РусКрипто16

Бабаш А.В.

Совершенные шифры.

- В работах Клода Эльвуда Шеннона, опубликованных в 1938-1962 годах и переведенных на русский язык в 1963г. описаны так называемые «совершенные шифры». Иногда, в современных терминах их называют теоретически стойкими шифрами.
- Примером такого шифра является шифр случайного гаммирования. Входным алфавитом такого шифра является множество номеров I={0,1,…N-1} букв упорядоченного алфавита открытых текстов. Тогда множество I^L является множеством возможных для шифрования текстов длины L. Одновременно I^L является множеством ключей шифра и множеством шифрованных текстов. Процесс шифрования открытого текста $i=i_1,i_2,\ldots,i_L$ случайно и равновероятно выбранным ключом $\gamma=\gamma_1,\gamma_2,\ldots,\gamma_L$ описывается уравнениями
  - $i_j+\gamma_j=z_j \mod N,\ j\in\{0,1,\ldots L\},$
- где $z=z_1,z_2,\ldots,z_L$ - шифрованный текст.
- Очевидно, в шифрованный текст z может быть зашифрован любой открытый текст i при подходящем выборе ключа γ. Таким образом, зная шифрованный текст, восстановить открытый текст не представляется возможным.

Более точно. **Алгебраическая модель шифра К. Шеннона**

$$(X, K, Y, (f_\chi)_{\chi \in K}),$$

где X, К, У – некоторые конечные множества, которые названы, соответственно, множеством открытых текстов, множеством ключей и множеством шифрованных сообщений (криптограмм). Уравнение шифрования имеет вид $f_\chi(x)=y$. И выполнены 2 условия:

1) функции $f_\chi: X \to Y$ инъективны,

2) Функция от двух переменных $\mathbf{f(x,\chi)}=f_\chi(x)$ сюръектина.

Заметим, что алгебраическая модель фиксированного шифра неоднозначна.

Вероятностная модель шифра К. Шеннона

$(X, K, Y, (f_\chi)_{\chi \in K}, P(X)=(p(x), x \in X), P(K)=(p(k), k \in K)$ – алгебраическая модель снабженная вероятностными распределениями на X и К.

Шифр **совершенный** по К. Шеннону, если имеет место равенство вероятностей: $p(x/y)=p(x)$ при любых $x \in X$, $y \in Y$.

Часто это понятие трактуют как теоретическую стойкость шифра.

Во всех учебниках пишут, что шифр случайного гаммирования теоретически стойкий. Я бы сказал, что при он стойкий при многих его моделях и добавил, что шифр простой замены, используемый для длин текстов равных 1, тоже теоретически стойкий.

Задача 1. Модель шифра К. Шеннона является трех основной алгеброй. На практике многие шифрующие устройства моделируются конечными автоматами. Заменим эту алгебру автоматом.

Пусть A=(X,S,Y,h,f) – конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, функцией перехода h, и функцией выхода f. Условимся о том, что входные последовательности автомата будут открытыми текстами, состояния – ключами, выходные последовательности A(s, J) автомата, отвечающие входным словам J и начальным состояниям s будут криптограммами. Фиксируя длину k входных слов J автомата. Условие совершенности автомата будет иметь вид: p(J/Q))=p(J) для любого входного слова J и любой выходной мультиграмме Q длины k.

Условие: p(J/Q))=p(J) можно заменить на условие: для любой выходной мультиграмме Q автомата имеет место равенство **p(Q/J(1))=p(Q/J(2))** для любых входных слов J(1), J(2) длины **k**.

Естественно, представляет интерес максимальное k=H(A) (степень вероятностной автономности), если такое k существует.

Результаты задачи 1.

Для любого перестановочного автомата A

H(A) $\leq$|S| для автомата Мили и H(A) $\leq$|S|-1 для автомата Мура.

H(A) $\leq$n для линейного векторного автомата размерности n над полем F(q).

Совершенные шифры это хорошие шифры, а какие шифры плохие?

Пример модели совсем плохого шифра.

(X, K, У, ($f\chi)\chi\in$К) с уравнением шифрования

$$\mathbf{f\chi(x)=y=(x,\chi)}$$

Остальные шифры находятся между совсем плохими и совсем хорошими. В плохом шифре по каждому шифртексту однозначно находится открытый текст. Видимо существуют усиления шифра, при которых открытый текст находится неоднозначно. Последнее предположение можно сформулировать так:

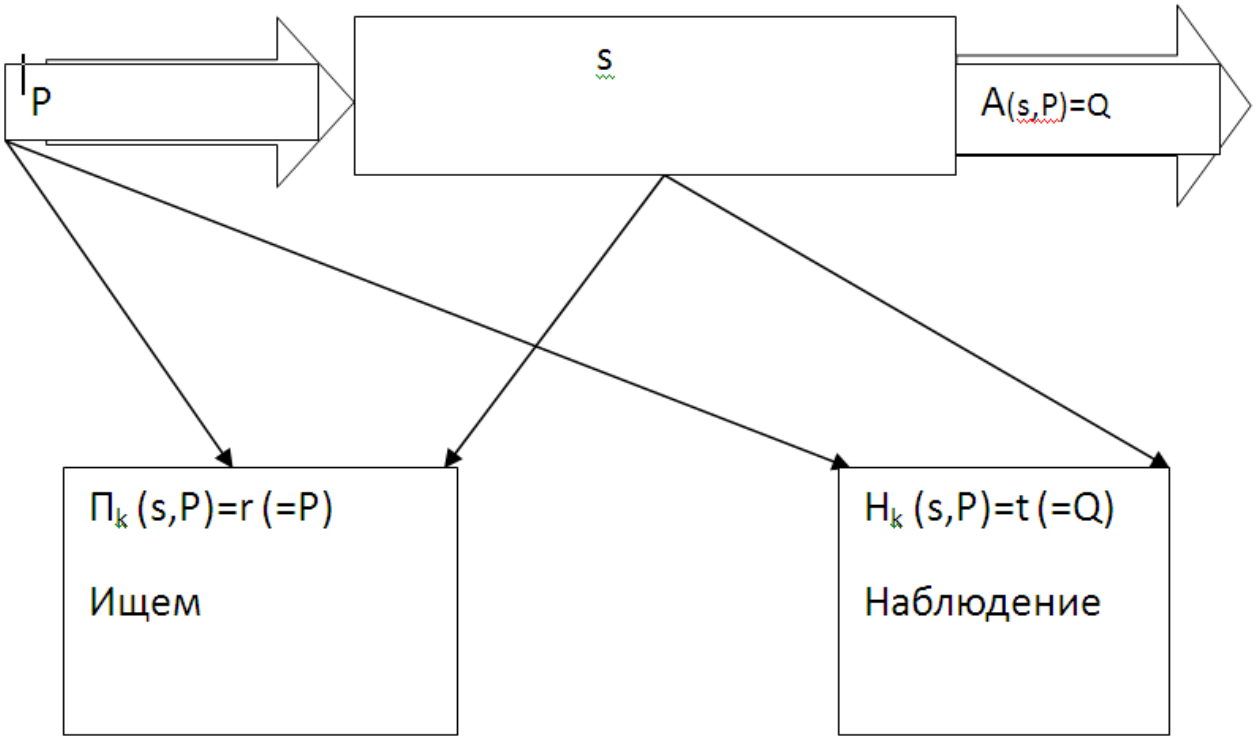
Для шифра **(**X, K, У, ($f\chi)\chi\in$К) существуют не константные функции Φ_1 и Φ_2, при которых

$$\Phi_1(x)=\Phi_2(f\chi(x)),\ \text{при любых } x,\ \chi.$$

Общая задача 2. A=(X,S,Y,h,f) – конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, функцией перехода h, и функцией выхода f;

- Для автомата A=(X,S,Y,h,f) и натурального числа k обозначим через R_k, T_k некоторые конечные множества. Рассмотрим сюръективные отображения
  - $H_k: S \times X^k \to T_k$, $\Pi_k: S \times X^k \to R_k$.
- Полагаем, что на автомат A с начальными состояниями s из S подаются входные слова $P \in X^k$. При этом пары $(s,P) \in S \times X^k$, при которых функционирует автомат, неизвестны. Для каждой пары $(s,P) \in S \times X^k$ известен элемент $t=H_k(s,P)$ – элемент наблюдения для пары (s,P). Задача состоит в определении информации об элементе $r=\Pi_k(s,P)$, r – значение исследуемого (искомого) параметра функционирования автомата A с начальным состоянием s при входном слове P. Под информацией о неизвестном элементе r понимается указание собственного подмножества R` множества $R_k$, в котором содержится r. Формально говоря, считаем, что задана некоторая функция $U_k$ на $R_k$ и ее значение $U_k(r)=j$ и определяет подмножество $R`=\{r`: r` \in R, U_k(r`)=j\}$ (укрупненное состояние). Считаем, что определение j (или, что то же самое, определение подмножества R`) проводится по известному элементу наблюдения $t=H_k(s,P)$. Формально полагаем, что имеется функция Φ_k, значение $\Phi_k(t)$ которой и задает j.

- Таким образом, имеем:
- k - натуральное число, указывающее на длину входных слов автомата;
- $П_k$: $S \times X^k \rightarrow R_k$ - функция цели;
- $r=П_k(s,P)$ – значение исследуемого параметра для тройки $(k,A,(s,P))$, $(s,P) \in S \times X^k$;
- H_k:$S \times X^k \rightarrow T_k$ - функция наблюдения;
- $t=H_k(s,P)$ – элемент наблюдения для тройки $(k,A,(s,P))$, $(s,P) \in S \times X^k$;
- $Ф_k$ – информационная функция наблюдения;
- U_k –информационная целевая функция наблюдения.



$\Phi_k(\Pi_k(s,P)) = U_k(H_k(s,P))$

$\Phi_k(P) = U_k(Q)$ – обобщение плохого шифра

- **Наблюдение $(k,T_k,R_k,H_k,П_k)$ автомата A назовем эффективным**, если найдутся не постоянные функции $Ф_k$ на T_k и U_k на R_k, при которых выполняется равенство
  - $Ф_k(H_k(s, P))=U_k(П_k(s,P))$ (1)
- при любой паре $(s,P)\in S\times X^k$. В таком случае будем говорить, что **автомат A находится под эффективным наблюдением $(k,T_k,R_k,H_k,П_k)$.**
- Отметим, что при постоянных функциях $Ф_k$, U_k равенство (1) не дает содержательной информации о значении исследуемого параметра r при наблюдении t.
- Для последовательности наблюдений $(k,T_k,R_k,H_k,П_k)$, $k\in\{1,2, \ldots\}$ за автоматом A минимальное k, при котором автомат A находится под эффективным наблюдением $(k,T_k,R_k,H_k,П_k)$ называется глубиной эффективного наблюдения автомата A для указанной последовательности и обозначается D(A). Если такого k не существует, то полагаем $D(A)=\infty$. **Функции $Ф_k$ и U_k, при k=D(A) называются основными функциями автомата под эффективным наблюдением $(k,T_k,R_k,H_k,П_k)$.**

- Сформулируем задачу с номером 2 более точно.
- В качестве наблюдения $(k,T_k,R_k,H_k,П_k)$ автомата $A=(X,S,Y,h,f)$ берутся следующие параметры: **T_k – множество всех выходных последовательностей $A(s, P)$ автомата A длины k, $R_k=X_k$, $H_k(s,P)= A(s, P)$, $П_k(s, P)=P$.** Такое наблюдение зависит от параметра k. С криптографической точки зрения естественно встает вопрос о существовании натурального k, при котором заданный автомат $A=(X,S,Y,h,f)$ будет под эффективным наблюдением $(k,T_k,R_k,H_k,П_k)$. При положительном ответе на этот вопрос естественно возникает дальнейшая задача оценки сверху такого минимального k. В случае доказательства того, что такого k не существует, шифр моделируемый таким автоматом, представляет особую ценность.

Результаты задачи 2.

Теорема 1. Автомат A=(X,S,Y,h,f) находится наблюдением $(k,T_k,R_k,H_k,П_k)$ тогда и только тогда, когда rang $H^*_k \vee П^*_k \geq 2$. При этом значения функций $Ф_k H_k$, $U_k П_k$ на $S \times X^k$ одинаковы и постоянны на классах $H^*_k \vee П^*_k$, а значения функций $Ф_k$, U_k постоянны, соответственно, на классах $T_k/П^*_k$ и R_k/H^*_k.

Пояснения обозначений.

Введем бинарные отношения эквивалентности $T_k/П^*_k$ на T_k и R_k/H^*_k на R_k посредством вспомогательного бинарного отношения ~ на T_k и R_k, рассматриваемых одновременно и как множества элементов множеств T_k, R_k и как множества соответствующих классов.

- $t \sim t` \Leftrightarrow \exists\, (s,P) \in t, (s`,P`) \in t`, r \in R_k : (s,P) \in r, (s`,P`) \in r.$
- Отношение эквивалентности $T_k/П^*_k$ есть транзитивное замыкание бинарного отношения ~ , т.е.
- $t_1\ T_k/П^*_k\ t_L \Leftrightarrow \exists\, t_2,\ldots,t_{L-1} \in T_k : t_1 \sim t_2 \sim \ldots \sim t_{L-1} \sim t_L.$
- Аналогично,
- $r \sim r` \Leftrightarrow \exists\, (s,P) \in r, (s`,P`) \in r`, t \in T_r : (s,P) \in t, (s`,P`) \in t,$
- а R_k/H^*_k – транзитивное замыкание отношения ~ на R_k.

Доказано, что

$$\text{rang } H^*_k \vee П^*_k = \text{rang } T_k/П^*_k = \text{rang } R_k/H^*_k \geq 2.$$

- **Теорема** 2. Глубина D(A) наблюдения автомата A для последовательности наблюдений $(k,T_k,R_k,H_k,П_k)$, $k\in\{1,2,\ldots\}$ совпадает с минимальным k, при котором $\text{rang } H^*_k \vee П^*_k \geq 2$. Если такого k не существует, то $D(A)=\infty$.
- **Основная задача**. Фиксируем наблюдение $(k,T_k,R_k,H_k,П_k)$ автомата A=(X,S,Y,h,f): T_k – множество всех выходных последовательностей A(s,P) автомата A длины k, $R_k=X_k$, $H_k(s,P)=A(s,P)$, $П_k(s, P)=P$. Для формулировки результатов введем определения.
- **Определение 1**. Автомат A=(X,S,Y,h,f) называется автоматом с потерей информации 2 типа (СПИ2), если для $L \geq \frac{|S|(|S|-1)}{2}+1$ при любой паре x, x’ из X найдутся s,s’ из S и $P, P' \in X^L$ для которых
- A(s,Px)=A(s’,P’,x’) и $h_{P_x} s = h_{P'_{x'}} s$

Определение 2. Автомат A=(X,S,Y,h,f) называется автоматом с потерей информации 1 типа (СПИ1), если для $L \geq \frac{|S|(|S|-1)}{2}+1$ при любой паре x, x’ из X найдутся s,s’ из S и

$P, P' \in X^{L}$ для которых A(s,Px)=A(s’,P’,x’)

Теорема 2. Если автомат A СПИ2 или престановочный и СПИ1, то A не может быть под эффективным наблюдением: **T_k – множество всех выходных последовательностей A(s, P) автомата A длины k, $R_k=X_k$, $H_k(s,P)= A(s, P)$, $П_k(s, P)=P$. Т.е. глубина** D(A) наблюдения автомата A для последовательности наблюдений ($k,T_k,R_k,H_k,П_k$), **равна бесконечности.**

Определение 3. Автомат A=(X,S,Y,h,f), |X|=|Y| называется обратимым (Курмит), если его функция выходов $f: S \times X \to Y$ при любом s из S осуществляет биекцию X в Y.

Теорема 3. Пусть A=(X,S,Y,h,f) перестановочный обратимый автомат, у которого h(s,x) не зависит от x из X и D – наименьшее общее кратное дли его циклов. Тогда для A найдется k<D+2, при котором наблюдение: **T_k – множество всех выходных последовательностей A(s, P) автомата A длины k, $R_k=X_k$, $H_k(s,P)= A(s, P)$, $П_k(s, P)=P$ эффективно .**

Литература

1. К. Шеннон Работы по теории информации и кибернетике. Ил, М.,1963, 829.
2. Huffman D.A. Canonical forms for information-lossless finite-state logical machines. IRE Trans. Circuit Theory, 6, Spec. Suppl., 1959, 41-59.
3. Huffman D.A. Notes on information-lossless finite-state automata. Nuovo cimento, 13, Suppl. 2, 1959, 397-405.
4. Even Sh. On information-lossless automata of finite order. IEEE Trans. Electronic Comput., 14, 1965, 4, 561-569.
5. Ивен Ш. Об автоматах конечного порядка без потери информации. Труды международного симпозиума по теории релейных устройств и конечных автоматов. М., «Наука», 1965, 269-279.
6. Курмит А.А. Автоматы без потери информации конечного порядка. «Зинатне», Рига, 1972, 264.
7. Бабаш А.В. Криптографические методы защиты информации. Том 3. М., РИОР ИНФРА-М, 2014, 216.