Защита информации.

Лабораторная работа 5. ХЕШ-ФУНКЦИИ

В лабораторной работе необходимо по алгоритму MD5 получить хеш-образ сообщения, состоящего из первых трех букв своей фамилии.

При оформлении отчета необходимо привести:

- теоретическую часть (лекция 10), включающую "Шаг основного цикла вычисления хеша" (рис.10.2), "Шаг цикла раунда" (рис.10.3) и таблицу "Раундовые функции RF" (табл.10.1);

- исходное сообщение (3 буквы фамилии) в символьном и десятичном представлениях в соответствии с кодировкой Windows 1251;

- прообраз сообщения в шестнадцатеричном представлении (512 бит), включая вспомогательные единичный и нулевые биты, а также биты, определяющие длину сообщения;

- исходные значения переменных A, B, C и D в шестнадцатеричном представлении (по 32 бита);

- для 1-го, 2-го и 16-го 32-битового блока прообраза - результаты вычислений переменных A, B, C и D в шестнадцатеричном представлении для всех раундов;

Раунд	Итерация	Значения переменных							
		в начале итерации				в конце итерации			
		A	B	C	D	A	B	C	D
1	1								
	2								
	...								
	16								
2	1								
	2								
	...								
	16								
3	1								
	2								
	...								
	16								
4	1								
	2								
	...								
	16								

- результат итогового сложения по модулю 2^{32} исходных значений переменных A, B, C и D со значениями этих переменных, полученных после 4-го раунда в шестнадцатеричном представлении (128 бит) до и после перестановки байт.

Контрольные вопросы

1. Дайте определение понятиям: «хеширование», «хеш-функция», «коллизия».

2. В каких целях используют хеш-функции на практике?

3. Приведите стандартную схему алгоритма генерации хеш-образа.

4. Как называется хеш-образ, полученный с применением закрытого ключа шифрования?