Введение

Предметом данной книги является изложение основ математической криптографии. Чтобы разъяснить этот предмет более детально, необходимо сначала договориться о терминах.

Криптография — инженерно-техническая дисциплина, основная задача которой состоит в разработке средств защиты информации, использующих математические методы. В процессе разработки и анализа криптографических схем возникают задачи, относящиеся к самым разным математическим дисциплинам. Всю эту совокупность задач мы называем математическими задачами криптографии.

Математическая (или теоретическая) криптография, или, что то же самое, криптология, представляет собой отрасль дискретной математики или математической кибернетики, которая изучает математические модели реальных криптографических схем. По-видимому, ни в одной другой инженерно-технической или научной дисциплине нет такого сходства между математическими моделями и реальными объектами. С одной стороны, это позволяет полагать или надеяться, что теоретическая криптография ближе к практике, чем любая другая математическая теория. С другой, такое сходство зачастую является причиной различного рода недоразумений, из которых основные — неправильная интерпретация результатов теоретических исследований и непонимание целей и задач самой теории.

Криптография состоит из двух частей. Одна из них занимается анализом криптографических схем на предмет выявления различного рода слабостей и называется криптоанализом. Вторая ведает всем, что связано с разработкой криптографических схем и не имеет специального названия. Ее следовало бы называть криптосинтезом. Аналогичное деление есть и в математической криптографии, но оно более условное, т. к. большинство теоретических результатов можно отнести и к криптосинтезу и к криптоанализу.

Подчеркнем, что приведенная выше терминология не является ни устоявшейся, ни общепринятой.

Всюду в данной книге при описании криптосистем используются термины шифрование и дешифрование. В литературе на русском языке более употребительны другие термины: зашифрование и расшифрование, а под дешифрованием обычно понимаются действия криптоаналитика. В слове “зашифрование” присутствует совершенно ненужная приставка, что, впрочем, несущественно. Но в термин “дешифрование” вкладывается другой, едва ли не противоположный, смысл. Мы используем этот термин в том же значении, в каком используются английский термин decryption и его аналоги в различных языках в зарубежной литературе. В отношении же нашей самобытной трактовки этого термина возможны два варианта: либо отгородиться от мирового криптографического сообщества железным занавесом, либо переучиваться. Третьего не дано: попробуйте представить себя, например, в роли синхронного переводчика.

Из используемых в данной книге специальных терминов большинство были придуманы автором, поскольку еще несколько лет назад в литературе на русском языке не существовало никаких эквивалентов соответствующих английских терминов. Многие из этих русскоязычных терминов не слишком удачны и вводились в свое время как временные, но за прошедшие годы ничего лучшего так и не появилось.

Основным в математической криптографии является понятие криптографического протокола. Соответственно, общая схема исследований такова:

- формализация понятия криптографического протокола данного типа;
- математическое определения стойкости формализованного протокола;
- поиск необходимых и достаточных условий существования стойких протоколов данного типа.

Те элементы, из которых строится тот или иной криптографический протокол, принято называть примитивами. Последние могут быть как криптографическими протоколами другого типа (примитивные криптографические протоколы), так и объектами иного рода, например функциями специального вида. Одно из важнейших направлений исследований в теоретической криптографии — поиск наиболее эффективных конструкций криптографических протоколов исходя из различных наборов примитивов. Необходимыми предпосылками являются изучение свойств всех используемых примитивов и разработка надлежащего математического аппарата.

От читателя данной книги требуется знание основных понятий криптографии, с которыми можно познакомиться, например, в книге ”Введение в криптографию” под редакцией В. В. Ященко.