**Всем доброго здоровья!**

У студентов, изучающих дисциплину КМЗИ, формально 1 мая не было лекции. В связи с этим я не напрягал вас заданиями.

Теперь придется наверстывать.

**В рамках лабораторной работы №7 (возможно, уже выполнялась) необходимо подробно проработать материал, относящийся к криптографическим аспектам алгоритма решения задачи об укладке ранца.** (см. *лабораторный практикум ч2-рабочий вариант.pdf* в папке КМЗИ на diskstation).

**Тема лекции на 08.05: Алгоритмы хеширования сообщений семейств MD и SHA и их использование в криптографии:**

- основные понятия, классификация и общая характеристика методов хеширования,

- односторонность преобразования и коллизия хеш-функций,

- общая структура и функционал алгоритмов хеширования семейства **MD,** основные шаги хеш-преобразования,

- общая структура и функционал алгоритмов хеширования семейства **SHA,** основные шаги хеш-преобразования,

- стойкость хешей к взлому; Парадокс «дней рождений» и его использование в криптографических приложениях (в т.ч. для анализа коллизий хеш-функций),

- структурные, функциональные особенности и криптостойкость белорусского государственного стандарта хеширования (СТБ 34.101.77-2016),

- криптографические и иные применения хеш-преобразований.

Методические материалы:

- Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студ. спец. 1-98 01 03 «Программное обеспечение информационной безопасности мобильных систем», направления спец. 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)», спец. 1-40 01 01 «Программное обеспечение информационных технологий» спец. 1-40 01 01 10 «Программмирование Интернет-приложений». - Минск : БГТУ, 2016. - 220 с. – пп.10.2-10.3 (файл-книга *криптография.pdf* в папке КМЗИ на diskstation),

- материалы к лабораторной работе №9 (файл *Лабораторная работа 9.pdf* в папке КМЗИ на diskstation),

- стандарт хеширования СТБ 34.101.77-2016 (в папке …/*Урбанович* на diskstation).

Дополнительно:

- Книга Б. Шнайера. Прикладная криптография. (файл SHnaier\_Brus\_Prikladnaya\_kriptografiya.\_Protokoly\_algoritmy\_i\_ishodnye\_teksty\_na\_yazyke\_S\_Litmir.net\_266719\_original\_ad9f9 в папке ЗИНИС на diskstation) – глава 18

**Выполнить задание!!!!**

1. Используя некоторый вектор ***S*** *=* (103, 107, 211, 430, 863, 1716, 3449, 6907, 13807, 27610), вычислить ключи для зашифрования и расшифрования сообщений (относится к ранцевому алгоритму).

2.Найти первообразные корни (если они существуют) чисел (р): 19, 23, 27, 31, 37.

3. Пользователю системы RSA с его собственными ключевыми параметрами n = 3337, е = 79 передано зашифрованное сообщение С, состоящее из трех блоков: чисел, соответствующих порядковым номерам Ваших фамилии, имени и отчества. Расшифровать это сообщение (взломав систему RSA пользователя).

Например, пользователь получил блоки шифртекста (02, 05, 33 – соответствуют **Б**огдановичу **Д**енису **Я**рославовичу – Ваш идентификатор). Нужно определить исходное сообщение (числа или буквы исходного сообщения).

! Для тех, кто не смог решить задачу, - облегченный ее вариант: ключевая информация базируется на использовании числа q=47.

4. Положим, что в системе применяется алгоритм шифрования/ расшифрования Эль-Гамаля. Известны некоторые параметры системы: р = 167, g = 5, y = g29 = 55 mod p.

Используя указанные и недостающие (выбрать самостоятельно) параметры, зашифровать свое имя (в любом языке) в предположении:

а) первая буква алфавита соответствует числу 0 и т. д., б) первая буква алфавита соответствует числу 1.

Проанализировать результат.

5. Задание 6 из вопросов для контроля и самоконтроля к ЛР №9.

6. Задание 8 из вопросов для контроля и самоконтроля к ЛР №9.

7. Задание 9 из вопросов для контроля и самоконтроля к ЛР №9.

**Последний срок выполнения задания – 14 мая**.

Все студенты группы пересылают выполненные задания (форма: электронный документ в текстовом формате или отсканированный рукописный текст) старосте группы, который создает архив и пересылает его на мой адрес ([pav.urb@yandex.by](mailto:pav.urb@yandex.by)) не позднее 15.05;

!!!! некоторые из предыдущих архивом представляли проблему для распаковки; предпочтительно – использовать ZIP, я должен иметь простой доступ к облаку, если используется этот ресурс.

Буду обращать внимание на самостоятельность выполнения задания.

**Задание – часть коллоквиума!**

**С наилучшими пожеланиями,**

**П.Урбанович**