26 Связь между филиалами

Задача. Компания Tenhtam является молодой и динамично развивающейся. Прием на работу в Tenhtam идет по всему миру. Для того, чтобы стать сотрудником требуется ответить всего на один вопрос: каким будет следующий элемент последовательности $\frac{4}{10}, \frac{25}{100}, \frac{168}{1000}, \frac{1229}{10000}$? Бобу поручено наладить защищенное взаимодействие между филиалами компании. Боб организовал в каждом филиале закрытую корпоративную сеть и установил шифровальную машину Amgine. На Amgine попадает вся исходящая корреспонденция филиала и, наоборот, Amgine доставляет сотрудникам филиала всю адресованную им корреспонденцию. Данные, передаваемые между машинами различных филиалов, зашифровываются на общем парном секретном ключе этих филиалов. Объем передаваемых данных быстро растет. Боб опасается, что Виктор, который контролирует открытые каналы связи, может накопить много шифрматериала и определить парный ключ. Поэтому каждое утро парный ключ меняется: новый парный ключ является результатом расшифрования текущей даты на старом ключе. Помогите Виктору найти парный ключ.

Решение. В вопросе указываются дроби $\pi(10^n)/10^n$, где $\pi(x)$ — число простых, не превосходящих x. Следующий элемент последовательности — 9592/100000.

Ответив на вопрос, Виктор устраивается на работу в некоторый филиал и передает дату очередной смены ключа самому себе как шифртекст. Результатом расшифрования будет новый парный ключ. Этот ключ позволит Виктору прочитывать весь трафик между филиалами, а также определять следующие парные ключи.

Интересно, что описанный механизм смены ключа определен в стандарте Интернет RFC 4357. Расшифровывается даже не дата, а фиксированная константа. □