Лабораторная работа № 4
Криптографические функции хэширования

Базовое задание (*6 баллов, дата сдачи ≤ 03.06.2021*).

На основе блочной криптосистемы, реализованной в лабораторной работе № 3, построить блочно-итерационную функцию хэширования с шаговой функцией σ (см. вариант в таблице). Описание блочно-итерационных функций хэширования см. в [1] (глава 4).

Фамилия, имя	$\sigma(X \| Y)$
Белицкий Евгений	$F_Y(X) \oplus X$
Бислюк Артём	$F_Y(X \oplus Y) \oplus X \oplus Y$
Бокун Адам	$F_Y(X) \oplus X \oplus Y$
Виноградова Анастасия	$F_Y(X \oplus Y) \oplus X$
Врублевская Екатерина	$F_X(Y) \oplus Y$
Доскоч Роман	$F_X(X \oplus Y) \oplus X \oplus Y$
Ищенко Иван	$F_X(Y) \oplus X \oplus Y$
Козунов Алексей	$F_X(X \oplus Y) \oplus Y$
Кукса Андрей	$F_{X \oplus Y}(X) \oplus X$
Левданская Елизавета	$F_{X \oplus Y}(Y) \oplus Y$
Мигас Злата	$F_{X \oplus Y}(X) \oplus Y$
Никончик Даниил	$F_{X \oplus Y}(Y) \oplus X$
Руткевич Родион	$F_{X \oplus Y}(Y) \oplus X$
Семенович Дмитрий	$F_X(Y) \oplus Y$
Икромов Джовид	$F_{X \oplus Y}(X) \oplus X$

Дополнительные задания (принимаются при условии, что сдано основное задание, *i*-ое дополнительное задание принимается при условии, что сданы дополнительные задания 1,..., *i*–1, *i* = 2, 3,...).

– 1. (2 *балла, дата сдачи ≤ 27.05.2021*). Найти коллизию построенной функции хэширования длины 24 бита.

– 2. (2 *балла, дата сдачи ≤ 20.05.2021*). Исследовать лавинный эффект для построенной функции хэширования *h* по следующей схеме:

а. Выбрать 100 различных сообщений: $x_1,...,x_{100}$.

б. В каждом из этих 100 сообщений изменить 1 бит, эти измененные сообщения обозначим $y_1,...,y_{100}$.

в. Вычислить хэш-значения: $h(x_1),..., h(x_{100}), h(y_1),..., h(y_{100})$.

г. Изобразить на графике множество точек: $\{(i, L(h(x_i), h(y_i))) : i = 1,...,100\}$. Где L – расстояние Хэмминга (число отличающихся бит строк $h(x_i)$ и $h(y_i)$ на одинаковых позициях, примеры: $L(000, 111) = 3$, $L(000, 000) = 0$, $L(000, 001) = 1$, $L(101, 111) = 1$, $L(100, 001) = 2$).

Прокомментировать полученные результаты.

– 3. (1+*4 балла, дата сдачи ≤ 13.05.2021*). Найти коллизию построенной функции хэширования длины 32 бита.

Литература

1. Криптографические методы. С.В. Агиевич. – 2014.
http://apmi.bsu.by/assets/files/agievich/cm.pdf