# Ученые факторизовали число RSA-240

Французским ученым удалось взломать самый длинный и сложный ключ шифрования RSA, существующий на сегодняшний день. Для этого они использовали несколько одновременно работающих кластеров компьютеров во Франции, Германии и США, сократив таким образом требуемое на взлом время с 35 млн до нескольких тысяч вычислительных часов.

Алгоритм шифрования RSA является одной из наиболее популярных форм шифрования. Алгоритм применяется в значительном количестве криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и пр.

Томе (Emmanuel Thomé) из Национального института исследований в информатике и автоматике и его коллеги смогли разложить на простые числа RSA-240 длиной 240 десятичных разрядов или 795 бит, так же им удалось вычислить дискретный логарифм такой же длины. Предыдущий рекорд разложения на простые множители был поставлен в 2010 году. Тогда удалось факторизовать число 768 битное число.

Подробнее: https://www.securitylab.ru/news/503232.php