем последовательно шифровать нужные нам содержательные тексты на одном ключе k. Или, что тоже самое, шифровать один открытый содержательный текст, длины L намного большей, чем N. В связи с чем, мы вводим новую функцию шифрования, использующую известную идею переноса слов на другую строку при печати содержательных текстов в книге. Отличие от алгоритма F заключается в том, что при шифровании текста $i_1 i_2 \ldots i_L$ при первой невозможности зашифровать первую i_j букву ($1<j$) из $i_2 \ldots i_L$, то есть, найти по приведенным правилам $\alpha(j)=i_j$, начинаем шифровать текст $i_j i_{j+1} \ldots i_L$ на этом же ключе k.

- **Дешифрование Тук тук.**
- Шифруем открытый текст $x=i_1 i_2 \ldots i_L$, i_m из I, L>>N, в котором **буква** α встретилась v(α) раз, v(α) – неизвестно.
- 1 2 3 4 5 6 7 … N-1 N номера символов ключа
- α(1)α(2)α(3) α(4)… α(N) ключ, (α(j) из I)
- Для каждой буквы α из I выписываем **номера букв ключа** зашифровывающих эту букву α. α [**3**:v(3), **6**:v(6), …**m**:$v(m_\alpha)$]. Номер **j** ключа использовался v(j) раз, v(j) –известны и v(3)+v(6)+….+ $v(m_\alpha)$= v(α), m_α - неизвестно .
- При достаточно большом L частоты v(α) букв открытого текста приблизительно известны. При и достаточно большом L>>N значения частот : v(3), v(6), …v(m), соответствующие каждой букве α, выравниваются v(3)≈v(6) ≈ …. ≈$v(m_\alpha)$≈v. При большом различии вероятностей букв открытого текста можно ранжировать их по величине v и привязать частоты к зашифрованной неизвестной букве α.

- **Нижняя оценка необходимой длины открытого текста для полного определения ключа**
- Ключ выбран случайно и равновероятно. Пусть p(α) вероятность буквы α в открытых текстах. Перейдем на язык ящиков и дробинок и подсчитаем на языке средних значений необходимую длину открытого текста для полного определения ключа. Среднее число ящиков в случайном ключе, содержащих букву α, есть $N|I|^{-1}$ для любого α. Число дробинок для ящиков помеченных α есть $n(\alpha)=Lp(\alpha)$. Положим
- $$B(\alpha)=\frac{n(\alpha)}{N|I|^{-1}}=\frac{Lp(\alpha).}{N|I|^{-1}}$$
- По известным формулам среднее число пустых ящиков оценивается сверху величиной

$$N|I|^{-1}e^{-B(\alpha)}$$

  - Полагая, что число пустых ящиков для самой редкой буквы максимально, можно оценить L ограничивая последнюю величину сверху единицей.

СПАСИБО!