Доброго антивирусного здоровья!

Тема лекции на 22.05: **Эллиптические кривые (ЭК) в криптографии. Стандарты РБ на основе ЭК.**

Изучить вопросы:

• математические основы операций над точками ЭК , уравнение Вейерштрасса;

* ЭК над действительными числами;
* ЭК над конечными полями;

• области использования ЭК в криптографии:

* реализация алгоритма Д-Х,
* реализация шифров,
* реализация ЭЦП;

• генерация ключевой информации с помощью ЭК;

• особенности государственных стандартов РБ на основе ЭК (ЭЦП и инфраструктура публичного ключа).

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 «Программирование Интернет-приложений». - Минск : БГТУ, 2016. - 220 с. – глава 12, п. 5.4.4 (файл книга криптография .pdf в папке ЗИНИС на diskstation),

- рабочие материалы к лабораторной работе 11 (соотв. Файл в папке …/Урбанович/ЗИНИС на diskstation),

- стандарты РБ: СТБ 34.101.45-2013 Стандарт РБ ЭЦП, СТБ 34.101.78-2019 Стандарт РБ Инфраструктура Откр Кл (соотв. Файлы в корне …/Урбанович на diskstation)

**Последний раздел коллоквиума!!!!**

1. Используя методы RSA, Эль-Гамаля и Шнорра, сгенерировать ключевую информацию, используя которую вычислить значение ЭЦП для сообщения, состоящего из 24 младших бит хеша (использовать алгоритм SHA1) собственной фамилии (понятно, что хеш нужно представить десятичным числом) и выполнить процедуру верификации подписи.
2. Каждый (самостоятельно!!!) выполняет (по образцу примеров 1 и 2 из приложенных материалов к лабораторной работе 11) по 3 задачи (вручную) на сложение точек ЭК. ЭК и точки выбрать самостоятельно.

Поскольку задание носит трафаретный характер, будет обращаться серьезное внимание (при оценке) на обоснование и последовательность выполняемых операций.

Задание выполняется в течение недели. Старосты групп пересылают мне архивы не позднее

30.05.

БЕРЕГИТЕ СЕБЯ!!!

П.Урбанович