Расчетное задание. **Имитостойкость шифров. Коды аутентификации и стратегии навязывания**

1. Алгебраическая и вероятностная модели кода аутентификации

Алгебраическая и вероятностная модели *кода аутентификации* определяются четвёркой (X,K,A,E) и шестёркой (X,K,A,P(X),P(K)) соответственно, где

X – множество возможных исходных сообщений (шифрвеличин),

K– множество ключей,

A – множество билетов аутентификации,

E – множество преобразований аутентификации, зависящих от ключа: $E=\{e_k : X \to A,\ k \in K\}$.

P(X) – распределение вероятностей на множестве исходных сообщений.

P(K) – распределение вероятностей на множестве ключей.

Сообщение, отправляемое получателю, есть пара y=(x,a), a= $E_k(x)$. Оно принадлежит *множеству сообщений* $M=X\times A$.

Распределения вероятностей P(X) и P(K) индуцируют распределение вероятностей P(M):

$$p(x,a)=p(x)\times p(a|x)= p(x)\times \sum_{a=e_k(x)} p(k) = p(x) \times p_{им}(x,a). \quad (1)$$

Предполагается, что отправителю и получателю известна алгебраическая модель и используемый ключ k. Это позволяет получателю проверить, удовлетворяет ли полученное им сообщение (x',a') равенству $a'=e_k(x')$. Это сообщение вследствие вмешательства третьей стороны может отличаться от (x,a). Если указанное равенство выполняется, то сообщение принимается получателем, иначе оно отклоняется.

Предполагается также, что третьей стороне известна вероятностная модель кода аутентификации и преданное сообщение (x,a), что позволяет ей сформировать сообщение (x',a') или заменить сообщение (x,a) сообщением (x',a') таким образом, чтобы вероятность того, что сообщение (x',a') удовлетворяет равенству $a'=e_k(x')$, была бы максимальной. Тем самым достигается максимальная вероятность $p_{им}$ имитации или $p_{подм}$ подмены сообщения третьей стороной.

2. Вычисление вероятностей имитации и подмены сообщения

Рассмотрим алгебраическую модель (X,K,A,E) кода аутентификации, в которой $X=A=Z_3$ и $K= Z_3\times Z_3$, а преобразование аутентификации для ключа $(i,j)\in K$ определятся соотношением $e_{i,j}(x)=ix+ j \bmod 3$.

Все значения $e_{i,j}(x)$ удобно представить в виде матрицы M аутентификации размеров $|K|\times|X|$. Её строки соответствуют ключам k , а столбцы – исходным сообщениям x. Элементы M(i,j) являются билетами аутентификации $e_{i,j}(x)$. Матрица аутентификации для рассматриваемого примера имеет вид

Ключ k	X		
	0	1	2
(0,0)	0	0	0
(0,1)	1	1	1
(0,2)	2	2	2
(1,0)	0	1	2
(1,1)	1	2	0
(1,2)	2	0	1
(2,0)	0	2	1
(2,1)	1	0	2
(2,2)	2	1	0

Допустим, что распределение вероятностей P(K) является равномерным, то есть для всех $k\in K$ p(k)=1/9. Распределение вероятностей P(X) не рассматриваем, так как в данном случае оно несущественно.

Заметим, что для каждого конкретного ключа k попытка имитации окажется успешной, если для выбранного третьей стороной сообщения x’ будет выполнено равенство $a'=e_k(x')$.

В таблице аутентификации для сообщения x’ возможны три варианта билета аутентификации и каждый конкретный билет встречается в каждом столбце таблицы по три раза и один из случаев использования конкретного билета соответствует успеху имитации (ключу, используемому принимающей стороной). Отсюда следует, что вероятность успешной имитации $p_{им}$ при использовании любого билета равна 1/3.

Рассмотрим теперь задачу подмены. По известной информации (x,a), решая уравнение

$$a=ix+j \bmod 3$$

относительно неизвестных i и j, получим три возможных решения, составляющих множество, которому принадлежит неизвестный третьей стороне ключ k. например, если (x,a)=(0,0), то

$$k\in\{ (0,0), (1,0), (2,0)\}.$$

Только один из них, например, (0,0) используется легальным получателем, а третья сторона, ввиду равновероятного распределения ключей, не имеет оснований отдать предпочтение ни одному из них. Успешная подмена шифрвеличины x, например, шифрвеличиной 2 может быть только при выборе ключа (0,0): если k=(0,0), то $e_k(2)=e_{(0,0)}(x)=0$, в то время как $e_{(1,0)}(2)=2, e_{(2,0)}(2)=1$. Таким образом, из трёх возможных вариантов подмены

$((x',a') \in \{(2,0),(2,1),(2,2)\})$ только первый окажется успешным. Но третья сторона не имеет оснований отдать предпочтение ни одному из этих вариантов. Ввиду равномерного распределения вероятностей ключей вероятность успеха подмены сообщения $p_{подм}$ равна 1/3.

Теперь посмотрим, как вычислить вероятность $p_{им}$ успешной имитации и вероятность $p_{подм}$ успешной подмены сообщения в общем виде. Как и раньше, мы обозначаем k ключ, используемый получателем. Не трудно видеть, что

$$p_{им}(x,a) = p(a = e_k(x)) = \sum_{\{k \in K / e_k(x) = a\}} p(k) .$$

Таким образом, вероятность $p_{им}(x,a)$ успеха имитации (x,a) легко подсчитать как сумму вероятностей ключей, соответствующих тем строкам таблицы аутентификации, которые в столбце x содержат значения a. Вероятность $p_{им}$ успешной имитации можно определить как

$$p_{им} = \max_{x \in X, a \in A} p_{им}(x,a). \qquad (2)$$

Обратим внимание, что эта вероятность не зависит от распределения вероятностей P(X) исходных сообщений.

Вероятность $p_{подм}(x',a';x,a)$ подмены аутентифицированного сообщения (x,a) ложно аутентифицированным сообщением (x',a'), $x' \neq x$ можно вычислить как

$$p_{подм}(y';y) = p_{подм}(x',a';x,a) = p(a' = e_k(x') | a = e_k(x)) =$$

$$= \frac{p((a' = e_k(x')) \wedge (a = e_k(x)))}{p(a = e_k(x))} = \frac{\sum_{(a' = e_k(x')) \wedge (a = e_k(x))} p(k)}{p_{им}(x,a)}. \qquad (3)$$

Для достижения максимальной вероятности успешной подмены данного сообщения (x,a) третья сторона вычислит

$$p_{подм}(x,a) = \max_{x' \in X, a' \in A} p_{подм}(x',a';x,a)$$

и выберет {x',a'} из условия $p_{подм}(x',a';x,a) = p_{подм}(x,a)$. Таким образом, вероятность $p_{подм}(x,a)$ есть вероятность успешной подмены известного аутентифицированного сообщения (x,a) некоторым ложно аутентифицированным сообщением {x',a'}.

Вероятность подмены $p_{подм}$ определяется как средняя вероятность подмены данного сообщения из множества сообщений с распределением вероятностей P(M) (3.1):

$$p_{подм} = \sum_{(x,a)\in M} p(x,a) p_{подм}(x,a).$$

Учитывая (3), это значение можно вычислить и более просто:

$$p_{подм} = \sum_{(x,a)\in M} p(x,a) p_{подм}(x,a) =$$

$$\sum_{(x,a)\in M} p(x)\times p_{им}(x,a) \max_{x'\in X, a'\in A} \frac{\sum\limits_{(a'=e_k(x'))\wedge(a=e_k(x))} p(k)}{p_{им}(x,a)} =$$

$$\sum_{(x,a)\in M} p(x)\times q_{(x,a)},$$

где $q_{(x,a)} = \max\limits_{x'\in X, a'\in A} \sum\limits_{(a'=e_k(x'))\wedge(a=e_k(x))} p(k)$.

В рассмотренном примере $p_{им}(x,a)=1/3$ для всех (x,a), поэтому $p_{им}=1/3$. Можно также проверить, что $p_{подм}(x',a';x,a)=1/3$ для всех $(x'a')$ и (x,a), следовательно $p_{подм}=1/3$ при любых распределениях вероятностей P(X). В общем же случае $p_{подм}$ зависит от P(X).

Пример 3.1. Рассмотрим код аутентификации ({1,2,3,4},{1,2,3},{1,2},E), в котором множество преобразований аутентификации задаётся следующей матрицей аутентификации:

Ключ k	p(k)	X			
		1	2	3	4
1	1/2	1	1	1	2
2	1/4	2	2	1	2
3	1/4	1	2	2	1

Пусть распределения вероятностей P(X) равномерное, то есть $p_X(1)= p_X(2)= p_X(3)= p_X(4)=1/4$, а распределение P(K) ключей таково, что $p_K(1)=1/2$, $p_K(2)= p_K(3)=1/4$.

Вероятности $p_{им}(x,a)$ имитации представлены в правом столбце таблицы ниже.

Как видим, $p_{им}=3/4$, и оптимальной стратегией имитации третьей стороны является навязывание одного из следующих сообщений: (1,1),(3,1) или (4,2).

Для вычисления вероятности $p_{подм}$ и оптимальной стратегии подмены вычислим вероятности $p_{подм}(x',a';x,a)$, $x'\neq x$. Они представлены в следующей таблице (строки соответствуют (x,a), столбцы соответствуют (x',a')

$p_{подм}$ (x’,a’,x,a)	(x’, a’)								$p_{им}$ (x,a)
(x,a)	(1,1)	(1,2)	(2,1)	(2,2)	(3,1)	(3,2)	(4,1)	(4,2)	
(1,1)			2/3	1/3	2/3	1/3	1/3	2/3	¾
(1,2)			0	1	1	0	1	0	¼
(2,1)	1	0			0	1	0	1	½
(2,2)	½	½			½	½	½	½	½
(3,1)	2/3	1/3	2/3	1/3			0	1	¾
(3,2)	1	0	0	1			1	0	¼
(4,1)	1	0	0	1	0	1			¼
(4,2)	2/3	1/3	2/3	1/3	1	0			¾

Из таблицы получаем, что $p_{подм}$ (1,1)=2/3, $p_{подм}$ (2,2)=1/2, $p_{подм}$(x,a)=1 при (x,a) $\notin \{(1,1),(2,2)\}$. Отсюда (учитывая, что

$$p(x,a)= p(x)p_{им}(x,a),\ p(x)=1/4),$$

получим $p_{подм}$ =7/8. Заметим, что в данном примере как следствие равномерности распределения P(X) выполняется равенство p(x,a)=q(x,a), как это представлено в следующей таблице

(x,a)	(1,1)	(1,2)	(2,1)	(2,2)	(3,1)	(3,2)	(4,1)	(4,2)
p(x,a)	½	¼	½	¼	¾	¼	¼	½
q(x,a)	½	¼	½	¼	¾	¼	¼	½

Оптимальная стратегия подмены третьей стороны, обеспечивающая $p_{подм}$ =7/8, представлена в следующей таблице

(x,a)	(1,1)	(1,2)	(2,1)	(2,2)	(3,1)	(3,2)	(4,1)	(4,2)
(x’,a’)	(2,1)	(2,2)	(1,1)	(1,1)	(4,2)	(1,1)	(1,1)	(3,1)

Задание. Написать программу для вычисления вероятностей $p_{подм}$(x’,a’;x,a), x’≠x, $p_{им}$(x,a), и оптимальной стратегии подмены при равномерном распределении вероятностей открытого текста и задаваемом распределении вероятностей ключа для кода аутентификации из примера 1.