УДК 512.624.95:378.147.091.3

Методические аспекты изучения современных криптографических систем в курсах технических вузов

Крупенкова Т.Г., Липницкий В.А.*
Белорусский национальный технический университет
Военная академия Республики Беларусь*

В высших технических учебных заведениях дисциплина «Высшая математика» надёжно закрепилась. Однако новые специальности требуют расширения курса математики. Для специальностей, связанных с защитой информации актуальными становятся разделы современной алгебры : теория чисел, теория групп, теория колец, теория полиномов, теория полей и полей Галуа.

Некогда криптография была прерогативой правительств. Военные дипломатические организации использовали её для обеспечения секретности своих сообщений. В настоящее время в её функции входит защита информации.

Новая техника базируется на современной математике.

Современная криптография базируется в кольцах Z/nZ.

Чем глубже и детальнее курс защиты информации, тем глубже требуется погружение в разделы современной алгебры и алгебраической геометрии.

Для изучения криптосистемы RSA нужно знание теории чисел, китайской теоремы об остатках.

Для изучения криптосистемы Эль Гамаля - циклических групп, более тонкое строение Z/nZ.

Для изучения криптосистемы Рабина - квадратичные вычеты, извлечение квадратных корней, числа Блюма.

Для изучения криптосистемы AES – полей Галуа (в $Z/2Z$).

В ближайшем будущем разрабатывается 4 вида новых криптосистем:

1) ECC – криптосистемы эллиптических кривых. Их изучение связано с алгебраической геометрией.

2) XTR – следы в конечных полях. Их изучение связано с Z/pZ.

3) Криптосистемы на основе некоммутативных групп

4) Криптосистема Мак-Элиса–Сидельникова базируется на помехоустойчивых кодах, которая строится на теории полей Галуа.

Таким образом, изучение криптографии требует углублённого изучения математики.

Если мы будем углубляться в аппаратную реализацию – мы привязываемся к современной технике.