Почему математика.

Прежде чем говорить о математике в контексте криптографии, следует упомянуть, что в настоящее время в нашем обществе широко распространено мнение о ненужности математического образования студентов не связанных непосредственно с математическими факультетами. К сожалению, недопонимание роли математики ведёт к уже осязаемому проседанию уровня общества во всех видах её организации. Часто от студентов-информатиков слышны вопросы такие, как: «Зачем нам нужен математический анализ, если мы никогда его в жизни не будем использовать?». В этом вопросе есть недопонимание смысла университетского образования. Во-1-ых, цель образования сформировать научное мышление. Научное мышление есть необходимое условие для способности приобретать и усваивать частный, для каждого индивидуума особенный, неповторимый профессиональный опыт, подобно тому, как операционная система есть основа для инсталляции программ на компьютер. Чтобы получить кратковременную конъюнктурную работу, можно выучиться в кружке вязания или программирования. Но для того, чтобы студент в будущем не был подвержен капризам конъюнктуры, у него должно быть универсальное мышление, способное к обучению долгие годы. Если на вступительных экзаменах в какую-нибудь школу анализа данных спрашивают об интегралах или замечательных пределах в математическом анализе, то это лишь вопрос по форме такой математический, а по содержанию ответа экзаменующегося узнают о его способности обучаться, понимать и научно, точно, аккуратно, грамотно, ясно мыслить. Ведь любую вычислительную проблему, например, взлома шифра, можно решить двумя способами: походом к экстрасенсу и тому подобным специалистам или в мире вычислительно-математических методов. Университет служит развитию возможностей студента во втором мире. Во-2-ых, математика, кроме инструмента формирования научного мышления и инструмента интеллектуального воздействия с целью убеждения, доказательства, играет роль, и как раз в первую очередь, языка общения, хорошо разработанного, сложного, на грани интеллектуальных возможностей современности. Ведь совсем не значит и не имеется в виду, что, изучая математику, студент становится математиком. Точно так же, изучая в школе русский язык, ученик не становится поэтом, писателем, лингвистом, журналистом или учителем русского языка. Язык – инструмент формирования, выражения, передачи и понимания мысли. Это основа всего общества. Математика играет эту роль в научном мире. Поэтому если на вступительных экзаменах в какую-нибудь школу анализа данных спрашивают об интегралах или замечательных пределах в математическом анализе, то это вопрос не только по форме такой, он также выясняет, владеет ли экзаменующийся математическим аппаратом, как основой для анализа данных и синтеза информации. Где большие объемы данных – там необходимо возникает математика для её обработки и понимания. В-3-их, конечно язык по важности стоит на втором месте после мысли, язык ей служит. Но мысль не возникает в пустом месте, а возникает в богатом, глубоком, с широким кругозором мышлении, границы которого очерчены же богатством или узостью языка. Часто можно слышать, что наши вузы готовят востребованных программистов. Но ведь программисты кодируют чьи-то идеи. И основные доходы получают те, кто эту идею придумал. Поэтому наши программисты подобны секретаршам у директоров предприятий: они хорошо, красиво и, может быть, грамотно пишут, и даже получают хорошую зарплату. Но ведь лучше иметь свои мысли, чем чужие. Программисты без математического образования – интеллектуальные рабы на интеллектуальных плантациях, работающие мачете, а не комбайном.

Математика развивает мышление, поэтому она трудная, поэтому ей сопротивляются студенты. Но ведь страна богаче, которая живет своими изобретениями, своими мыслями, от которых получает доход, и не ленится трудиться. Поэтому общество без математики теряет свой уровень жизни в условиях глобальной экономики.

Иллюстрацией сказанному служит криптография. В настоящее время криптография является сложной математической наукой. Почему – сказано выше. Здесь можно еще добавить, что алгоритмы защиты информации требуют обоснованного убеждения пользователей в их стойкости и правильности, поэтом роль математики в криптографии проявляется в полной мере: она служит и как инструмент доказательства, и как средство общения, и как среда рождения новых криптографических идей, мышления.

Изучению необходимого для введения в криптографию минимума «иностранного» языка абстрактной алгебры и теории чисел посвящен данный курс.

Хотелось бы сказать, что при изучении предлагаемого курса студенту необходимо знакомство с математикой в несколько большем объеме, чем предусмотрено в средней школе, что студенту необходимо знать основы линейной алгебры, математического анализа, теории вероятностей, дискретной математики (комбинаторики, теории графов, теории формальных языков) и теории алгоритмов. Но практика показывает плохую математическую подготовку студентов, ограничивающую возможности преподавателя по специальности защиты информации. Поэтому курс имеет лишь элементарный характер.