

• ВИКТОРИЯ ЖУРАВЛЁВА •

ИСТОРИЯ ШИФРОВ





Бывает ли, что во время урока тебе хочется отправить другу сообщение? Конечно, сделать это тихо и незаметно — очень важно. Но самое главное — чтобы содержание этой записки не стало известно никому, кроме друга, которому она предназначалась: ни любопытным одноклассникам, ни строгому учителю.

Такие же задачи во все времена стояли не только перед учениками, но и перед купцами, военными и даже королями. Поэтому искусство шифрования и секретной передачи посланий всегда ценилось и совершенствовалось. Шифры постоянно усложнялись, ведь как только они становились известны посторонним, пользоваться ими было уже небезопасно. Как же люди в различные времена передавали свои секреты? Как сейчас зашифровать своё послание так, чтобы его не прочитал посторонний? Ответы на эти вопросы даёт интереснейшая наука — криптография.

Слово «криптография» произошло от древнегреческих слов «крíптос» (тайный) и «грáфо» (пишу). В русском языке шифрование так и называлось — тайнопись. Главная цель этой науки — скрыть смысл сообщения, делая его понятным только тому, кому оно адресовано. Для этого текст зашифровывается по особому правилу, которое известно только адресату. Если же такое письмо попадёт в чужие руки, то его смысл останется никому не понятным.



Из глубины столетий

Наука шифрования столь же древняя, сколь и сама письменность. Как только люди начинали вести важную переписку, у них возникала мысль скрыть свои послания от посторонних глаз. Тайными посланиями обменивались короли и дипломаты, военачальники и купцы. Нередко от того, будет ли прочитано неприятелем секретное сообщение, зависела судьба целой страны.

Различные способы тайной переписки существовали и в Древнем Египте, и в Древней Греции и Риме, и в средневековой Европе, и в Древней Руси. Сегодня принципы шифрования используются всеми странами для сохранения государственных интересов, а также в сфере защиты компьютерной информации и в банковском деле.

Послания из Спарты

Многие принципы современных систем шифрования были придуманы ещё в древности. Один из самых интересных шифров был изобретён в древнегреческом городе Спárта в пятом веке до нашей эры. Для того чтобы закодировать послание, нужно было взять два одинаковых деревянных дорожных посоха, которые назывались «скитáла», и пергаментную* ленту.

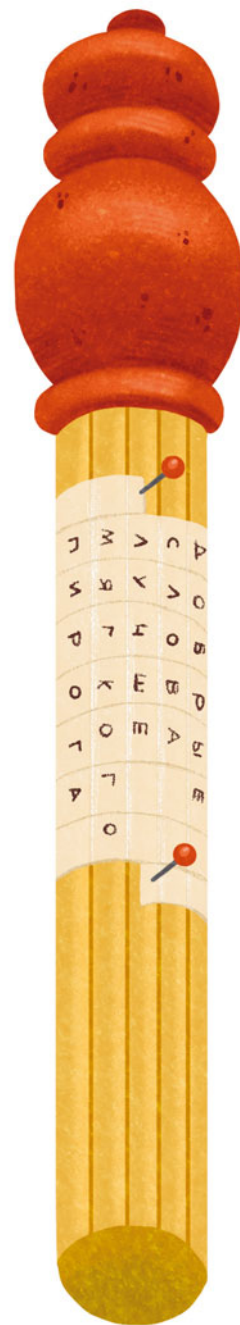
Для создания модели скиталы у себя дома мы можем воспользоваться карандашами и тонкой полоской бумаги шириной один сантиметр. Обернув полосу по спирали вокруг карандаша, напомним небольшую фразу в несколько строчек, вписывая по одной букве на каждый оборот бумаги. Например, напомним поговорку, распределяя каждое слово на отдельной строке:

**ДОБРЫЕ
СЛОВА
ЛУЧШЕ
МЯГКОГО
ПИРОГА**

Затем разматываем ленту — перед нами совершенно непонятный набор букв:

ДСЛМПОЛУЯИБОИГРРВШКОЫАЕОГЕГА

Но если мы снова обернём записку вокруг карандаша, то все буквы встанут на свои места и прочитать текст будет легко. Однако только в том случае,



* Пергамент — обработанная особым образом кожа животного, служившая до изобретения бумаги материалом для письма.

если толщина карандаша у получателя записки будет такая же, как и толщина карандаша у отправителя. Вы можете наладить с друзьями такую переписку, при этом следует хранить в тайне от других, вокруг каких именно предметов вы оборачиваете ваши послания.

Впрочем, разгадать такой шифр можно и без помощи дополнительных средств, хотя спартанские разведчики уничтожали свои посохи при первых же намёках на опасность. Для разгадки было необходимо лишь догадаться, сколько строчек имеется в тайном послании. Если строчек пять, как в нашем варианте, то мы должны записать сначала первую букву, затем — шестую, потом — одиннадцатую и так далее. Следующее слово будет начинаться со второй буквы шифровки, потом — седьмая буква и так далее. Третье слово начинается соответственно с третьей буквы шифровки. Количество знаков между буквами одного слова всегда одинаковое.

Попробуем потренироваться. В замечательной книге «Фиалковый венец» известного писателя Джеффри Триза юные жители древнегреческого города Афины перехватили тайное послание из Спарты, написанное на тонкой полоске кожи. А поскольку посох они не нашли, то стали записывать буквы следующим образом:

ОАНАЕНОП

КТЫНТЯМП

ОЕЙБПТЕИ

НЛПУРВГЯ

ЧЬЛДИДИ

Прочитайте сначала все первые буквы получившихся строк, затем — вторые, потом — третьи и так до самого конца, а затем ответьте, в чьём доме будут происходить дальнейшие события?

